ANEXO III – Formulário de Proposta de Preços

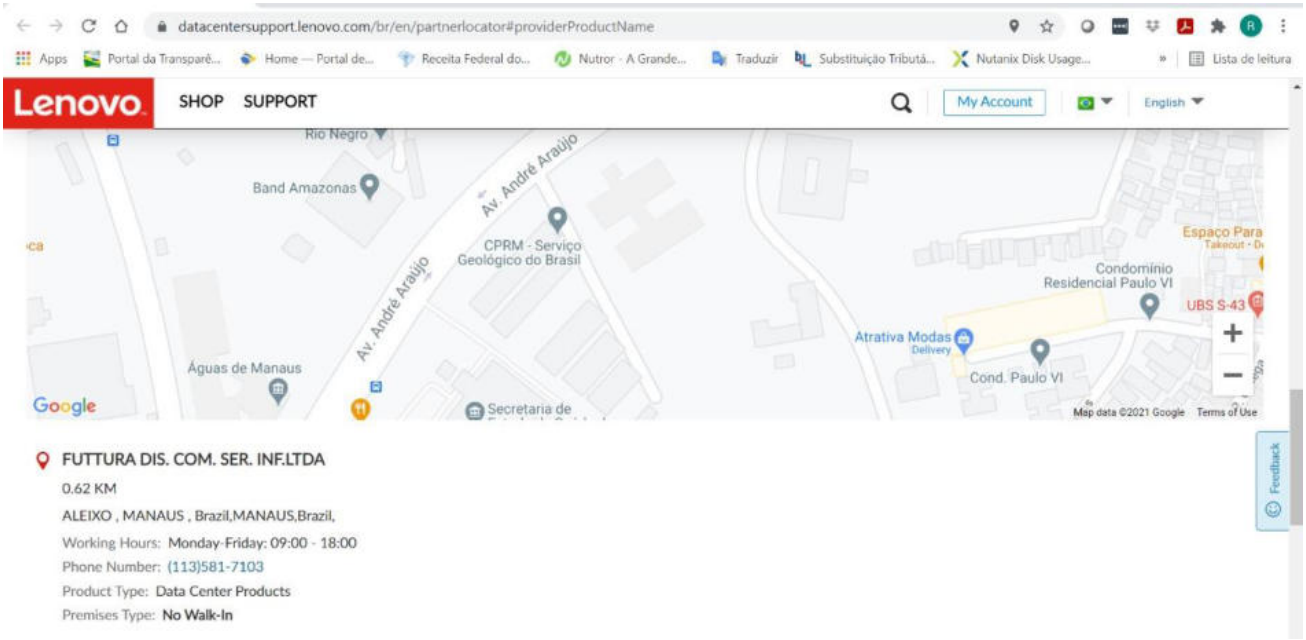
RAZÃO SOCIAL: **CLEAR TECNOLOGIA DA INFORMAÇÃO LTDA.**		
CNPJ: **30.088.923/0001-08**	TELEFONES: **+55 92 3042-0123**	
E-MAIL: **rferreira@clearit.com.br**		
ENDEREÇO: **Rua Franco de Sá, 270 – Sala 408 – São Francisco – 69079-209 – Manaus – AM**		
BANCO: **237 - Bradesco**	AGÊNCIA: **0301**	C/C: **032817-0**

ITEM	DESCRIÇÃO	UNIDADE	QTD.	VALOR UNITÁRIO	VALOR TOTAL
1	Servidor de Rack tipo gabinete, conforme especificações técnicas constantes no item 1 deste Termo de Referência. Marca: LENOVO | THINKSYSTEM SR530	Unid.	70	R$ 31.201,16	R$ 2.184.081,20
2	Unidade de Disco de 8TB SAS de 12Gb/s, conforme especificações técnicas constantes no item 2 deste Termo de Referência. Marca: LENOVO | 7XB7A00045	Unid.	170	R$ 2.716,00	R$ 461.720,00
3	Unidade de Disco de 12TB SAS de 12Gb/s, conforme especificações técnicas constantes no item 3 deste Termo de Referência. Marca: LENOVO | 7XB7A00067	Unid.	40	R$ 3.891,00	R$ 155.640,00
4	Fonte de alimentação (110/220) de 750W, conforme especificações técnicas constantes no item 4 deste Termo de Referência. Marca: LENOVO | 7X77A01303	Unid.	70	R$ 1.161,87	R$ 81.330,90
5	Unidade de memória de 16GB DDR4 de 2666MHz, conforme especificações técnicas constantes no item 5 deste Termo de Referência. Marca: LENOVO | 7N67A00883	Unid.	20	R$ 2.172,80	R$ 43.456,00
6	Rack de Torre Fechado, 42U, conforme especificações técnicas constantes no item 6 deste Termo de Referência. Marca: IPMETAL	Unid.	234	R$ 10.437,00	R$ 2.442.258,00
7	Rack de Parede Telecom 19", 12U, conforme especificações técnicas constantes no item 7 deste Termo de Referência. Marca: IPMETAL	Unid.	60	R$ 2.340,00	R$ 140.400,00
8	Ponto de Acesso WI-FI com PoE, conforme especificações técnicas constantes no item 8 deste Termo de Referência. Marca: UBIQUITI | UAP-AC-PRO	Unid.	170	R$ 1.490,00	R$ 253.300,00
9	Bateria de Nobreak, conforme especificações técnicas constantes no item 9 deste Termo de Referência. Marca: UNICOBA | UNIPOWER UP1270E	Unid.	1500	R$ 113,46	R$ 170190,00
				TOTAL	R$ 5.932.376,10
Cinco milhões, novecentos e trinta e dois mil, trezentos e setenta e seis Reais e dez centavos					

Validade da proposta: 60 (sessenta) dias.

Observação: Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

A LENOVO declara ainda que os drivers, atualizações e suporte dos produtos Lenovo estão disponíveis para download, e busca das autorizadas tecnicas Lenovo mais próxima no site: https://datacentersupport.lenovo.com/br/en/serviceprovider#providerProductName .
A Lenovo dispõe de telefone gratuito 0800-701-4815 (ligações fora da cidade de São Paulo) para abertura de chamados técnicos em Língua Portuguesa e service desk.



Manaus, 15 de abril de 2021.

ROGERIO AUGUSTO FERREIRA:10134666836

Assinado de forma digital por ROGERIO AUGUSTO FERREIRA:10134666836
Dados: 2021.04.15 13:04:46 -03'00'

Rogério Augusto Ferreira
Diretor Administrativo - Representante legal

PROPOSTA TÉCNICA

ESPECIFICAÇÕES TÉCNICAS DOS OBJETOS

MARCA: Lenovo
MODELO: ThinkSystem SR530
DESCRIÇÃO TÉCNICA
ITEM 01 - MODELO SERVIDOR DE RACK
Especificações
Arquitetura e gabinete
- Os servidores possuem arquitetura de processadores que permitem a execução de aplicativos de 32 e 64 bits.
- Compatível com a arquitetura x86/64, na versão ofertada;
- Suporte à migração de máquinas virtuais entre diferentes versões de processadores do mesmo fabricante (extended migration/flex migration);
- Suporte à virtualização de servidores;
- Ocupa 1U no rack;
- O Gabinete é do mesmo fabricante do equipamento.
Placa Mãe e microcomponentes
- A placa mãe é da mesma marca do fabricante do processador do equipamento;
- O Chipset é do mesmo fabricante do processador ou do fabricante da placa mãe, sendo específico para servidores.
BIOS ou UEFI
- O BIOS ou UEFI é desenvolvido pelo mesmo fabricante do equipamento;
- O BIOS ou UEFI possui recurso de controle de permissão através de senhas, uma para inicializar o equipamento e outra para acesso e alterações das configurações do BIOS ou UEFI;
- Possibilidade de selecionar a unidade de inicialização do sistema contemplando disco rígido, unidade USB ou via rede local;
- O BIOS ou UEFI possui recursos de inserção de comandos remotamente através de scripts;
- O BIOS ou UEFI possui número de série / Serviço do equipamento, bem como um campo editável que permita inserir identificação de ativo e que possa ser consultado por software de gerenciamento.
- BIOS/UEFI é 100% (cem por cento) compatível com software de gerenciamento;
- Implementação em memória atualizável por software;
- Relógio calendário (ano com quatro posições) de tempo real, não volátil protegido por bateria;
- Todos os itens integrados à placa principal possuem recursos para desativação, preferencialmente, via BIOS.
Processador
- Possui 01 processador x86, com extensão de 64 bits, com dez núcleos ou mais sendo próprio para servidores;
- O processador está de acordo com a pontuação de desempenho;
- Suporte a software de gerenciamento remoto do Servidor;
- Possui memória cache L3 de 13,75 MB;
- Possui tecnologia Intel Turbo Boost;
- Opera com QuickPath InterConnect (QPI) de, no mínimo, 9.6 GTps;
- Possui tecnologia de otimização para virtualização;
- Possui tecnologia Hyper Threading para até 10 Cores e 20 threads total;
- Possui barramento de sistema (bus) com desempenho igual ao utilizado no respectivo teste (benchmark) publicado pela organização SPEC;

- Todos os servidores X86 fornecidos possuem sistema de detecção de falha dos componentes vitais ao sistema (CPU, memória, discos, ventiladores e fontes).

Desempenho

- O modelo de equipamento ofertado possui índice de desempenho SPEC 2017 INTEGER BASELINE de 119 pontos auditado pelo Standard Performance Evaluation Corporation, por CPU;
- Os resultados estão publicados no site www.spec.org para comprovação.

Memória

- O processador suporta memória RAM do tipo RDIMM DDR4 (Registered DIMM DDR4) com ECC (Error Checkin and Correction) que opere em frequência igual a 2666MHz;
- O servidor possui 32GB de memória RAM em módulos de memória tipo RDIMM DDR4 de pelo menos, 16GB cada, com tecnologia de distribuição de informação detectada pelo recurso ECC, para que, em um caso de falha de memória, as informações possam ser reconstruídas;
- Possui possibilidade de expansão de memória para, pelo menos, 384GB (registered DDR4 DIMMs) e possui 12 slots de memória.

Expansão

- O sistema suporta, pelo menos, três slots tipo PCI Express versão 3.0 ou superior de 8 vias (x8) ou mais rápido;
- Tem 1 slot específico para uma placa 1/10Gbits dual-port. não sendo esse um dos dois slots citados no item acima, podendo ser um slot on-board.

Porta de E/S

- Todos os conectores das portas de entrada/saída de sinal são identificados pelos respectivos nomes ou símbolos;
- O equipamento possui 03 portas USB versão 3.0, sendo pelo menos 01 (uma) delas situadas na parte frontal do gabinete e 02 (duas) na parte traseira;
- O equipamento possui 01 (uma) porta para monitor de vídeo padrão VGA na parte traseira do equipamento, e possibilidade de incluir mais 01 (uma) porta padrão VGA na parte frontal.

Interface de Rede Gigabit RJ-45

- O equipamento possui 2 (duas) interfaces de rede com conector tipo RJ 45;
- As interfaces são capazes de operar nos padrões 10/100/1000;
- IEEE 802.1Qbg Edge Virtual Bridging;
- TCP, IP, and UDP checksum offload;
- Large Send Offload (LSO) and Generic Send Offload (GSO)
- Permite implementação de load balance e failover;
- Admite-se interface de rede embutida na placa principal, desde que mantidas as características descritas nos subitens anteriores.

Fonte de Alimentação e Sistema de Ventilação

- O equipamento suporta fontes de alimentação redundantes e hot, cada uma com potência suficiente para manter o funcionamento do equipamento em sua configuração máxima;
- 01 (uma) fonte de alimentação por equipamento;
- A fonte possui LED indicador de status e suportar uma faixa de tensão de entrada de 100 a 127 VAC e 200 a 240 VAC em 60 Hz, com chaveamento automático de voltagem;
- Recurso de troca sem interrupção para as fontes;
- A fonte possui, no mínimo 750 W de potência e certificação 80+ Platinum comprovada mediante publicação no site www.plugloadsolutions.com/80pluspowersupplies.aspx;
- É fornecido cabo de alimentação para a fonte de alimentação de forma a possibilitar sua instalação;
- O equipamento possui ventilação adequada para a refrigeração de seu sistema interno na sua configuração máxima e dentro dos limites de temperatura adequados para operação;

- Os ventiladores são redundantes.

Software de Gerenciamento

- É fornecido software de gerenciamento desenvolvido pelo fabricante do equipamento;
- O equipamento ofertado possui placa de gerenciamento remoto in band que possibilite seu gerenciamento através de porta RJ-45, não sendo essa nenhuma das interfaces de rede mencionadas no item interface de Rede;
- Solução de gerenciamento de sistemas físicos e virtuais em ambiente heterogêneo, com suporte a vários sistemas operacionais e tecnologias de virtualização;
- O Módulo / Placa de gerenciamento é do mesmo fabricante do equipamento, mantendo total compatibilidade com o mesmo e integração total com o software de gerenciamento solicitado. Tal solução possui as seguintes características;
- Faz uso de criptografia para acesso a console WEB e console CLI, de forma a dificultar a interceptação de dados;
- Possui interface de linha de comando e Web. Para interface Web, por meio de browser padrão pode realizar as tarefas de monitoração e controle, sem nenhum software adicional e independente do sistema operacional;
- Permite visualizar e interagir com aplicativos em um sistema remoto, exibindo a imagem da tela do sistema, utilizando ferramentas de controle remoto padrão de mercado, incluindo o VNC (Virtual Network Computing), RDP (Remote Desktop) e controle remoto baseado na Web para RSA;
- O chip/ placa/ módulo é único em cada servidor e fornece diagnósticos, presença virtual e controle remoto para gerenciar, monitorar e resolver problemas;
- Segurança de acesso e utilização do protocolo TCP/IP;
- É totalmente compatível com os padrões de gerenciamento IPMI (Intelligent Platform Management Interface) 2.0;
- Permite controle remoto tipo virtual KVM, mesmo quando o sistema operacional estiver inoperante;
- Informa o status do equipamento, indicando os componentes com falha e notificando o administrador via e-mail ou trap SNMP;
- Suporta o envio de mensagens de Pré-Falha para no mínimo processadores, fontes, memória, ventiladores e discos;
- Permite remotamente o acesso as mensagens do equipamento, por serial ou LAN;
- Suporte a SSL e SSH de no mínimo 128bits;
- Permite transferir arquivos de um local para outro e sincronizar arquivos, diretórios ou unidades, utilizando uma alternativa segura para o FTP;
- Possui tecnologia de mídia virtual, possibilitando que imagens ISSO sejam montadas remotamente ou através de compartilhamentos CIFS, NFS ou HTTPFS, permitindo inclusive a inicialização (boot) através dessas unidades;
- Permite o desligamento e reinicialização do servidor através da console de gerenciamento, mesmo em condições de indisponibilidade do sistema operacional, além de permitir atualização e configuração remota do BIOS e fornecer indicação de abertura de gabinete e número de série do equipamento;
- Possui gestão automática de chamados ao suporte;
- Permite a descoberta, navegação e visualização de sistemas na rede de dados, permitindo o inventário detalhado e relacionamento com os demais recursos da rede.

Documentação Técnica

- Certificação de compatibilidade com o sistema Vmware ESXi 6.7 U2 publicada no site https://www.vmware.com/resources;

- Certificação de compatibilidade com o sistema operacional RedHat Enterprise Linux 8.x publicada no site https://access.redhat.com/ecosystem/hardware/;
- Certificado da serie ISO-9001 do fabricante do equipamento;
- Certificado de conformidade contra incidentes elétricos e combustão dos materiais elétricos, (Norma IEC 60950) comprovado através de certificado ou relatório de avaliação de conformidade emitido por um órgão credenciado pelo INMETRO ou Certificado internacional, (Safety of Information Technology Equipment Including Eletrical Business Equipment);
- Certificado quanto à emissão de radiação radiada e conduzida. Expedido por órgãos competentes comprovando que o equipamento detém da norma CISPR 22 / EN55022;
- Todos os periféricos, placas, controladoras, módulos de memória, disco rígido, são do mesmo fabricante.

Garantia

- O prazo de garantia padrão é, de 03 (três) anos acrescidos de 02 (dois) anos de garantia estendida, totalizado 05 (cinco) anos de garantia, contado do recebimento provisório. Apresentamos junto a proposta comercial a relação atualizada de assistência técnica autorizada do fabricante para todo o território nacional;
- Os produtos fornecidos estão cobertos por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento;

COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 01 - MODELO SERVIDOR DE RACK	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
Arquitetura e gabinete	N/A	N/A	N/A
- Os servidores deverão possuir arquitetura de processadores que permitam a execução de aplicativos de 32 e 64 bits.	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Intel® 64 Sim
- Compatível com a arquitetura x86/64, na versão mais atualizada do modelo ofertado;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Intel® 64 Sim
- Suporte à migração de máquinas virtuais entre diferentes versões de processadores do mesmo fabricante (extended migration/flex migration);	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Tecnologia de virtualização Intel® (VT-x) Sim Tecnologia de virtualização Intel® para E/S dirigida (VT-d) Sim

- Suporte à virtualização de servidores;	lp1045.pdf	2	Intel Virtualization Technology integrates hardware-level virtualization hooks that allow operating system vendors to better utilize the hardware for virtualization workloads.
- Deve ocupar, no máximo, 1U no rack;	lp1045.pdf	1	Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.
- O Gabinete deverá ser do mesmo fabricante do equipamento.	lp1045.pdf	1	Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth.

			Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.
Placa Mãe e microcomponentes	N/A	N/A	N/A
- A placa mãe deve ser da mesma marca do fabricante do processador do equipamento, não sendo aceitas soluções de outros fabricantes em regime de OEM ou customizações;	lp1045.pdf	6	Chipset Intel C622.
- O Chipset deve ser do mesmo fabricante do processador ou do fabricante da placa mãe, sendo específico para servidores.	lp1045.pdf	6	Chipset Intel C622.
BIOS ou UEFI	N/A	N/A	N/A
- O BIOS ou UEFI deve ser desenvolvido pelo mesmo fabricante do equipamento ou o fabricante deve ter direito de cópia sobre esse BIOS, comprovando através de atestado fornecido pelo fabricante do equipamento;	uefi_setting_guide.pdf	1	UEFI is an interface packed with various features, including system information and settings, boot and runtime services, BMC settings, system event logs, and user security. This guide applies to the following server models:
- O BIOS ou UEFI deve possuir recurso de controle de permissão através de senhas, uma para inicializar o equipamento e outra para acesso e alterações das	uefi_setting_guide.pdf uefi_setting_guide.pdf	38 49	Secure Boot Configuration User security Use this menu to set or change Power-On and Administrator passwords.

configurações do BIOS ou UEFI;			
- Possibilidade de selecionar a unidade de inicialização do sistema contemplando disco rígido, unidade USB ou via rede local;	uefi_setting_guide.pdf	43 e 44	Add UEFI Full Path Boot Option Add one UEFI application or one removable file systems as boot option. Set Boot Priority Set boot priority of the devices in a device group.
- O BIOS ou UEFI deve possuir recursos de inserção de comandos remotamente através de scripts;	uefi_setting_guide.pdf	3	Perform the following steps to first launch the UEFI setup utilities. 1. (Optional)Connect the local keyboard, video, and mouse (KVM) to the server using a cable, or open the Remote Console page on the Lenovo XClarity Controller web user interface (XCC WebUI).
- O BIOS ou UEFI deve possuir número de série / Serviço do equipamento, bem como um campo editável que permita inserir identificação de ativo e que possa ser consultado por software de gerenciamento.	Think_BIOS_Configurator_Manual.pdf	3	At the top of the application screen is the File Actions section. On the left it is possible to browse to and select an .INI file that was previously generated by this program. Once selected, click Apply Settings File to make any changes detected in the .INI file. All the settings are read into the potential changes and then compared to the

			current settings of the machine. Only those that are different will be applied. A dialog box is displayed once the import is completed showing the settings that were successfully changed. This feature is also available via command line which is discussed in the Execution via Command Line section.
- BIOS/UEFI deve ser 100% (cem por cento) compatível com software de gerenciamento;	xcc_book.pdf	1	This document explains how to use the functions of the XClarity Controller in a ThinkSystem server. The XClarity Controller works with the XClarity Provisioning Manager and UEFI to provide systems-management capability for ThinkSystem servers.
- Implementação em memória atualizável por software;	LXPM_user_guide.pdf	42	Firmware Update Click the Firmware Update tab in the left pane to enter the Firmware Update interface. You can update the UEFI firmware, Lenovo XClarity Controller, LXPM V3, Windows drivers, and Linux drivers for your server in the Firmware Update interface. To download the update packages, go to:

- Relógio calendário (ano com quatro posições) de tempo real, não volátil protegido por bateria;	uefi_setting_guide.pdf maintenance_manual.pdf	40 e 41 26	Date and time Use this menu to set the local Date and Time of the system. Clear CMOS jumper JP3 • Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: Clear the real-time clock (RTC) registry.
- Todos os itens que forem integrados à placa principal deverão possuir recursos para desativação, preferencialmente, via BIOS.	uefi_setting_guide.pdf maintenance_manual.pdf	11 23	System setting Select System Settings and press Enter. Then the following window is displayed: Figure 10. System board components
Processador	N/A	N/A	N/A
- Deve possuir 01 processador x86, com extensão de 64 bits, com dez núcleos ou mais sendo próprio para servidores;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- O processador deverá ser de acordo com a pontuação de desempenho, conforme informado no item abaixo com a devida comprovação;	N/A	N/A	N/A
- Suporte a software de gerenciamento remoto do Servidor;	lxca_users_guide.pdf	2	Configuration management You can quickly provision and pre-provision all of your servers using a consistent configuration. Configuration settings (such as local storage, I/O adapters, boot settings, firmware, ports, and

			management controller and UEFI settings) are saved as a server pattern that can be applied to one or more managed servers. When the server patterns are updated, the changes are automatically deployed to the applied servers.
- Deve possuir memória cachê L3 de 13,75 MB;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- Deve possuir tecnologia Intel Turbo Boost;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	2	Tecnologia Intel® Turbo Boost 2.0
- Deve operar com QuickPath InterConnect (QPI) de, no mínimo, 9.6 GTps;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- Deve possuir tecnologia de otimização para virtualização;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	2	Tecnologia de virtualização Intel® (VT-x) Sim Tecnologia de virtualização Intel® para E/S dirigida (VT-d) Sim Intel® VT-x com Tabelas de páginas estendidas (EPT) Sim
- Possuir tecnologia Hyper Threading para até 10 Cores e 20 threads total;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	1	Número de núcleos 10 Nº de threads 20
- Possuir barramento de sistema (bus) com desempenho igual ou	cpu2017-20190513-13808.pdf	1	Hardware

superior ao utilizado no respectivo teste (benchmark) publicado pela organização SPEC;			
- Todos os servidores X86 fornecidos pela CONTRATADA, deverão prover sistema de detecção de falha dos componentes vitais ao sistema (CPU, memória, discos, ventiladores e fontes).	lp1045.pdf	3	Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
Desempenho	N/A	N/A	N/A
- O modelo de equipamento ofertado deve possuir índice de desempenho SPEC 2017 INTEGER BASELINE de, no mínimo, 40 pontos auditado pelo Standard Performance Evaluation Corporation, por CPU. Não serão aceitos modelos de equipamentos não auditados pelo Standard Performance Evaluation Corporation;	cpu2017-20190513-13808.pdf	1	SPECrate2017_int_base = 119
- Os resultados devem estar publicados no site www.spec.org para comprovação.	cpu2017-20190513-13808.pdf	1	SPECrate2017_int_base = 119

Memória	N/A	N/A	N/A
- O processador deve suportar memória RAM do tipo RDIMM DDR4 (Registered DIMM DDR4) com ECC (Error Checkin and Correction) ou tecnologia equivalente e que opere em freqüência igual ou superior a 2666MHz;	lp1045.pdf	6	Memory protection Error correction code (ECC), SDDC (for x4-based memory DIMMs), ADDDC (for x4-based memory DIMMs, requires Intel Xeon Gold or Platinum processors), memory mirroring, memory rank sparing, patrol scrubbing, and demand scrubbing.
- O servidor deve possuir, no mínimo, 32GB de memória RAM em módulos de memória tipo RDIMM DDR4 de pelo menos, 16GB cada, com tecnologia de distribuição de informação detectada pelo recurso ECC, para que, em um caso de falha de memória, as informações possam ser reconstruídas;	Conforme Proposta Comercial		
- Deve possuir possibilidade de expansão de memória para, pelo menos, 384GB (registered DDR4 DIMMs) e possuir no mínimo 12 slots de memória.	lp1045.pdf	6	Memory Up to 12 DIMM sockets (6 DIMMs per processor; six memory channels per processor with one DIMM per channel) with support for the following TruDDR4 RDIMM types and capacities: 8 GB, 16 GB, 32 GB, and 64 GB 2933 MHz. 16 GB and 32 GB 2666 MHz.
Expansão	N/A	N/A	N/A

- O sistema deve suportar, pelo menos, três slots tipo PCI Express versão 3.0 ou superior de 8 vias (x8) ou mais rápido;	lp1045.pdf	6	I/O expansion slots Up to three slots depending on the riser cards installed. The slots are as follows: Slot 1: PCIe 3.0 x8; low profile Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length Slot 3: PCIe 3.0 x8 or x16; low profile PCIe x16 slot 3 requires the second processor to be installed.
- Deverá ter, pelo menos, 1 slot específico para uma placa 1/10Gbits dual-port. não sendo esse um dos dois slots citados no item acima, podendo ser um slot on-board.	lp1045.pdf	6	Network interfaces Onboard LOM slot for up to two additional 1/10 Gb Ethernet ports: 2x 10 GbE RJ-45 ports (no 10/100 Mb support) 1x RJ-45 10/100/1000 Mb Ethernet systems management port.
Porta de E/S	N/A	N/A	N/A
- Todos os conectores das portas de entrada/saída de sinal devem ser identificados pelos respectivos nomes ou símbolos;	lp1045.pdf	4	Figure 2. Front view of the SR530: 4x 3.5-inch drive bays Figure 3. Front view of the SR530: 8x 2.5-inch drive bays
- O equipamento deve possuir, no mínimo, 03 portas USB versão 3.0, sendo pelo menos 01 (uma) delas situadas na parte frontal do gabinete e 02 (duas) na parte traseira;	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.

- O equipamento deve possuir, no mínimo, 01 (uma) porta para monitor de vídeo padrão VGA na parte traseira do equipamento, e possibilidade de incluir mais 01 (uma) porta padrão VGA na parte frontal.	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
Interface de Rede Gigabit RJ-45	N/A		
- O equipamento deve possuir, no mínimo, 2 (duas) interfaces de rede com conector tipo RJ 45;	lp0654.pdf	1	The Intel Ethernet Connection X722 is a network controller embedded into the Intel C624 "Lewisburg" PCH chipset of Lenovo ThinkSystem servers. The controller connects to available 10 GbE and 1 Gigabit Ethernet LAN-on-motherboard (LOM) adapter cards and onboard connectors to provide a comprehensive 1 GbE / 10 GbE networking solution for ThinkSystem customers.
- As interfaces devem ser capazes de operar nos padrões 10/100/1000;	lp0654.pdf	8 10	Adapter connectors: 10 GbE 10GBASE-T adapters: RJ45 connectors 10 GbE standards: IEEE 802.3ab 1000BASE-T copper twisted pair Gigabit Ethernet IEEE 802.3an 10GBASE-T copper twisted pair 10 Gb Ethernet

- IEEE 802.1Qbg Edge Virtual Bridging;	lp0654.pdf	8	Virtual Bridging Support: VEPA/802.1Qbg
- TCP, IP, and UDP checksum offload;	lp0654.pdf	9	TCP/UDP/IP/SCTP Checksum Offload
- Large Send Offload (LSO) and Generic Send Offload (GSO)	lp0654.pdf	6	VXLAN, NVGRE and GENEVE Hardware Offloads: These stateless offloads preserve application performance for overlay networks. With these offloads, it is possible to distribute network traffic across CPU cores. At the same time, the controller offloads LSO, GSO, and checksum from the host software, which reduces CPU overhead.
- Permitir implementação de load balance e failover;	lp0654.pdf	10	IEEE 802.3ad Link Aggregation Control Protocol
- Admite-se interface de rede embutida na placa principal, desde que mantidas as características descritas nos subitens anteriores.	lp1045.pdf	6	The SR530 server has two onboard 1 GbE ports (no 10/100 Mb support) and up to two additional onboard 1/10 GbE network ports (no 10/100 Mb support) with optional LOM cards. Onboard ports and LOM cards use the Intel Ethernet Connection X722 1/10 GbE technology integrated into the Intel C622 Platform Controller Hub (PCH).
Fonte de Alimentação e Sistema de Ventilação	N/A	N/A	N/A
- O equipamento deve suportar fontes de alimentação	lp1045.pdf	6	Power supply Up to two redundant hot-swap 550 W or 750 W

redundantes e hot, cada uma com potência suficiente para manter o funcionamento do equipamento em sua configuração máxima;			(100 - 240 V) High Efficiency Platinum or 750 W (200 - 240 V) High Efficiency Titanium AC power supplies. HVDC support (PRC only).
- No mínimo, 01 (uma) fonte de alimentação por equipamento;	Conforme Proposta Comercial	N/A	N/A
- A fonte deve possuir LED indicador de status e suportar uma faixa de tensão de entrada de 100 a 127 VAC e 200 a 240 VAC em 60 Hz, com chaveamento automático de voltagem;	maintenance_manual.pdf	21	The following illustration shows the LEDs on the rear view of server models with three PCIe slots. The LEDs on the rear view of server models with two PCIe slots are the same.
- Recurso de troca sem interrupção para as fontes;	lp1045.pdf	35	Power supplies and cables The SR530 server supports up to two redundant power supplies and is capable of N+N redundancy depending on the configuration. A second power supply can be added to the models that come with one power supply. The following table lists the power supply options.
- A fonte deve possuir, no mínimo 750 W de potência e certificação 80+ Platinum comprovada mediante publicação no site www.plugloadsolutions.com/80pluspowersupplies.aspx;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Deve ser fornecido cabo de alimentação para a fonte de	Conforme Proposta Comercial		

alimentação de forma a possibilitar sua instalação;			
- O equipamento deve possuir ventilação adequada para a refrigeração de seu sistema interno na sua configuração máxima e dentro dos limites de temperatura adequados para operação;	lp1045.pdf	35	Cooling The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.
- Os ventiladores devem ser redundantes.	lp1045.pdf	35	Cooling The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.
Software de Gernciamento	N/A	N/A	N/A

- Deverá ser fornecido software de gerenciamento desenvolvido pelo fabricante do equipamento;	xcc_book.pdf	1	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers. It is the follow-on to the Integrated Management Module II (IMM2) service processor that consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities into a single chip on the server system board. It provides features such as the following: • Choice of a dedicated or shared Ethernet connection for systems management • Support for HTML5 • Support for access via XClarity Mobile • XClarity Provisioning Manager • Remote configuration using XClarity Essentials or XClarity Controller CLI. • Capability for applications and tools to access the XClarity Controller either locally or remotely • Enhanced remote-presence capabilities. • REST API (Redfish schema) support for additional web-related

			services and software applications.
- O equipamento ofertado deverá possuir placa de gerenciamento remoto in band que possibilite seu gerenciamento através de porta RJ-45, não sendo essa nenhuma das interfaces de rede mencionadas no item interface de Rede;	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port. Systems management XClarity Controller (XCC) Standard, Advanced, or Enterprise (Pilot 4 chip), proactive platform alerts, XClarity Provisioning Manager, XClarity Essentials, XClarity Administrator, XClarity Integrators for VMware vCenter and Microsoft System Center, XClarity Energy Manager, Capacity Planner.

- Solução de gerenciamento de sistemas físicos e virtuais em ambiente heterogêneo, com suporte a vários sistemas operacionais e tecnologias de virtualização;	lxca_users_guide.pdf	1 2 4	Hardware management XClarity Administrator provides agent-free hardware management. It can automatically discover manageable devices, including server, network, and storage hardware. Inventory data is collected for managed devices for an at-a-glance view of the managed hardware inventory and status. Operating-system deployment You can use XClarity Administrator to manage a repository of operating-system images and to deploy operating-system images to up to 28 servers managed servers concurrently. Integration with other managed software XClarity Administrator modules integrate XClarity Administrator with third-party management software to provide discovery, monitoring, configuration, and management functions to reduce the cost and complexity of routine system administration for supported devices. For more information about XClarity

			Administrator, see the following documents: • Lenovo XClarity Integrator for Microsoft System Center • Lenovo XClarity Integrator for VMware vCenter • Lenovo XClarity Integrator for Nutanix Prism
- O Módulo / Placa de gerenciamento deve ser do mesmo fabricante do equipamento, mantendo total compatibilidade com o mesmo e integração total com o software de gerenciamento solicitado. Tal solução deve possuir as seguintes características;	xcc_book.pdf	1	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers.
- Fazer uso de criptografia para acesso a console WEB e console CLI, de forma a dificultar a interceptação de dados;	xcc_book.pdf	6	Use the information in this topic to view the list of supported browsers, cipher suites and operating systems for your server. For increased security,

			only high strength ciphers are now supported when using HTTPS. When using HTTPS, the combination of your client operating system and browser must support one of the following cipher suites:
- Possuir interface de linha de comando e Web. Para interface Web, por meio de browser padrão poder realizar as tarefas de monitoração e controle, sem nenhum software adicional e independente do sistema operacional;	xcc_book.pdf	6 89	Use the information in this topic to view the list of supported browsers, cipher suites and operating systems for your server. Use the XClarity Controller command line interface (CLI) to access the XClarity Controller without having to use the web interface. It provides a subset of the management functions that are provided by the web interface.
- Permitir visualizar e interagir com aplicativos em um sistema remoto, exibindo a imagem da tela do sistema, utilizando ferramentas de controle remoto padrão de mercado, incluindo o VNC (Virtual Network Computing), RDP (Remote Desktop) e controle remoto baseado na Web para RSA	xcc_book.pdf	61	Remote Console Functionality Use the information in this topic to understand how to remotely view and interact with the server console. You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console. You can assign a disk image (ISO or IMG file) as a virtual drive on the server.

			The remote console functionality is available with the XClarity Controller Advanced and XClarity Controller Enterprise features and is only available through the web interface. You must log in to the XClarity Controller with a user ID that has Supervisor access or Remote Console Access privileges to use the remote console features.
- O chip/ placa/ módulo deve ser único em cada servidor e fornecer diagnósticos, presença virtual e controle remoto para gerenciar, monitorar e resolver problemas;	xcc_book.pdf	1 61	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers. You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console.
- Segurança de acesso e utilização do protocolo TCP/IP;	xcc_book.pdf	36	SSL overview This topic is an overview of the SSL security protocol. SSL is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that prevents

			eavesdropping, tampering, and message forgery. You can configure the XClarity Controller to use SSL support for different types of connections, such as secure web server (HTTPS), secure LDAP connection (LDAPS), CIM over HTTPS, and SSH server, and to manage the certificates that are required for SSL.
- Ser totalmente compatível com os padrões de gerenciamento IPMI (Intelligent Platform Management Interface) 2.0;	xcc_book.pdf	2	Industry Standard Management Interfaces • IPMI 2.0 Interface • Redfish • CIM-XML • DCMI 1.5 • SNMPv3 • SNMPv1 (Traps Only) requires minimum v2.10 or v2.12 XCC Firmware updates depending on server type. See XCC Firmware update Change file for details.
- Deve permitir controle remoto tipo virtual KVM, mesmo quando o sistema operacional estiver inoperante;	xcc_book.pdf	61 61 63	You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console. The remote console is able to display only the video that is generated by the video controller on the system board. Remote console

			capture screen Use the information in this topic to understand how to use the remote console screen capture feature. The screen capture feature in the remote console window captures the video display contents of the server. To capture and save a screen image, complete the following steps:
- Deve informar o status do equipamento, indicando os componentes com falha e notificando o administrador via e-mail ou trap SNMP;	xcc_book.pdf	52	To add and modify email and syslog notifications or SNMP TRAP recipients, use the information in this topic.
- Suportar o envio de mensagens de Pré-Falha para no mínimo processadores, fontes, memória, ventiladores e discos;	lp1045.pdf	3	Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.

- Deve permitir remotamente o acesso as mensagens do equipamento, por serial ou LAN;	xcc_book.pdf	33	Enabling or Disabling IPMI Network Access Use the information in this topic to control IPMI network access to the XClarity Controller. Click Network under BMC Configuration to view or modify XClarity Controller IPMI settings. Complete the following fields to view or modify IPMI settings: IPMI over LAN Access Click the switch to enable or disable IPMI network access to the XClarity Controller. Important: • If you are not using any tools or applications that access the XClarity Controller through the network using the IPMI protocol, it is highly recommended that you disable IPMI network access for improved security. • IPMI over LAN access to the XClarity Controller is disabled by default.

- Suporte a SSL e SSH de no mínimo 128bits;	xcc_book.pdf	3 6	Network Protocols • DHCP • DNS • DDNS • HTTP/HTTPS • SNMPv3 • SNMPv1 (Traps only) • SSL • SSH • SMTP • LDAP client • NTP • SLP • SSDP • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-SHA256
- Permitir transferir arquivos de um local para outro e sincronizar arquivos, diretórios ou unidades, utilizando uma alternativa segura para o FTP;	xcc_book.pdf	65 68	Media mount methods – SFTP – SSH File Transfer Protocol – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the checkbox.

			– Enter the credentials that are need to for the XClarity Controller to access the file on the remote system.
- Deve possuir tecnologia de mídia virtual, possibilitando que imagens ISSO sejam montadas remotamente ou através de compartilhamentos CIFS, NFS ou HTTPFS, permitindo inclusive a inicialização (boot) através dessas unidades;	xcc_book.pdf	65 e 66	Media mount methods – CIFS - Common Internet File System: – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the check box. – Enter the credentials that are needed for the XClarity Controller to access the file on the remote system. Note: The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space. – Mount options are optional and defined by the CIFS protocol. – If the remote server belongs to a collection of servers, where the security is centrally handled, enter

			the domain name to which the remote server belongs. – NFS - Network File System: – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the checkbox. – Mount options are optional and defined by the NFS protocol. Both NFSv3 and NFSv4 are supported. For example, to use NFSv3, you need to specify option 'nfsvers=3'. If the NFS server uses AUTH_ SYS security flavor to authenticate NFS operations, you need to specify option 'sec=sys'. – HTTPFS – HTTP Fuse-based File System: – Enter the URL that locates the file on the remote system – If you want the file to be presented to the server as read-only virtual media, tick the check box.

- Deve permitir o desligamento e reinicialização do servidor através da console de gerenciamento, mesmo em condições de indisponibilidade do sistema operacional, além de permitir atualização e configuração remota do BIOS e fornecer indicação de abertura de gabinete e número de série do equipamento;	xcc_book.pdf xcc_book.pdf LXPM_user_guide.pdf LXPM_user_guide.pdf	62 197 10 44	Remote power control This topic explains how to send server power and restart commands from the remote console window. You can send server power and restart commands from the remote console window without returning to the main web page. To control the server power with the remote console, click Power and select one of the following commands: Chassis Intrusion Detection You can enable this function to protect your server by detecting any physical movement of the top cover. System Summary Click the System Summary tab in the left pane to view the following system information in the right p Click the UEFI Setup tab in the left pane to enter the UEFI Setup interface. In the UEFI Setup interface, you can view and change the UEFI settings of your server.

- Possuir gestão automática de chamados ao suporte;	xcc_book.pdf	43	Lenovo is committed to security. When enabled, Call Home automatically contacts Lenovo to open a service ticket and sends in service data collected from a managed device whenever that device reports a hardware failure. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later, your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel.
- Permitir a descoberta, navegação e visualização de sistemas na rede de dados, permitindo o inventário detalhado e relacionamento com os demais recursos da rede.	lxca_users_guide.pdf	1	Lenovo XClarity Administrator is a centralized, resource-management solution that simplifies infrastructure management, speeds responses, and enhances the availability of Lenovo® server systems and solutions. It runs as a virtual appliance that automates discovery, inventory, tracking, monitoring, and provisioning for server, network, and

			storage hardware in a secure environment.
Documentação Técnica	N/A		
- Certificação de compatibilidade com o sistema Vmware ESXi 6.7 U2 publicada no site https://www.vmware.com/resources;	VMware Compatibility Guide - System Search.pdf	1	Model ThinkSystem SR530 CPU Series Intel Xeon Gold 6200/5200 (Cascade-LakeSP/Refresh) Series
- Certificação de compatibilidade com o sistema operacional RedHat Enterprise Linux 8.x publicada no site https://access.redhat.com/ecosystem/hardware/;	ThinkSystem SR530 (Xeon SP Gen 2) - Red Hat Certified Hardware - Red Hat Customer Portal.pdf	1	Products Level
- Certificado da serie ISO-9001 do fabricante do equipamento;	Lenovo ISO 9001.pdf	1	CERTIFICATE
- Certificado de conformidade contra incidentes elétricos e combustão dos materiais elétricos, (Norma IEC 60950) comprovador através de certificado ou relatório de avaliação de conformidade emitido por um órgão credenciado pelo INMETRO ou Certificado internacional, (Safety of Information Technology Equipment Including Eletrical Business Equipment);	lp1045.pdf	51	Regulatory compliance The ThinkSystem SR530 server conforms to the following regulations: United States: FCC Part 15, Class A; UL 60950-1 Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1 Mexico: NOM-19 Argentina: IEC60950-1 European Union: CE Mark (EN55022 Class A, IEC/EN60950-1, EN55024, EN61000-3-2, EN61000-3-3)

- Certificado quanto à emissão de radiação radiada e conduzida. Expedido por órgãos competentes comprovando que o equipamento detém da norma CISPR 22 / EN55022;	lp1045.pdf	51	Australia/New Zealand: AS/NZS CISPR 22 Class A
- A documentação solicitada juntamente com a proposta de preços, será apresentada por parte da licitante detentora do menor lance, Caso não remeta a documentação a licitante terá desclassificada a sua proposta de preços;	N/A	N/A	N/A
- Todos os periféricos, placas, controladoras, módulos de memória, disco rígido, deverão ser do mesmo fabricante, ou homologados pelo mesmo.	Conforme Proposta Comercial		
Garantia	N/A		
- O prazo de garantia padrão deverá ser, no mínimo, de 03 (três) anos acrescidos de 02 (dois) anos de garantia estendida, totalizado 05 (cinco) anos de garantia, contado do recebimento provisório. Caso o licitante não seja o próprio fabricante, deverá ser apresentada junto a proposta comercial a relação atualizada de assistência técnica	Conforme Proposta Comercial	N/A	N/A

autorizada do fabricante para todo o território nacional;			
- Todas as características descritas devem ser comprovadas através de catálogos, manuais, etc;	N/A	N/A	N/A
- Os produtos fornecidos estarão cobertos por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento;	N/A	N/A	N/A
- Declaração da licitante informando a rede autorizada de assistência técnica no Estado do Amazonas. Durante o período de garantia a empresa vencedora devera, sem ônus adicional, fornecer as atualizações (“patches”) corretivas do software e firmware do equipamento fornecido; A empresa vencedora prestará garantia ao sistema fornecido nas seguintes condições: fornecerá informações detalhadas sobre o suporte técnico gratuito (inclusive a ligação telefônica por meio de DDG) em português durante o período de garantia,	N/A	N/A	N/A

incluindo atualização de software. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada gratuita (DDG) em horário comercial, de segunda a sexta-feira (8x5). A contratada deverá possuir central de atendimento técnico, com abertura de chamados via DDG 0800 ou portal web ou e-mail (informar os dados de contato na proposta) realizando a gestão dos processos de suporte e atendimento ‘’on-site”. O equipamento deverá possuir 5 anos de garantia “on-site” com atendimento durante horário comercial (8x5) e dias úteis com presença de técnico “on-site”; Os componentes, peças e materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento;			
- Condições de Entrega: O transporte dos equipamentos até o local especificado,	N/A	N/A	N/A

será realizado pela empresa vencedora (inclusive os procedimentos de seguro, embalagem e transporte até o local especificado);			
- A verificação quanto ao estado dos equipamentos após o transporte será de exclusiva responsabilidade da empresa vencedora, sendo que, quaisquer danos observados no transporte, a qualquer tempo, serão reparados pela empresa vencedora;	N/A	N/A	N/A
- Condições Gerais de Fornecimento: Todos os itens de Hardware deverão ser do mesmo fabricante, mesmo que em regime OEM, neste último caso apresentar comprovação desta condição; O sistema deverá ser fornecido com todos os cabos necessários para a interconexão dos equipamentos adquiridos, além de todos os acessórios de montagem e operação; Apresentar atestado de capacidade técnica compatível com os equipamentos solicitados em quantidade similar com fornecimento e instalação; Os serviços de manutenção e suporte deverão ser	Conforme Proposta Comercial	N/A	N/A

prestados pelo próprio fabricante do equipamento ou através da proponente;			
- PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação;	Conforme Proposta Comercial	N/A	N/A
- Deverá informar o site onde se encontra o catálogo para confirmação das características do equipamento.	N/A	N/A	N/A

MARCA: Lenovo
MODELO: ThinkSystem 3.5 8TB 7.2K SAS 12Gb Hot Swap 512e HDD
DESCRIÇÃO TÉCNICA
ITEM 02 - UNIDADE DE DISCO DE 8TB SAS DE 12GB/S
Especificações mínimas:
- É compatível com o equipamento descrito no item 1;
- Possui o mesmo nível de suporte e garantia;
- Possui formato de 3,5” Hot Swap SATA (HDDs);
- Tem velocidade de 7.200 rpm;
- Tem interface SAS de 12 Gb/s;
- Possui 8TB de capacidade bruta.

COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 02 - UNIDADE DE DISCO DE 8TB SAS DE 12GB/S	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir formato de 3,5” Hot Swap SATA (HDDs);	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Ter velocidade mínima de 7.200 rpm;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Ter no mínimo interface SAS de 12 Gb/s;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Possuir no mínimo 8TB de capacidade bruta.	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4

MARCA: Lenovo
MODELO: ThinkSystem 3.5 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
DESCRIÇÃO TÉCNICA

ITEM 03 - UNIDADE DE DISCO DE 12TB SAS DE 12GB/S
Especificações mínimas:
- É compatível com o equipamento descrito no item 1;
- Possui o mesmo nível de suporte e garantia;
- Possui formato de 3,5” Hot Swap SATA (HDDs);
- Tem velocidade de 7.200 rpm;
- Tem interface SAS de 12 Gb/s;
- Possui 12TB de capacidade bruta.

COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 03 - UNIDADE DE DISCO DE 12TB SAS DE 12GB/S	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir formato de 3,5” Hot Swap SATA (HDDs);	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Ter velocidade mínima de 7.200 rpm;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Ter no mínimo interface SAS de 12 Gb/s;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Possuir no mínimo 12TB de capacidade bruta.	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD

MARCA: Lenovo
MODELO: ThinkSystem 750W(230/115V) Platinum Hot-Swap Power Supply
DESCRIÇÃO TÉCNICA
ITEM 04 - FONTE DE ALIMENTAÇÃO (110/220) DE 750W
Especificações mínimas:
- É compatível com o equipamento descrito no item 1;

- Possui o mesmo nível de suporte e garantia;
- Possui LED indicador de status e suporta uma faixa de tensão de entrada de 100 a 127 VAC e 200 a 240 VAC em 60 Hz, com chaveamento automático de voltagem;
- Tem recurso de troca sem interrupção;
- Possui 750 W de potência e certificação 80+ Platinum comprovada mediante publicação no site www.plugloadsolutions.com/80pluspowersupplies.aspx.

COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 04 - FONTE DE ALIMENTAÇÃO (110/220) DE 750W	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir LED indicador de status e suportar uma faixa de tensão de entrada de 100 a 127 VAC e 200 a 240 VAC em 60 Hz, com chaveamento automático de voltagem;	lp1045.pdf maintenance_manual.pdf	35 21	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply The following illustration shows the LEDs on the rear view of server models with three PCIe slots. The LEDs on the rear view of server models with two PCIe slots are the same.
- Ter recurso de troca sem interrupção;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Possuir, no mínimo 750 W de potência e certificação 80+ Platinum comprovada mediante publicação no site www.plugloadsolution	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply

s.com/80pluspowersupplies.aspx.			

MARCA: Lenovo
MODELO: ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM
DESCRIÇÃO TÉCNICA
ITEM 05 - UNIDADE DE MEMÓRIA DE 16GB DDR4 DE 2666MHZ
Especificações mínimas:
- É compatível com o equipamento descrito no item 1;
- Possui o mesmo nível de suporte e garantia;
- Memória RAM do tipo RDIMM DDR4 (Registered DIMM DDR4) com ECC (Error Checkin and Correction) ou tecnologia equivalente e que opere em frequência igual ou superior a 2666MHz.
COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 05 - UNIDADE DE MEMÓRIA DE 16GB DDR4 DE 2666MHZ	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	19	ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Ser, no mínimo, memória RAM do tipo RDIMM DDR4 (Registered DIMM DDR4) com ECC (Error Checkin and Correction) ou tecnologia equivalente e que opere em frequência igual ou superior a 2666MHz.	lp1045.pdf	19	ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM

MARCA: IP METAL
MODELO: RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm
DESCRIÇÃO TÉCNICA
ITEM 06 - RACK DE TORRE FECHADO
Especificações mínimas:
- Largura: 600 mm;

- Altura: 42US;
- Profundidade: 1070 mm;
- Atende as especificações ANSI/EIA RS-310-E;
- O equipamento é totalmente desmontável para facilitar a montagem e o transporte (rá ser entregue montado);
- A estrutura é em aço SAE 1010/1020 # 2 mm;
- Possui porta frontal curva em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°;
- Possui porta traseira bipartida em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°;
- Ambas as portas possuem fechaduras escamoteáveis com sistema automático de destrave;
- É fornecido com tampas laterais em aço SAE 1010/1020 # 1,2 mm, removíveis através de fechos rápidos, com opção para colocação de fechadura;
- O teto está preparado para instalação de kit de ventiladores, tipo bandeja;
- Possui planos de montagem frontal e traseiro, galvanizados, anti-estáticos e numerados de 1 a 44 US;
- Possui 2 guias de cabos verticais em aço SAE 1010/1020 # 1,0 mm, com anéis internos em termoplástico de alto impacto, nas dimensões de 44U x 95 mm x 70 mm (A x L x P), sendo fixadas na parte frontal do Rack;
- O teto e a base do Rack têm abertura para entrada e saída de cabos, e tampas removíveis;
- A estrutura do Rack possui terminais de aterramento;
- É fornecido com pés niveladores e rodízios, sendo 2 com travas e 2 sem travas;
- Suporta uma carga estática até 800 kg;
- O Rack possui pintura micro epóxi na cor preta;
- Acompanha:
- Duas Réguas de tomadas 19” de 12 posições 20ª;
- Uma Bandeja Fixa, Instalada e Fixada nos Trilhos Frontais e Traseiros do Rack;
- Um kit de Ventilação contendo 2 Ventiladores Exaustores com 1U de tamanho 127/220v, instalado e fixando no Rack na Parte Superior;
- Três Patch Pannel 1U, com 24 portas com conectores fêmeas RJ45 CAT 5e;
- Três guia de cabos;
- Garantia mínima de 12 meses.

COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 06 - RACK DE TORRE FECHADO	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Largura: 600 mm;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT
- Altura: 42US;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT

- Profundidade: 1070 mm;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT
- Deve atender as especificações ANSI/EIA RS-310-E;	Rack Servidor 42U 2mm.pdf	1	Atende especificações ANSI/EIA RS-310-D, I EC 297-2, DIN 41494 partes 1 e 7;
- O equipamento deve ser totalmente desmontável para facilitar a montagem e o transporte (deverá ser entregue montado);	Rack Servidor 42U 2mm.pdf	1	Rack totalmente desmontável;
- A estrutura deve ser em aço SAE 1010/1020 # 2 mm;	Rack Servidor 42U 2mm.pdf	1	Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável;
- Deve possuir porta frontal curva em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°;	Rack Servidor 42U 2mm.pdf	1	Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável;
- Deve possuir porta traseira bipartida em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°;	Rack Servidor 42U 2mm.pdf	1	Porta traseira bipartida perfurada com índice de ventilação de 71%, em aço SAE 1010/1020 1,2 mm, reversíveis em relação ao lado de abertura da porta e intercambiáveis, possibilitando a instalação em ambas a faces do rack (traseira ou frontal), fechadura escamoteável;

- Ambas as portas devem possuir fechaduras escamoteáveis com sistema automático de destrave; - Deve ser fornecido com tampas laterais em aço SAE 1010/1020 # 1,2 mm, removíveis através de fechos rápidos, com opção para colocação de fechadura;	Rack Servidor 42U 2mm.pdf	1	• Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável; • Porta traseira bipartida perfurada com índice de ventilação de 71%, em aço SAE 1010/1020 1,2 mm, reversíveis em relação ao lado de abertura da porta e intercambiáveis, possibilitando a instalação em ambas a faces do rack (traseira ou frontal), fechadura escamoteável;
- O teto deve estar preparado para instalação de kit de ventiladores, tipo bandeja;	Rack Servidor 42U 2mm.pdf	1	Laterais em aço 1,2 mm, removíveis, com fecho rápido (Opcional fechadura do tipo cilíndrico);
- Deve possuir planos de montagem frontal e traseiro, galvanizados, anti-estáticos e numerados de 1 a 44 US;	Rack Servidor 42U 2mm.pdf	2	Teto em aço SAE 1010/1020 # 1,2 mm, com perfuração tipo colmeia, preparado para instalação de unidade de ventilação;
- Deve possuir2 guias de cabos verticais em aço SAE 1010/1020 # 1,0 mm, com anéis internos em termoplástico de alto impacto, nas dimensões de 44U x 95 mm x 70 mm (A x L x	Rack Servidor 42U 2mm.pdf	2	Planos em aço SAE 1010/1020 # 2 mm, galvanizados e anti-estáticos;

P), sendo fixadas na parte frontal do Rack;			
- O teto e a base do Rack deve ter abertura para entrada e saída de cabos, e tampas removíveis;	CatlogoIPMetal.pdf	10	GUIA VERTICAL 44U X 90 X 70 MM
- A estrutura do Rack deve possuir terminais de aterramento;	Rack Servidor 42U 2mm.pdf	1	Entrada e saída de cabos pelo teto ou pela base com tampa modular fechada com parafusos, para que quando não utilizada, não haja ingresso de objetos indesejados no interior do rack;
- Deve ser fornecido com pés niveladores e rodízios, sendo 2 com travas e 2 sem travas;	Rack Servidor 42U 2mm.pdf	1	Fornecido com terminais de aterramento;
- Deve suportar uma carga estática até 800 kg;	Rack Servidor 42U 2mm.pdf	1	• Base em aço SAE 1010/1020 # 1,2 mm, preparada para a instalação de rodízios e pés niveladores simultâneos;
- O Rack deve possuir pintura micro epóxi na cor preta;	Rack Servidor 42U 2mm.pdf	1	Suporte de carga estática para até 800 kg;
- Deverá vir acompanhado:	Rack Servidor 42U 2mm.pdf	1	Pintura pó em micro epóxi na cor preta RAL 9004;
- Duas Réguas de tomadas 19” de 12 posições 20ª;	Conforme Proposta Comercial	N/A	N/A
- Uma Bandeja Fixa, Instalada e Fixada nos Trilhos Frontais e Traseiros do	Conforme Proposta Comercial	N/A	N/A
- Rack;	Conforme Proposta Comercial	N/A	N/A
- Um kit de Ventilação contendo 2 Ventiladores Exaustores com 1U de tamanho	Conforme Proposta Comercial	N/A	N/A

- 127/220v, instalado e Fixando no Rack na Parte Superior;	Conforme Proposta Comercial	N/A	N/A
- Três Patch Pannel 1U, com 24 portas com conectores fêmea RJ45 CAT 5e;	Conforme Proposta Comercial	N/A	N/A
- Três guia de cabos;	Conforme Proposta Comercial	N/A	N/A
- Garantia mínima de 12 meses.	Conforme Proposta Comercial	N/A	N/A

MARCA: IP METAL
MODELO: RACK PAREDE DESMONTAVEL 12U X 600 MM 19 POL.
DESCRIÇÃO TÉCNICA
ITEM 07 - RACK TELECOM DE PAREDE
Especificações mínimas:
- Rack de parede 19” x 12U;
- 600mm de largura e profundidade de 600mm;
- Atender especificações ANSI/EIA RS-310-D, IEC 297-2;
- Porta frontal reversível em vidro temperado, com fechadura tipo cilindro;
- Confeccionado em aço SAE 1020;
- Estrutura em aço 1.5 mm;
- Capacidade de carga estática de 60kg;
- Laterais com fecho rápido com a opção de utilização de chaves nas laterais;
- Entrada e saída de cabos pelo teto ou pela base do rack com acabamento de proteção;
- Teto com preparação para instalação de ventiladores;
- Terminal de aterramento;
- Acompanha:
- Régua de tomadas 19” de 6 posições 20A;
- Um Patch Pannel 1U, com 24 portas com conectores fêmeas RJ45 CAT 5e;
- Um guia de cabos;
- Dezesseis conjuntos de Porca-Gaiola para fixação de Acessórios e Ativos.
- Garantia mínima de 12 meses.

COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 07 - RACK TELECOM DE PAREDE	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Rack de parede 19” x 12U;	Rack Parede 12U 600mm.pdf	1	Altura de 12U – 634 mm;
- 600mm de largura e profundidade de 600mm (mínimo)	Rack Parede 12U 600mm.pdf	1	

- Atender especificações ANSI/EIA RS-310-D, IEC 297-2;	Rack Parede 12U 600mm.pdf	1	Atende especificações ANSI/EIA RS 310-D, IEC 297-2, DIN 41494 partes 1 e 7;
- Porta frontal reversível em vidro temperado, com fechadura tipo cilindro;	Rack Parede 12U 600mm.pdf	1	Porta frontal reversível, com moldura em aço 0,9 mm de espessura, com visor de vidro temperado 4 mm, com ângulo de abertura de 180°, fechadura tipo cilindro com fechadura simples;
- Confeccionado em aço SAE 1020;	Rack Parede 12U 600mm.pdf	1	Fabricado em aço SAE 1020;
- Estrutura em aço 1.5 mm;	Rack Parede 12U 600mm.pdf	1	Estrutura em aço 1,5 mm de espessura, com terminais de aterramento;
- Capacidade de carga estática de 60kg;	Rack Parede 12U 600mm.pdf	1	Capacidade de carga estática até 60 kg;
- Laterais com fecho rápido com a opção de utilização de chaves nas laterais;	Rack Parede 12U 600mm.pdf	1	Laterais removíveis, com fecho rápido;
- Entrada e saída de cabos pelo teto ou pela base do rack com acabamento de proteção;	Rack Parede 12U 600mm.pdf	1	Entrada e saída de cabos pelo teto, com furações oblongadas;
- Teto com preparação para instalação de ventiladores;	Rack Parede 12U 600mm.pdf	1	Teto preparado para instalação de ventiladores;
- Terminal de aterramento;	Rack Parede 12U 600mm.pdf	1	Estrutura em aço 1,5 mm de espessura, com terminais de aterramento;
- Deverá vir acompanhado:	N/A	N/A	N/A
- Régua de tomadas 19” de 6 posições 20A;	Conforme Proposta Comercial	N/A	N/A
- Um Patch Pannel 1U, com 24 portas com conectores fêmea RJ45 CAT 5e;	Conforme Proposta Comercial	N/A	N/A

- Um guia de cabos;	Conforme Proposta Comercial	N/A	N/A
- Dezesseis conjuntos de Porca-Gaiola para fixação de Acessórios e Ativos.	Conforme Proposta Comercial	N/A	N/A
- Garantia mínima de 12 meses.	Conforme Proposta Comercial	N/A	N/A

MARCA: Ubiquiti
MODELO: UAP-AC-PRO
DESCRIÇÃO TÉCNICA
ITEM 08 - PONTO DE ACESSO WI-FI COM PoE
Especificações mínimas:
- Equipamento de ponto de acesso para WLAN, de uso interno (indoor), atendendo aos padrões IEEE 802.11b, IEEE 802.11g, 802.11n, 802.11ac com configuração via software.
- Possui pelo menos dois rádios, permitindo simultaneamente, usuários configurados nos padrões IEEE 802.11b/g/n, na faixa de frequência de 2.4GHz e 802.11n/ac, na faixa de frequência de 5GHz.
- Implementa funcionamento em modo de gerenciamento centralizado pela SOLUÇÃO CENTRALIZADA, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF e outras funcionalidades de Solução Centralizada.
- O ponto de acesso está diretamente conectado à Solução Centralizada da WLAN, inclusive via roteamento da camada de rede OSI.
- Possibilita alimentação elétrica local entre 100V e 230V, em corrente alternada e frequência de 60hz.
- Permite a alimentação elétrica via Power over Ethernet (padrões IEEE 802.3af ou 802.3at) através de uma única interface de rede.
- É fornecido com o adaptador que permita a alimentação via Power over Ethernet (PoE).
- Implementa as seguintes taxas de transmissão e com fallback automático, valores mínimos:
- 802.11b - 1, 2, 5.5, 11 Mbps
- 802.11g - 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 802.11n - 6.5 Mbps a 450 Mbps (MCS0 - MCS23, HT 20/40)
- 802.11ac - 6.5 Mbps a 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)
- Implementa o protocolo de enlace CSMA/CA para acesso ao meio de transmissão.
- Possui capacidade de selecionar automaticamente o canal de transmissão.
- Permite o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.
- Possui suporte a pelo menos 4 SSIDs.
- Implementa diferentes tipos de combinações de criptografia/autenticação por SSID.
- Implementa padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras.
- Não há licença restringindo o número de usuários por ponto de acesso.
- Suporta 200 clientes conectados por ponto de acesso no modo concorrente.
- Possui antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11b/g/n/ac com ganho de pelo menos 3 dBi, com padrão de irradiação omnidirecional multi-banda dipolar, integral e dual mínimo 3X3 MIMO com diversidade espacial.
- Possui potência máxima de transmissão de 22 dBm para IEEE 802.11b/g/n/ac.

- Implementa a pilha de protocolos TCP/IP.
- Implementa VLANs conforme padrão IEEE 802.1q.
- Possui duas interfaces IEEE 802.3 10/100/1000 BaseT Ethernet, auto- sensing, autoMDI/MDX, com conectores RJ-45, para conexão à rede local fixa.
- Implementa o protocolo NTP ou SNTP.
- Possui ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Implementa os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
- Possuir suporte a MIB II, conforme RFC 1213.
- Implementa cliente DHCP, para configuração automática de rede.
- Possui LED's indicativos do estado de operação e atividade dos rádios.
- Possui estrutura que permita fixação do equipamento em teto e parede e acessórios para que possa ser feita a fixação.
- Implementa associação dinâmica de regras de acesso e de QoS por usuário, com base nos parâmetros da etapa de autenticação.
- Possibilita roaming layer 2 (modelo OSI) com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VOIP, streaming de vídeo, videoconferência.
- Implementa criptografia do tráfego local.
- Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.
- Acompanha todos os acessórios necessários para operacionalização do equipamento.
- A solução ofertada possui homologação junto à ANATEL conforme a resolução nº 242, de 30 de novembro de 2000. A exigência de certificação de Produtos de Telecomunicação classificáveis nas Categorias I, II e III do art. 4o da Resolução Anatel 242/2000 é pré-requisito obrigatório para fins de comercialização e utilização no país, para atendimento ao disposto no parágrafo único do art. 20 da Resolução 242 da Anatel. Todas as certificações necessárias m estar disponíveis publicamente nos sítio eletrônico da agência reguladora conforme endereço eletrônico http://sistemas.anatel.gov.br/sgch/

COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 08 - PONTO DE ACESSO WI-FI COM PoE	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Equipamento de ponto de acesso para WLAN, de uso interno (indoor), atendendo aos padrões IEEE 802.11b, IEEE 802.11g, 802.11n, 802.11ac com configuração via software.	UniFi_AC_APs_DS.pdf	10	Wi-Fi Standards 802.11 a/b/g/n/r/k/v/ac

- Deve possuir pelo menos dois rádios, permitindo simultaneamente, usuários configurados nos padrões IEEE 802.11b/g/n, na faixa de frequência de 2.4GHz e 802.11n/ac, na faixa de frequência de 5GHz.	UniFi_AP-AC-Pro_QSG.pdf	26	2G Data Rate Control Select this option to determine what bit rates your 2 4 GHz network will allow Disabling lower bit rates can improve performance for higherdensity networks but will make some older devices incompatible with your network and limit the range of your wireless network 5G Data Rate Control Select this option to determine what bit rates your network will allow Disabling lower bit rates can improve performance for higherdensity networks but will make some older devices incompatible with your network and limit the range of your wireless network
- Deve implementar funcionamento em modo de gerenciamento centralizado pela SOLUÇÃO CENTRALIZADA, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF e outras funcionalidades deSolução Centralizadaritas nesta especificação.	UniFi_AP-Pro_UG.pdf	8	The UniFi Controller software that comes with your UniFi AP-Pro has a browser-based interface for easy configuration and management.

- O ponto de acesso poderá estar diretamente ou remotamente conectado à Solução Centralizada da WLAN, inclusive via roteamento da camada de rede OSI.	UniFi_Controller_V5_UG.pdf	1	Network Topology Requirements • A DHCP-enabled network (so any device can obtain an IP address) • One of the following: • UniFi Cloud Key • A management station running the UniFi Controller software, located either on-site and connected to the same Layer-2 network, or off-site* in a cloud or NOC • For the public address system capability of the UAP-AC-EDU: A compatible Android™ or iOS device located on the same Layer-2 network as the UniFi Controller and UniFi APs
- Possibilitar alimentação elétrica local entre 100V e 230V, em corrente alternada e frequência de 60hz.	PoE_Adapters_DS.pdf	8	U-POE-af 100-240VAC @ 50/60Hz
- Permitir a alimentação elétrica via Power over Ethernet (padrões IEEE 802.3af ou 802.3at) através de uma única interface de rede.	UniFi_AC_APs_DS.pdf	10	Power Method Passive Power over Ethernet (48V), 802.3af/802.3at Supported (Supported Voltage Range: 44 to 57VDC)
- Deve ser fornecido com o adaptador que permita a alimentação via Power over Ethernet (PoE).	UniFi_AP-AC-Pro_QSG.pdf	2	Package Contents

- Implementar as seguintes taxas de transmissão e com fallback automático, valores mínimos:	UniFi_AC_APs_DS.pdf	10	Supported Data Rates (Mbps)
- 802.11b - 1, 2, 5.5, 11 Mbps	UniFi_AC_APs_DS.pdf	10	802.11b 1, 2, 5.5, 11 Mbps
- 802.11g - 6, 9, 12, 18, 24, 36, 48, 54 Mbps	UniFi_AC_APs_DS.pdf	10	802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 802.11n - 6.5 Mbps a 450 Mbps (MCS0 - MCS23, HT 20/40)	UniFi_AC_APs_DS.pdf	10	802.11n 6.5 Mbps to 450 Mbps (MCS0 - MCS23, HT 20/40)
- 802.11ac - 6.5 Mbps a 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)	UniFi_AC_APs_DS.pdf	10	802.11ac 6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)
- Implementar o protocolo de enlace CSMA/CA para acesso ao meio de transmissão.	UniFi_AC_APs_DS.pdf	10	Standard Data Rates 802.11ac 6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80) 802.11n 6.5 Mbps to 450 Mbps (MCS0 - MCS23, HT 20/40) 802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b 1, 2, 5.5, 11 Mbps
- Possuir capacidade de selecionar automaticamente o canal de transmissão.	UniFi - RF Scan Suggested Channels Feature – Ubiquiti Support and Help Center.pdf	1 e 2	The WiFi spectrum must be scanned, manually analyzed, and a channel plan created. Suggested Channels does this automatically: after an RF scan has been triggered, the best channel found will be selected and automatically set, based on how busy the

			channel is, the RSSI of the channel, and whether or not the same SSID is already transmitting on that channel.
- Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.	UniFi_Controller_V5_UG.pdf	135	Transmit Power By default the transmit power is set to Auto You can also manually select the following:
- Possuir suporte a pelo menos 4 SSIDs.	UniFi_AC_APs_DS.pdf	10	BSSID Up to 8 per Radio
- Implementar diferentes tipos de combinações de criptografia/autenticação por SSID.	UniFi_Controller_V5_UG.pdf	23	Create Wireless Network Click to add a wireless network Go to the Create or Edit a Wireless Network section WPA-Personal WPA or Wi-Fi Protected Access was developed as an encryption method stronger than WEP WPA-Personal requires a passphrase to connect to the wireless network
- Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras.	UniFi_AC_APs_DS.pdf	10	WMM Voice, Video, Best Effort, and Background
- Não deve haver licença restringindo o número de usuários por ponto de acesso.	UniFi_AC_APs_DS.pdf	10	Concurrent Clients 250+
- Suportar mínimo 200 clientes conectados	UniFi_AC_APs_DS.pdf	10	Concurrent Clients 250+

por ponto de acesso no modo concorrente.			
- Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11b/g/n/ac com ganho de pelo menos 3 dBi, com padrão de irradiação omnidirecional multi-banda dipolar, integral e dual mínimo 3X3 MIMO com diversidade espacial.	UniFi_AC_APs_DS.pdf	10	Antennas (3) Dual-Band Antennas, 2.4 GHz: 3 dBi, 5 GHz: 3 dBi
- Possuir potência máxima de transmissão de, no mínimo, 22 dBm para IEEE 802.11b/g/n/ac.	UniFi_AC_APs_DS.pdf	10	Maximum TX Power 2.4 GHz 22 dBm 5 GHz 22 dBm
- Implementar a pilha de protocolos TCP/IP.	UniFi_Controller_V5_UG.pdf	1 15	Network Topology Requirements • A DHCP-enabled network (so any device can obtain na IP address) Launch Using Cloud If cloud access is available, then you can use it to access the UniFi Controller Click the appropriate option: Launch using Cloud, Launch using hostname of your Controller, or Launch using IP of your Controller For cloud access, these are the requirements: • Ports 443 (TCP), 3478 (UDP), and 443 (UDP) must be open

- Implementar VLANs conforme padrão IEEE 802.1q.	UniFi_AC_APs_DS.pdf	10	VLAN 802.1Q
- Possuir, no mínimo, duas interfaces IEEE 802.3 10/100/1000 BaseT Ethernet, auto-sensing, autoMDI/MDX, com conectores RJ-45, para conexão à rede local fixa.	UniFi_AC_APs_DS.pdf	10	Networking Interface (2) 10/100/1000 Ethernet Ports
- Implementar o protocolo NTP ou SNTP.	UniFi - Explaining the config.properties File – Ubiquiti Support and Help Center.pdf	4	To change the default NTP server being used, config.ntp_server=0.ubnt.pool.ntp.org
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.	UniFi_Controller_V5_UG.pdf	114	Controller Logs This screen displays device, management, and system log entries
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.	UniFi - UniFi Overview – Ubiquiti Support and Help Center.pdf	5	SNMP v1/2c/3
- Possuir suporte a MIB II, conforme RFC 1213.	UniFi - UniFi Overview – Ubiquiti Support and Help Center.pdf	5	SNMP v1/2c/3
- Implementar cliente DHCP, para configuração automática de rede.	UniFi_Controller_V5_UG.pdf	7	Network Topology Requirements • A DHCP-enabled network (for the wired Access Point to obtain an IP address as well as for the wireless Access Points after the deployment)
- Possuir LED's indicativos do estado de operação e atividade dos rádios.	UniFi_AP-AC-Pro_QSG.pdf	5	Hardware Overview LED
- Possuir estrutura que permita fixação do equipamento em teto	UniFi_AC_APs_DS.pdf	10	Mounting Wall/Ceiling (Kits Included)

e parede e fornecer acessórios para que possa ser feita a fixação.			
- Implementar associação dinâmica de regras de acesso e de QoS por usuário, com base nos parâmetros da etapa de autenticação.	UniFi_AC_APs_DS.pdf	10	Advanced QoS Per-User Rate Limiting
- Possibilitar roaming layer 2 (modelo OSI) com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VOIP, streaming de vídeo, videoconferência.	UniFi - Fast Roaming – Ubiquiti Support and Help Center.pdf	1	As wireless devices improve in power and portability, exceptional on-the-go performance is expected from devices such as tablets, cell phones, and mobile VoIP.
- Implementar criptografia do tráfego local.	UniFi_AC_APs_DS.pdf	10	Wireless Security WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
- Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.	UniFi_Controller_V5_UG.pdf	23	WPA-Personal WPA or Wi-Fi Protected Access was developed as an encryption method stronger than WEP WPA-Personal requires a passphrase to connect to the wireless network
- Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento.	Conforme Proposta Comercial	N/A	N/A

- A solução ofertada deve possuir homologação junto à ANATEL conforme a resolução nº 242, de 30 de novembro de 2000. A exigência de certificação de Produtos de Telecomunicação classificáveis nas Categorias I, II e III do art. 4o da Resolução Anatel 242/2000 é pré-requisito obrigatório para fins de comercialização e utilização no país, para atendimento ao disposto no parágrafo único do art. 20 da Resolução 242 da Anatel. Todas as certificações necessárias devem estar disponíveis publicamente nos sítio eletrônico da agência reguladora conforme endereço eletrônico http://sistemas.anatel.gov.br/sgch/	5ae31c1bbfc33.pdf	1	Modelo - Nome Comercial (s): UAP-AC-PRO (*) - (UAP-AC-PRO (*))

MARCA: UNIPOWER
MODELO: UP1270E
DESCRIÇÃO TÉCNICA
ITEM 09 - BATERIA DE NOBREAK - REPOSIÇÃO
Especificações mínimas:
- VRLA (Chumbo Ácida Selada Regulada por Válvula)
- Vida útil: 02 anos.
- Tensão Nominal: 12V.
- Capacidade C20: 7AH.
- Terminal: tipo Faston 187 - Posição D.
- Temperatura: +15ºC a 50ºC.
- Dimensões aproximadas do produto: 15,1 x 6,5 x 10,0cm.
- Peso aproximado do produto: 1,860Kg.

- Garantia do fornecedor: 12 meses.
- Tecnologia AGM com eletrólito absorvido.
- Livre de Manutenção.
- Vaso em resina ABS especial com elevada resistência mecânica.
- Atende o guia EUROBAT.
- São seguras para o transporte aéreo (IATA-A67).

COMPROVAÇÃO TÉCNICA DO ITEM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 09 - BATERIA DE NOBREAK - REPOSIÇÃO	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- VRLA (Chumbo Ácida Selada Regulada por Válvula	1555958987folder-UNIPOWER_2019_web.pdf	2	A linha excede todos os requisitos da ANATEL, atestando o desempenho excepcional das baterias UNIPOWER® VRLA certificado pelo CPqD.
- Vida útil: 02 anos.	1555958987folder-UNIPOWER_2019_web.pdf	2	As baterias UNIPOWER® têm capacidade extra para suportar condições extremas de descarga em aplicações cíclicas ou em flutuação, sendo consideradas baterias de alta integridade, com vida útil projetada para mais de 10 anos, Certificado ANATEL 570.
- Tensão Nominal: 12V.	1555958987folder-UNIPOWER_2019_web.pdf	2	UP1270 E
- Capacidade C20: 7AH.	1555958987folder-UNIPOWER_2019_web.pdf	2	UP1270 E
- Terminal: tipo Faston 187 - Posição D.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Tipo Terminal Faston 187

- Temperatura: +15ºC a 50ºC.	ManualTecnicoBateria Unipower.pdf	6	Armazenagem A bateria quando armazenada completamente descarregada por um longo período sofre o processo de “sulfatação”. Quanto mais avançado o grau de “sulfatação” da bateria menor é a capacidade de armazenar energia da bateria.Atabela abaixo mostra o tempo máximo de armazenagem em diferentes temperaturas ambientes.
- Dimensões aproximadas do produto: 15,1 x 6,5 x 10,0cm.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Comprimento Largura Altura
- Peso aproximado do produto: 1,860Kg.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Peso (kg)
- Garantia do fornecedor: 12 meses.	Conforme Proposta Comercial	N/A	N/A
- Tecnologia AGM com eletrôlito absorvido.	1555958987folder-UNIPOWER_2019_web .pdf	1	Eletrólito Absorvido em Manta de Fibra de Vidro (AGM) Baixa resistência interna e maior eficiência em altas correntes de descargas. Por que escolher as baterias VRLA UNIPOWER®? UNIPOWER®, marca comercial da UNICOBA Baterias, está presente no mercado desde 1978 e

			conquistou a liderança absoluta em baterias seladas VRLA com produtos de alta qualidade, tecnologia de ponta e portfólio incomparáve
- Livre de Manutenção.	Conforme Proposta Comercial	N/A	N/A
- Vaso em resina ABS especial com elevada resistência mecânica.	1555958987folder-UNIPOWER_2019_web .pdf	1	CAIXA EM ABS Mais robustez, maior proteção para os componentes internos
- Atende o guia EUROBAT.	Conforme Proposta Comercial	N/A	N/A
- São seguras para o transporte aéreo (IATA-A67).	Conforme Proposta Comercial	N/A	N/A

DA GARANTIA

A garantia de todos os itens apresentados está em conformidade com os requisitos do edital referente ao pregão eletrônico 16/2021 do Tribunal de Justiça do Estado do Amazonas.

DOS SERVIÇOS

Os serviços inclusos estão em conformidade com os requisitos do edital referente ao pregão eletrônico 16/2021 do Tribunal de Justiça do Estado do Amazonas.

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 01 - MODELO SERVIDOR DE RACK	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
Arquitetura e gabinete	N/A	N/A	N/A
- Os servidores deverão possuir arquitetura de processadores que permitam a execução de aplicativos de 32 e 64 bits.	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Intel® 64 Sim
- Compatível com a arquitetura x86/64, na versão mais atualizada do modelo ofertado;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Intel® 64 Sim
- Suporte à migração de máquinas virtuais entre diferentes versões de processadores do mesmo fabricante (extended migration/flex migration);	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Tecnologia de virtualização Intel® (VT-x) Sim Tecnologia de virtualização Intel® para E/S dirigida (VT-d) Sim
- Suporte à virtualização de servidores;	lp1045.pdf	2	Intel Virtualization Technology integrates hardware-level virtualization hooks that allow operating system vendors to better utilize the hardware for virtualization workloads.
- Deve ocupar, no máximo, 1U no rack;	lp1045.pdf	1	Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.
- O Gabinete deverá ser do mesmo fabricante do equipamento.	lp1045.pdf	1	Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.
Placa Mãe e microcomponentes	N/A	N/A	N/A
- A placa mãe deve ser da mesma marca do fabricante do processador do equipamento, não sendo aceitas soluções de outros fabricantes em regime de OEM ou customizações;	lp1045.pdf	6	Chipset Intel C622.
- O Chipset deve ser do mesmo fabricante do processador ou do fabricante da placa mãe, sendo específico para servidores.	lp1045.pdf	6	Chipset Intel C622.
BIOS ou UEFI	N/A	N/A	N/A
- O BIOS ou UEFI deve ser desenvolvido pelo mesmo fabricante do equipamento ou o fabricante deve ter direito de cópia sobre esse BIOS, comprovando através de atestado fornecido pelo fabricante do equipamento;	uefi_setting_guide.pdf	1	UEFI is an interface packed with various features, including system information and settings, boot and runtime services, BMC settings, system event logs, and user security. This guide applies to the following server models:
- O BIOS ou UEFI deve possuir recurso de controle de permissão através de senhas, uma para inicializar o equipamento e outra para acesso e alterações das configurações do BIOS ou UEFI;	uefi_setting_guide.pdf uefi_setting_guide.pdf	38 49	Secure Boot Configuration User security Use this menu to set or change Power-On and Administrator passwords.

- Possibilidade de selecionar a unidade de inicialização do sistema contemplando disco rígido, unidade USB ou via rede local;	uefi_setting_guide.pdf	43 e 44	Add UEFI Full Path Boot Option Add one UEFI application or one removable file systems as boot option. Set Boot Priority Set boot priority of the devices in a device group.
- O BIOS ou UEFI deve possuir recursos de inserção de comandos remotamente através de scripts;	uefi_setting_guide.pdf	3	Perform the following steps to first launch the UEFI setup utilities. 1. (Optional)Connect the local keyboard, video, and mouse (KVM) to the server using a cable, or open the Remote Console page on the Lenovo XClarity Controller web user interface (XCC WebUI).
- O BIOS ou UEFI deve possuir número de série / Serviço do equipamento, bem como um campo editável que permita inserir identificação de ativo e que possa ser consultado por software de gerenciamento.	Think_BIOS_Configurator_Manual.pdf	3	At the top of the application screen is the File Actions section. On the left it is possible to browse to and select an .INI file that was previously generated by this program. Once selected, click Apply Settings File to make any changes detected in the .INI file. All the settings are read into the potential changes and then compared to the current settings of the machine. Only those that are different will be applied. A dialog box is displayed once the import is completed showing the settings that were successfully changed. This feature is also available via command line which is discussed in the Execution via Command Line section.
- BIOS/UEFI deve ser 100% (cem por cento) compatível com software de gerenciamento;	xcc_book.pdf	1	This document explains how to use the functions of the XClarity Controller in a ThinkSystem server. The XClarity Controller works with the XClarity Provisioning Manager and UEFI to provide systems-management capability for ThinkSystem servers.
- Implementação em memória atualizável por software;	LXPM_user_guide.pdf	42	Firmware Update Click the Firmware Update tab in the left pane to enter the Firmware Update interface. You can update the UEFI firmware, Lenovo XClarity Controller, LXPM V3, Windows drivers, and Linux drivers for your server in the Firmware Update interface. To download the update packages, go to:
- Relógio calendário (ano com quatro posições) de tempo real, não volátil protegido por bateria;	uefi_setting_guide.pdf maintenance_manual.pdf	40 e 41 26	Date and time Use this menu to set the local Date and Time of the system. Clear CMOS jumper JP3 • Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: Clear the real-time clock (RTC) registry.
- Todos os itens que forem integrados à placa principal deverão possuir recursos para desativação, preferencialmente, via BIOS.	uefi_setting_guide.pdf maintenance_manual.pdf	11 23	System setting Select System Settings and press Enter. Then the following window is displayed: Figure 10. System board components
Processador	N/A	N/A	N/A
- Deve possuir 01 processador x86, com extensão de 64 bits, com dez núcleos ou mais sendo próprio para servidores;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- O processador deverá ser de acordo com a pontuação de desempenho, conforme informado no item abaixo com a devida comprovação;	N/A	N/A	N/A

- Suporte a software de gerenciamento remoto do Servidor;	lxca_users_guide.pdf	2	Configuration management You can quickly provision and pre-provision all of your servers using a consistent configuration. Configuration settings (such as local storage, I/O adapters, boot settings, firmware, ports, and management controller and UEFI settings) are saved as a server pattern that can be applied to one or more managed servers. When the server patterns are updated, the changes are automatically deployed to the applied servers.
- Deve possuir memória cachê L3 de 13,75 MB;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- Deve possuir tecnologia Intel Turbo Boost;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	2	Tecnologia Intel® Turbo Boost 2.0
- Deve operar com QuickPath InterConnect (QPI) de, no mínimo, 9.6 GTps;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- Deve possuir tecnologia de otimização para virtualização;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	2	Tecnologia de virtualização Intel® (VT-x) Sim Tecnologia de virtualização Intel® para E/S dirigida (VT-d) Sim Intel® VT-x com Tabelas de páginas estendidas (EPT) Sim
- Possuir tecnologia Hyper Threading para até 10 Cores e 20 threads total;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	1	Número de núcleos 10 Nº de threads 20
- Possuir barramento de sistema (bus) com desempenho igual ou superior ao utilizado no respectivo teste (benchmark) publicado pela organização SPEC;	cpu2017-20190513-13808.pdf	1	Hardware
- Todos os servidores X86 fornecidos pela CONTRATADA, deverão prover sistema de detecção de falha dos componentes vitais ao sistema (CPU, memória, discos, ventiladores e fontes).	lp1045.pdf	3	Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
Desempenho	N/A	N/A	N/A
- O modelo de equipamento ofertado deve possuir índice de desempenho SPEC 2017 INTEGER BASELINE de, no mínimo, 40 pontos auditado pelo Standard Performance Evaluation Corporation, por CPU. Não serão aceitos modelos de equipamentos não auditados pelo Standard Performance Evaluation Corporation;	cpu2017-20190513-13808.pdf	1	SPECrate2017_int_base = 119
- Os resultados devem estar publicados no site www.spec.org para comprovação.	cpu2017-20190513-13808.pdf	1	SPECrate2017_int_base = 119
Memória	N/A	N/A	N/A
- O processador deve suportar memória RAM do tipo RDIMM DDR4 (Registered DIMM DDR4) com ECC (Error Checkin and Correction) ou tecnologia equivalente e que opere em freqüência igual ou superior a 2666MHz;	lp1045.pdf	6	Memory protection Error correction code (ECC), SDDC (for x4-based memory DIMMs), ADDDC (for x4-based memory DIMMs, requires Intel Xeon Gold or Platinum processors), memory mirroring, memory rank sparing, patrol scrubbing, and demand scrubbing.
- O servidor deve possuir, no mínimo, 32GB de memória RAM em módulos de memória tipo RDIMM DDR4 de pelo menos, 16GB cada, com tecnologia de distribuição de informação detectada pelo recurso ECC, para que, em um caso de falha de memória, as informações possam ser reconstruídas;	Conforme Proposta Comercial		

- Deve possuir possibilidade de expansão de memória para, pelo menos, 384GB (registered DDR4 DIMMs) e possuir no mínimo 12 slots de memória.	lp1045.pdf	6	Memory Up to 12 DIMM sockets (6 DIMMs per processor; six memory channels per processor with one DIMM per channel) with support for the following TruDDR4 RDIMM types and capacities: 8 GB, 16 GB, 32 GB, and 64 GB 2933 MHz. 16 GB and 32 GB 2666 MHz.
Expansão	N/A	N/A	N/A
- O sistema deve suportar, pelo menos, três slots tipo PCI Express versão 3.0 ou superior de 8 vias (x8) ou mais rápido;	lp1045.pdf	6	I/O expansion slots Up to three slots depending on the riser cards installed. The slots are as follows: Slot 1: PCIe 3.0 x8; low profile Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length Slot 3: PCIe 3.0 x8 or x16; low profile PCIe x16 slot 3 requires the second processor to be installed.
- Deverá ter, pelo menos, 1 slot específico para uma placa 1/10Gbits dual-port. não sendo esse um dos dois slots citados no item acima, podendo ser um slot on-board.	lp1045.pdf	6	Network interfaces Onboard LOM slot for up to two additional 1/10 Gb Ethernet ports: 2x 10 GbE RJ-45 ports (no 10/100 Mb support) 1x RJ-45 10/100/1000 Mb Ethernet systems management port.
Porta de E/S	N/A	N/A	N/A
- Todos os conectores das portas de entrada/saída de sinal devem ser identificados pelos respectivos nomes ou símbolos;	lp1045.pdf	4	Figure 2. Front view of the SR530: 4x 3.5-inch drive bays Figure 3. Front view of the SR530: 8x 2.5-inch drive bays
- O equipamento deve possuir, no mínimo, 03 portas USB versão 3.0, sendo pelo menos 01 (uma) delas situadas na parte frontal do gabinete e 02 (duas) na parte traseira;	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
- O equipamento deve possuir, no mínimo, 01 (uma) porta para monitor de vídeo padrão VGA na parte traseira do equipamento, e possibilidade de incluir mais 01 (uma) porta padrão VGA na parte frontal.	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
Interface de Rede Gigabit RJ-45	N/A		
- O equipamento deve possuir, no mínimo, 2 (duas) interfaces de rede com conector tipo RJ 45;	lp0654.pdf	1	The Intel Ethernet Connection X722 is a network controller embedded into the Intel C624 "Lewisburg" PCH chipset of Lenovo ThinkSystem servers. The controller connects to available 10 GbE and 1 Gigabit Ethernet LAN-on-motherboard (LOM) adapter cards and onboard connectors to provide a comprehensive 1 GbE / 10 GbE networking solution for ThinkSystem customers.
- As interfaces devem ser capazes de operar nos padrões 10/100/1000;	lp0654.pdf	8 10	Adapter connectors: 10 GbE 10GBASE-T adapters: RJ45 connectors 10 GbE standards: IEEE 802.3ab 1000BASE-T copper twisted pair Gigabit Ethernet IEEE 802.3an 10GBASE-T copper twisted pair 10 Gb Ethernet
- IEEE 802.1Qbg Edge Virtual Bridging;	lp0654.pdf	8	Virtual Bridging Support: VEPA/802.1Qbg
- TCP, IP, and UDP checksum offload;	lp0654.pdf	9	TCP/UDP/IP/SCTP Checksum Offload

- Large Send Offload (LSO) and Generic Send Offload (GSO)	lp0654.pdf	6	VXLAN, NVGRE and GENEVE Hardware Offloads: These stateless offloads preserve application performance for overlay networks. With these offloads, it is possible to distribute network traffic across CPU cores. At the same time, the controller offloads LSO, GSO, and checksum from the host software, which reduces CPU overhead.
- Permitir implementação de load balance e failover;	lp0654.pdf	10	IEEE 802.3ad Link Aggregation Control Protocol
- Admite-se interface de rede embutida na placa principal, desde que mantidas as características descritas nos subitens anteriores.	lp1045.pdf	6	The SR530 server has two onboard 1 GbE ports (no 10/100 Mb support) and up to two additional onboard 1/10 GbE network ports (no 10/100 Mb support) with optional LOM cards. Onboard ports and LOM cards use the Intel Ethernet Connection X722 1/10 GbE technology integrated into the Intel C622 Platform Controller Hub (PCH).
Fonte de Alimentação e Sistema de Ventilação	N/A	N/A	N/A
- O equipamento deve suportar fontes de alimentação redundantes e hot, cada uma com potência suficiente para manter o funcionamento do equipamento em sua configuração máxima;	lp1045.pdf	6	Power supply Up to two redundant hot-swap 550 W or 750 W (100 - 240 V) High Efficiency Platinum or 750 W (200 - 240 V) High Efficiency Titanium AC power supplies. HVDC support (PRC only).
- No mínimo, 01 (uma) fonte de alimentação por equipamento;	Conforme Proposta Comercial	N/A	N/A
- A fonte deve possuir LED indicador de status e suportar uma faixa de tensão de entrada de 100 a 127 VAC e 200 a 240 VAC em 60 Hz, com chaveamento automático de voltagem;	maintenance_manual.pdf	21	The following illustration shows the LEDs on the rear view of server models with three PCIe slots. The LEDs on the rear view of server models with two PCIe slots are the same.
- Recurso de troca sem interrupção para as fontes;	lp1045.pdf	35	Power supplies and cables The SR530 server supports up to two redundant power supplies and is capable of N+N redundancy depending on the configuration. A second power supply can be added to the models that come with one power supply. The following table lists the power supply options.
- A fonte deve possuir, no mínimo 750 W de potência e certificação 80+ Platinum comprovada mediante publicação no site www.plugloadsolutions.com/80pluspowersupplies.aspx;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Deve ser fornecido cabo de alimentação para a fonte de alimentação de forma a possibilitar sua instalação;	Conforme Proposta Comercial		
- O equipamento deve possuir ventilação adequada para a refrigeração de seu sistema interno na sua configuração máxima e dentro dos limites de temperatura adequados para operação;	lp1045.pdf	35	Cooling The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.
- Os ventiladores devem ser redundantes.	lp1045.pdf	35	Cooling The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.
Software de Gernciamento	N/A	N/A	N/A

- Deverá ser fornecido software de gerenciamento desenvolvido pelo fabricante do equipamento;	xcc_book.pdf	1	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers. It is the follow-on to the Integrated Management Module II (IMM2) service processor that consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities into a single chip on the server system board. It provides features such as the following: • Choice of a dedicated or shared Ethernet connection for systems management • Support for HTML5 • Support for access via XClarity Mobile • XClarity Provisioning Manager • Remote configuration using XClarity Essentials or XClarity Controller CLI. • Capability for applications and tools to access the XClarity Controller either locally or remotely • Enhanced remote-presence capabilities. • REST API (Redfish schema) support for additional web-related services and software applications.
- O equipamento ofertado deverá possuir placa de gerenciamento remoto in band que possibilite seu gerenciamento através de porta RJ-45, não sendo essa nenhuma das interfaces de rede mencionadas no item interface de Rede;	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port. Systems management XClarity Controller (XCC) Standard, Advanced, or Enterprise (Pilot 4 chip), proactive platform alerts, XClarity Provisioning Manager, XClarity Essentials, XClarity Administrator, XClarity Integrators for VMware vCenter and Microsoft System Center, XClarity Energy Manager, Capacity Planner.

- Solução de gerenciamento de sistemas físicos e virtuais em ambiente heterogêneo, com suporte a vários sistemas operacionais e tecnologias de virtualização;	lxca_users_guide.pdf	1 2 4	Hardware management XClarity Administrator provides agent-free hardware management. It can automatically discover manageable devices, including server, network, and storage hardware. Inventory data is collected for managed devices for an at-a-glance view of the managed hardware inventory and status. Operating-system deployment You can use XClarity Administrator to manage a repository of operating-system images and to deploy operating-system images to up to 28 servers managed servers concurrently. Integration with other managed software XClarity Administrator modules integrate XClarity Administrator with third-party management software to provide discovery, monitoring, configuration, and management functions to reduce the cost and complexity of routine system administration for supported devices. For more information about XClarity Administrator, see the following documents: • Lenovo XClarity Integrator for Microsoft System Center • Lenovo XClarity Integrator for VMware vCenter • Lenovo XClarity Integrator for Nutanix Prism
- O Módulo / Placa de gerenciamento deve ser do mesmo fabricante do equipamento, mantendo total compatibilidade com o mesmo e integração total com o software de gerenciamento solicitado. Tal solução deve possuir as seguintes características;	xcc_book.pdf	1	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers.
- Fazer uso de criptografia para acesso a console WEB e console CLI, de forma a dificultar a interceptação de dados;	xcc_book.pdf	6	Use the information in this topic to view the list of supported browsers, cipher suites and operating systems for your server. For increased security, only high strength ciphers are now supported when using HTTPS. When using HTTPS, the combination of your client operating system and browser must support one of the following cipher suites:
- Possuir interface de linha de comando e Web. Para interface Web, por meio de browser padrão poder realizar as tarefas de monitoração e controle, sem nenhum software adicional e independente do sistema operacional;	xcc_book.pdf	6 89	Use the information in this topic to view the list of supported browsers, cipher suites and operating systems for your server. Use the XClarity Controller command line interface (CLI) to access the XClarity Controller without having to use the web interface. It provides a subset of the management functions that are provided by the web interface.

- Permitir visualizar e interagir com aplicativos em um sistema remoto, exibindo a imagem da tela do sistema, utilizando ferramentas de controle remoto padrão de mercado, incluindo o VNC (Virtual Network Computing), RDP (Remote Desktop) e controle remoto baseado na Web para RSA	xcc_book.pdf	61	Remote Console Functionality Use the information in this topic to understand how to remotely view and interact with the server console. You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console. You can assign a disk image (ISO or IMG file) as a virtual drive on the server. The remote console functionality is available with the XClarity Controller Advanced and XClarity Controller Enterprise features and is only available through the web interface. You must log in to the XClarity Controller with a user ID that has Supervisor access or Remote Console Access privileges to use the remote console features.
- O chip/ placa/ módulo deve ser único em cada servidor e fornecer diagnósticos, presença virtual e controle remoto para gerenciar, monitorar e resolver problemas;	xcc_book.pdf	1 61	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers. You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console.
- Segurança de acesso e utilização do protocolo TCP/IP;	xcc_book.pdf	36	SSL overview This topic is an overview of the SSL security protocol. SSL is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that prevents eavesdropping, tampering, and message forgery. You can configure the XClarity Controller to use SSL support for different types of connections, such as secure web server (HTTPS), secure LDAP connection (LDAPS), CIM over HTTPS, and SSH server, and to manage the certificates that are required for SSL.
- Ser totalmente compatível com os padrões de gerenciamento IPMI (Intelligent Platform Management Interface) 2.0;	xcc_book.pdf	2	Industry Standard Management Interfaces • IPMI 2.0 Interface • Redfish • CIM-XML • DCMI 1.5 • SNMPv3 • SNMPv1 (Traps Only) requires minimum v2.10 or v2.12 XCC Firmware updates depending on server type. See XCC Firmware update Change file for details.
- Deve permitir controle remoto tipo virtual KVM, mesmo quando o sistema operacional estiver inoperante;	xcc_book.pdf	61 61 63	You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console. The remote console is able to display only the video that is generated by the video controller on the system board. Remote console capture screen Use the information in this topic to understand how to use the remote console screen capture feature. The screen capture feature in the remote console window captures the video display contents of the server. To capture and save a screen image, complete the following steps:

- Deve informar o status do equipamento, indicando os componentes com falha e notificando o administrador via e-mail ou trap SNMP;	xcc_book.pdf	52	To add and modify email and syslog notifications or SNMP TRAP recipients, use the information in this topic.
- Suportar o envio de mensagens de Pré-Falha para no mínimo processadores, fontes, memória, ventiladores e discos;	lp1045.pdf	3	Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
- Deve permitir remotamente o acesso as mensagens do equipamento, por serial ou LAN;	xcc_book.pdf	33	Enabling or Disabling IPMI Network Access Use the information in this topic to control IPMI network access to the XClarity Controller. Click Network under BMC Configuration to view or modify XClarity Controller IPMI settings. Complete the following fields to view or modify IPMI settings: IPMI over LAN Access Click the switch to enable or disable IPMI network access to the XClarity Controller. Important: • If you are not using any tools or applications that access the XClarity Controller through the network using the IPMI protocol, it is highly recommended that you disable IPMI network access for improved security. • IPMI over LAN access to the XClarity Controller is disabled by default.

- Suporte a SSL e SSH de no mínimo 128bits;	xcc_book.pdf	3 6	Network Protocols • DHCP • DNS • DDNS • HTTP/HTTPS • SNMPv3 • SNMPv1 (Traps only) • SSL • SSH • SMTP • LDAP client • NTP • SLP • SSDP • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-SHA256
- Permitir transferir arquivos de um local para outro e sincronizar arquivos, diretórios ou unidades, utilizando uma alternativa segura para o FTP;	xcc_book.pdf	65 68	Media mount methods – SFTP – SSH File Transfer Protocol – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the checkbox. – Enter the credentials that are need to for the XClarity Controller to access the file on the remote system.

- Deve possuir tecnologia de mídia virtual, possibilitando que imagens ISSO sejam montadas remotamente ou através de compartilhamentos CIFS, NFS ou HTTPFS, permitindo inclusive a inicialização (boot) através dessas unidades;	xcc_book.pdf	65 e 66	Media mount methods – CIFS - Common Internet File System: – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the check box. – Enter the credentials that are needed for the XClarity Controller to access the file on the remote system. Note: The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space. – Mount options are optional and defined by the CIFS protocol. – If the remote server belongs to a collection of servers, where the security is centrally handled, enter the domain name to which the remote server belongs. – NFS - Network File System: – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the checkbox. – Mount options are optional and defined by the NFS protocol. Both NFSv3 and NFSv4 are supported. For example, to use NFSv3, you need to specify option 'nfsvers=3'. If the NFS server uses AUTH_ SYS security flavor to authenticate NFS operations, you need to specify option 'sec=sys'. – HTTPFS – HTTP Fuse-based File System: – Enter the URL that locates the file on the remote system – If you want the file to be presented to the server as read-only virtual media, tick the check box.
- Deve permitir o desligamento e reinicialização do servidor através da console de gerenciamento, mesmo em condições de indisponibilidade do sistema operacional, além de permitir atualização e configuração remota do BIOS e fornecer indicação de abertura de gabinete e número de série do equipamento;	xcc_book.pdf xcc_book.pdf LXPM_user_guide.pdf LXPM_user_guide.pdf	62 197 10 44	Remote power control This topic explains how to send server power and restart commands from the remote console window. You can send server power and restart commands from the remote console window without returning to the main web page. To control the server power with the remote console, click Power and select one of the following commands: Chassis Intrusion Detection You can enable this function to protect your server by detecting any physical movement of the top cover. System Summary Click the System Summary tab in the left pane to view the following system information in the right p Click the UEFI Setup tab in the left pane to enter the UEFI Setup interface. In the UEFI Setup interface, you can view and change the UEFI settings of your server.

- Possuir gestão automática de chamados ao suporte;	xcc_book.pdf	43	Lenovo is committed to security. When enabled, Call Home automatically contacts Lenovo to open a service ticket and sends in service data collected from a managed device whenever that device reports a hardware failure. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later, your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel.
- Permitir a descoberta, navegação e visualização de sistemas na rede de dados, permitindo o inventário detalhado e relacionamento com os demais recursos da rede.	lxca_users_guide.pdf	1	Lenovo XClarity Administrator is a centralized, resource-management solution that simplifies infrastructure management, speeds responses, and enhances the availability of Lenovo® server systems and solutions. It runs as a virtual appliance that automates discovery, inventory, tracking, monitoring, and provisioning for server, network, and storage hardware in a secure environment.
Documentação Técnica	N/A		
- Certificação de compatibilidade com o sistema Vmware ESXi 6.7 U2 publicada no site https://www.vmware.com/resources;	VMware Compatibility Guide - System Search.pdf	1	Model ThinkSystem SR530 CPU Series Intel Xeon Gold 6200/5200 (Cascade-LakeSP/Refresh) Series
- Certificação de compatibilidade com o sistema operacional RedHat Enterprise Linux 8.x publicada no site https://access.redhat.com/ecosystem/hardware/;	ThinkSystem SR530 (Xeon SP Gen 2) - Red Hat Certified Hardware - Red Hat Customer Portal.pdf	1	Products Level
- Certificado da serie ISO-9001 do fabricante do equipamento;	Lenovo ISO 9001.pdf	1	CERTIFICATE
- Certificado de conformidade contra incidentes elétricos e combustão dos materiais elétricos, (Norma IEC 60950) comprovador através de certificado ou relatório de avaliação de conformidade emitido por um órgão credenciado pelo INMETRO ou Certificado internacional, (Safety of Information Technology Equipment Including Eletrical Business Equipment);	lp1045.pdf	51	Regulatory compliance The ThinkSystem SR530 server conforms to the following regulations: United States: FCC Part 15, Class A; UL 60950-1 Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1 Mexico: NOM-19 Argentina: IEC60950-1 European Union: CE Mark (EN55022 Class A, IEC/EN60950-1, EN55024, EN61000-3-2, EN61000-3-3)
- Certificado quanto à emissão de radiação radiada e conduzida. Expedido por órgãos competentes comprovando que o equipamento detém da norma CISPR 22 / EN55022;	lp1045.pdf	51	Australia/New Zealand: AS/NZS CISPR 22 Class A
- A documentação solicitada juntamente com a proposta de preços, será apresentada por parte da licitante detentora do menor lance, Caso não remeta a documentação a licitante terá desclassificada a sua proposta de preços;	N/A	N/A	N/A
- Todos os periféricos, placas, controladoras, módulos de memória, disco rígido, deverão ser do mesmo fabricante, ou homologados pelo mesmo.	Conforme Proposta Comercial		
Garantia	N/A		
- O prazo de garantia padrão deverá ser, no mínimo, de 03 (três) anos acrescidos de 02 (dois) anos de garantia estendida, totalizado 05 (cinco) anos de garantia, contado do recebimento provisório. Caso o licitante não seja o próprio fabricante, deverá ser apresentada junto a proposta comercial a relação atualizada de assistência técnica autorizada do fabricante para todo o território nacional;	Conforme Proposta Comercial	N/A	N/A
- Todas as características descritas devem ser comprovadas através de catálogos, manuais, etc;	N/A	N/A	N/A

- Os produtos fornecidos estarão cobertos por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento;	N/A	N/A	N/A
- Declaração da licitante informando a rede autorizada de assistência técnica no Estado do Amazonas. Durante o período de garantia a empresa vencedora devera, sem ônus adicional, fornecer as atualizações (“patches”) corretivas do software e firmware do equipamento fornecido; A empresa vencedora prestará garantia ao sistema fornecido nas seguintes condições: fornecerá informações detalhadas sobre o suporte técnico gratuito (inclusive a ligação telefônica por meio de DDG) em português durante o período de garantia, incluindo atualização de software. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada gratuita (DDG) em horário comercial, de segunda a sexta-feira (8x5). A contratada deverá possuir central de atendimento técnico, com abertura de chamados via DDG 0800 ou portal web ou e-mail (informar os dados de contato na proposta) realizando a gestão dos processos de suporte e atendimento ‘’on-site”. O equipamento deverá possuir 5 anos de garantia “on-site” com atendimento durante horário comercial (8x5) e dias úteis com presença de técnico “on-site”; Os componentes, peças e materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento;	N/A	N/A	N/A
- Condições de Entrega: O transporte dos equipamentos até o local especificado, será realizado pela empresa vencedora (inclusive os procedimentos de seguro, embalagem e transporte até o local especificado);	N/A	N/A	N/A
- A verificação quanto ao estado dos equipamentos após o transporte será de exclusiva responsabilidade da empresa vencedora, sendo que, quaisquer danos observados no transporte, a qualquer tempo, serão reparados pela empresa vencedora;	N/A	N/A	N/A
- Condições Gerais de Fornecimento: Todos os itens de Hardware deverão ser do mesmo fabricante, mesmo que em regime OEM, neste último caso apresentar comprovação desta condição; O sistema deverá ser fornecido com todos os cabos necessários para a interconexão dos equipamentos adquiridos, além de todos os acessórios de montagem e operação; Apresentar atestado de capacidade técnica compatível com os equipamentos solicitados em quantidade similar com fornecimento e instalação; Os serviços de manutenção e suporte deverão ser prestados pelo próprio fabricante do equipamento ou através da proponente;	Conforme Proposta Comercial	N/A	N/A
- PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a “repetição” deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação;	Conforme Proposta Comercial	N/A	N/A
- Deverá informar o site onde se encontra o catálogo para confirmação das características do equipamento.	N/A	N/A	N/A

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 02 - UNIDADE DE DISCO DE 8TB SAS DE 12GB/S	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir formato de 3,5” Hot Swap SATA (HDDs);	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Ter velocidade mínima de 7.200 rpm;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Ter no mínimo interface SAS de 12 Gb/s;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Possuir no mínimo 8TB de capacidade bruta.	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 03 - UNIDADE DE DISCO DE 12TB SAS DE 12GB/S	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir formato de 3,5” Hot Swap SATA (HDDs);	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Ter velocidade mínima de 7.200 rpm;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Ter no mínimo interface SAS de 12 Gb/s;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Possuir no mínimo 12TB de capacidade bruta.	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 04 - FONTE DE ALIMENTAÇÃO (110/220) DE 750W	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir LED indicador de status e suportar uma faixa de tensão de entrada de 100 a 127 VAC e 200 a 240 VAC em 60 Hz, com chaveamento automático de voltagem;	lp1045.pdf maintenance_manual.pdf	35 21	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply The following illustration shows the LEDs on the rear view of server models with three PCIe slots. The LEDs on the rear view of server models with two PCIe slots are the same.
- Ter recurso de troca sem interrupção;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Possuir, no mínimo 750 W de potência e certificação 80+ Platinum comprovada mediante publicação no site www.plugloadsolutions.com/80pluspowersupplies.aspx.	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 05 - UNIDADE DE MEMÓRIA DE 16GB DDR4 DE 2666MHZ	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	19	ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Ser, no mínimo, memória RAM do tipo RDIMM DDR4 (Registered DIMM DDR4) com ECC (Error Checkin and Correction) ou tecnologia equivalente e que opere em frequência igual ou superior a 2666MHz.	lp1045.pdf	19	ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 06 - RACK DE TORRE FECHADO	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Largura: 600 mm;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT
- Altura: 42US;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT
- Profundidade: 1070 mm;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT
- Deve atender as especificações ANSI/EIA RS-310-E;	Rack Servidor 42U 2mm.pdf	1	Atende especificações ANSI/EIA RS-310-D, I EC 297-2, DIN 41494 partes 1 e 7;
- O equipamento deve ser totalmente desmontável para facilitar a montagem e o transporte (deverá ser entregue montado);	Rack Servidor 42U 2mm.pdf	1	Rack totalmente desmontável;
- A estrutura deve ser em aço SAE 1010/1020 # 2 mm;	Rack Servidor 42U 2mm.pdf	1	Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável;
- Deve possuir porta frontal curva em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°;	Rack Servidor 42U 2mm.pdf	1	Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável;
- Deve possuir porta traseira bipartida em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°;	Rack Servidor 42U 2mm.pdf	1	Porta traseira bipartida perfurada com índice de ventilação de 71%, em aço SAE 1010/1020 1,2 mm, reversíveis em relação ao lado de abertura da porta e intercambiáveis, possibilitando a instalação em ambas a faces do rack (traseira ou frontal), fechadura escamoteável;
- Ambas as portas devem possuir fechaduras escamoteáveis com sistema automático de destrave; - Deve ser fornecido com tampas laterais em aço SAE 1010/1020 # 1,2 mm, removíveis através de fechos rápidos, com opção para colocação de fechadura;	Rack Servidor 42U 2mm.pdf	1	• Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável; • Porta traseira bipartida perfurada com índice de ventilação de 71%, em aço SAE 1010/1020 1,2 mm, reversíveis em relação ao lado de abertura da porta e intercambiáveis, possibilitando a instalação em ambas a faces do rack (traseira ou frontal), fechadura escamoteável;
- O teto deve estar preparado para instalação de kit de ventiladores, tipo bandeja;	Rack Servidor 42U 2mm.pdf	1	Laterais em aço 1,2 mm, removíveis, com fecho rápido (Opcional fechadura do tipo cilíndrico);
- Deve possuir planos de montagem frontal e traseiro, galvanizados, anti-estáticos e numerados de 1 a 44 US;	Rack Servidor 42U 2mm.pdf	2	Teto em aço SAE 1010/1020 # 1,2 mm, com perfuração tipo colmeia, preparado para instalação de unidade de ventilação;
- Deve possuir2 guias de cabos verticais em aço SAE 1010/1020 # 1,0 mm, com anéis internos em termoplástico de alto impacto, nas dimensões de 44U x 95 mm x 70 mm (A x L x P), sendo fixadas na parte frontal do Rack;	Rack Servidor 42U 2mm.pdf	2	Planos em aço SAE 1010/1020 # 2 mm, galvanizados e anti-estáticos;
- O teto e a base do Rack deve ter abertura para entrada e saída de cabos, e tampas removíveis;	CatlogoIPMetal.pdf	10	GUIA VERTICAL 44U X 90 X 70 MM
- A estrutura do Rack deve possuir terminais de aterramento;	Rack Servidor 42U 2mm.pdf	1	Entrada e saída de cabos pelo teto ou pela base com tampa modular fechada com parafusos, para que quando não utilizada, não haja ingresso de objetos indesejados no interior do rack;
- Deve ser fornecido com pés niveladores e rodízios, sendo 2 com travas e 2 sem travas;	Rack Servidor 42U 2mm.pdf	1	Fornecido com terminais de aterramento;
- Deve suportar uma carga estática até 800 kg;	Rack Servidor 42U 2mm.pdf	1	• Base em aço SAE 1010/1020 # 1,2 mm, preparada para a instalação de rodízios e pés niveladores simultâneos;
- O Rack deve possuir pintura micro epóxi na cor preta;	Rack Servidor 42U 2mm.pdf	1	Suporte de carga estática para até 800 kg;
- Deverá vir acompanhado:	Rack Servidor 42U 2mm.pdf	1	Pintura pó em micro epóxi na cor preta RAL 9004;
- Duas Réguas de tomadas 19” de 12 posições 20ª;	Conforme Proposta Comercial	N/A	N/A
- Uma Bandeja Fixa, Instalada e Fixada nos Trilhos Frontais e Traseiros do	Conforme Proposta Comercial	N/A	N/A
- Rack;	Conforme Proposta Comercial	N/A	N/A

- Um kit de Ventilação contendo 2 Ventiladores Exaustores com 1U de tamanho	Conforme Proposta Comercial	N/A	N/A
- 127/220v, instalado e Fixando no Rack na Parte Superior;	Conforme Proposta Comercial	N/A	N/A
- Três Patch Pannel 1U, com 24 portas com conectores fêmea RJ45 CAT 5e;	Conforme Proposta Comercial	N/A	N/A
- Três guia de cabos;	Conforme Proposta Comercial	N/A	N/A
- Garantia mínima de 12 meses.	Conforme Proposta Comercial	N/A	N/A
	Conforme Proposta Comercial	N/A	N/A

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 07 - RACK TELECOM DE PAREDE	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Rack de parede 19” x 12U;	Rack Parede 12U 600mm.pdf	1	Altura de 12U – 634 mm;
- 600mm de largura e profundidade de 600mm (mínimo)	Rack Parede 12U 600mm.pdf	1	
- Atender especificações ANSI/EIA RS-310-D, IEC 297-2;	Rack Parede 12U 600mm.pdf	1	Atende especificações ANSI/EIA RS 310-D, IEC 297-2, DIN 41494 partes 1 e 7;
- Porta frontal reversível em vidro temperado, com fechadura tipo cilindro;	Rack Parede 12U 600mm.pdf	1	Porta frontal reversível, com moldura em aço 0,9 mm de espessura, com visor de vidro temperado 4 mm, com ângulo de abertura de 180°, fechadura tipo cilindro com fechadura simples;
- Confeccionado em aço SAE 1020;	Rack Parede 12U 600mm.pdf	1	Fabricado em aço SAE 1020;
- Estrutura em aço 1.5 mm;	Rack Parede 12U 600mm.pdf	1	Estrutura em aço 1,5 mm de espessura, com terminais de aterramento;
- Capacidade de carga estática de 60kg;	Rack Parede 12U 600mm.pdf	1	Capacidade de carga estática até 60 kg;
- Laterais com fecho rápido com a opção de utilização de chaves nas laterais;	Rack Parede 12U 600mm.pdf	1	Laterais removíveis, com fecho rápido;
- Entrada e saída de cabos pelo teto ou pela base do rack com acabamento de proteção;	Rack Parede 12U 600mm.pdf	1	Entrada e saída de cabos pelo teto, com furações oblongadas;
- Teto com preparação para instalação de ventiladores;	Rack Parede 12U 600mm.pdf	1	Teto preparado para instalação de ventiladores;
- Terminal de aterramento;	Rack Parede 12U 600mm.pdf	1	Estrutura em aço 1,5 mm de espessura, com terminais de aterramento;
- Deverá vir acompanhado:	N/A	N/A	N/A
- Régua de tomadas 19” de 6 posições 20A;	Conforme Proposta Comercial	N/A	N/A
- Um Patch Pannel 1U, com 24 portas com conectores fêmea RJ45 CAT 5e;	Conforme Proposta Comercial	N/A	N/A
- Um guia de cabos;	Conforme Proposta Comercial	N/A	N/A
- Dezesseis conjuntos de Porca-Gaiola para fixação de Acessórios e Ativos.	Conforme Proposta Comercial	N/A	N/A
- Garantia mínima de 12 meses.	Conforme Proposta Comercial	N/A	N/A

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 08 - PONTO DE ACESSO WI-FI COM PoE	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Equipamento de ponto de acesso para WLAN, de uso interno (indoor), atendendo aos padrões IEEE 802.11b, IEEE 802.11g, 802.11n, 802.11ac com configuração via software.	UniFi_AC_APs_DS.pdf	10	Wi-Fi Standards 802.11 a/b/g/n/r/k/v/ac
- Deve possuir pelo menos dois rádios, permitindo simultaneamente, usuários configurados nos padrões IEEE 802.11b/g/n, na faixa de frequência de 2.4GHz e 802.11n/ac, na faixa de frequência de 5GHz.	UniFi_AP-AC-Pro_QSG.pdf	26	2G Data Rate Control Select this option to determine what bit rates your 2 4 GHz network will allow Disabling lower bit rates can improve performance for higherdensity networks but will make some older devices incompatible with your network and limit the range of your wireless network 5G Data Rate Control Select this option to determine what bit rates your network will allow Disabling lower bit rates can improve performance for higherdensity networks but will make some older devices incompatible with your network and limit the range of your wireless network
- Deve implementar funcionamento em modo de gerenciamento centralizado pela SOLUÇÃO CENTRALIZADA, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF e outras funcionalidades deSolução Centralizadaritas nesta especificação.	UniFi_AP-Pro_UG.pdf	8	The UniFi Controller software that comes with your UniFi AP-Pro has a browser-based interface for easy configuration and management.

- O ponto de acesso poderá estar diretamente ou remotamente conectado à Solução Centralizada da WLAN, inclusive via roteamento da camada de rede OSI.	UniFi_Controller_V5_UG.pdf	1	Network Topology Requirements • A DHCP-enabled network (so any device can obtain an IP address) • One of the following: • UniFi Cloud Key • A management station running the UniFi Controller software, located either on-site and connected to the same Layer-2 network, or off-site* in a cloud or NOC • For the public address system capability of the UAP-AC-EDU: A compatible Android™ or iOS device located on the same Layer-2 network as the UniFi Controller and UniFi APs
- Possibilitar alimentação elétrica local entre 100V e 230V, em corrente alternada e frequência de 60hz.	PoE_Adapters_DS.pdf	8	U-POE-af 100-240VAC @ 50/60Hz
- Permitir a alimentação elétrica via Power over Ethernet (padrões IEEE 802.3af ou 802.3at) através de uma única interface de rede.	UniFi_AC_APs_DS.pdf	10	Power Method Passive Power over Ethernet (48V), 802.3af/802.3at Supported (Supported Voltage Range: 44 to 57VDC)
- Deve ser fornecido com o adaptador que permita a alimentação via Power over Ethernet (PoE).	UniFi_AP-AC-Pro_QSG.pdf	2	Package Contents
- Implementar as seguintes taxas de transmissão e com fallback automático, valores mínimos:	UniFi_AC_APs_DS.pdf	10	Supported Data Rates (Mbps)
- 802.11b - 1, 2, 5.5, 11 Mbps	UniFi_AC_APs_DS.pdf	10	802.11b 1, 2, 5.5, 11 Mbps
- 802.11g - 6, 9, 12, 18, 24, 36, 48, 54 Mbps	UniFi_AC_APs_DS.pdf	10	802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 802.11n - 6.5 Mbps a 450 Mbps (MCS0 - MCS23, HT 20/40)	UniFi_AC_APs_DS.pdf	10	802.11n 6.5 Mbps to 450 Mbps (MCS0 - MCS23, HT 20/40)
- 802.11ac - 6.5 Mbps a 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)	UniFi_AC_APs_DS.pdf	10	802.11ac 6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)
- Implementar o protocolo de enlace CSMA/CA para acesso ao meio de transmissão.	UniFi_AC_APs_DS.pdf	10	Standard Data Rates 802.11ac 6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80) 802.11n 6.5 Mbps to 450 Mbps (MCS0 - MCS23, HT 20/40) 802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b 1, 2, 5.5, 11 Mbps

- Possuir capacidade de selecionar automaticamente o canal de transmissão.	UniFi - RF Scan Suggested Channels Feature – Ubiquiti Support and Help Center.pdf	1 e 2	The WiFi spectrum must be scanned, manually analyzed, and a channel plan created. Suggested Channels does this automatically: after an RF scan has been triggered, the best channel found will be selected and automatically set, based on how busy the channel is, the RSSI of the channel, and whether or not the same SSID is already transmitting on that channel.
- Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.	UniFi_Controller_V5_UG.pdf	135	Transmit Power By default the transmit power is set to Auto You can also manually select the following:
- Possuir suporte a pelo menos 4 SSIDs.	UniFi_AC_APs_DS.pdf	10	BSSID Up to 8 per Radio
- Implementar diferentes tipos de combinações de criptografia/autenticação por SSID.	UniFi_Controller_V5_UG.pdf	23	Create Wireless Network Click to add a wireless network Go to the Create or Edit a Wireless Network section WPA-Personal WPA or Wi-Fi Protected Access was developed as an encryption method stronger than WEP WPA-Personal requires a passphrase to connect to the wireless network
- Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras.	UniFi_AC_APs_DS.pdf	10	WMM Voice, Video, Best Effort, and Background
- Não deve haver licença restringindo o número de usuários por ponto de acesso.	UniFi_AC_APs_DS.pdf	10	Concurrent Clients 250+
- Suportar mínimo 200 clientes conectados por ponto de acesso no modo concorrente.	UniFi_AC_APs_DS.pdf	10	Concurrent Clients 250+
- Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11b/g/n/ac com ganho de pelo menos 3 dBi, com padrão de irradiação omnidirecional multi-banda dipolar, integral e dual mínimo 3X3 MIMO com diversidade espacial.	UniFi_AC_APs_DS.pdf	10	Antennas (3) Dual-Band Antennas, 2.4 GHz: 3 dBi, 5 GHz: 3 dBi
- Possuir potência máxima de transmissão de, no mínimo, 22 dBm para IEEE 802.11b/g/n/ac.	UniFi_AC_APs_DS.pdf	10	Maximum TX Power 2.4 GHz 22 dBm 5 GHz 22 dBm

- Implementar a pilha de protocolos TCP/IP.	UniFi_Controller_V5_UG.pdf	1 15	Network Topology Requirements • A DHCP-enabled network (so any device can obtain na IP address) Launch Using Cloud If cloud access is available, then you can use it to access the UniFi Controller Click the appropriate option: Launch using Cloud, Launch using hostname of your Controller, or Launch using IP of your Controller For cloud access, these are the requirements: • Ports 443 (TCP), 3478 (UDP), and 443 (UDP) must be open
- Implementar VLANs conforme padrão IEEE 802.1q.	UniFi_AC_APs_DS.pdf	10	VLAN 802.1Q
- Possuir, no mínimo, duas interfaces IEEE 802.3 10/100/1000 BaseT Ethernet, auto-sensing, autoMDI/MDX, com conectores RJ-45, para conexão à rede local fixa.	UniFi_AC_APs_DS.pdf	10	Networking Interface (2) 10/100/1000 Ethernet Ports
- Implementar o protocolo NTP ou SNTP.	UniFi - Explaining the config.properties File – Ubiquiti Support and Help Center.pdf	4	To change the default NTP server being used, config.ntp_server=0.ubnt.pool.ntp.org
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.	UniFi_AP-AC-Pro_QSG.pdf	5	Hardware Overview LED
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.	UniFi - UniFi Overview – Ubiquiti Support and Help Center.pdf	5	SNMP v1/2c/3
- Possuir suporte a MIB II, conforme RFC 1213.	UniFi - UniFi Overview – Ubiquiti Support and Help Center.pdf	5	SNMP v1/2c/3
- Implementar cliente DHCP, para configuração automática de rede.	UniFi_Controller_V5_UG.pdf	7	Network Topology Requirements • A DHCP-enabled network (for the wired Access Point to obtain an IP address as well as for the wireless Access Points after the deployment)
- Possuir LED's indicativos do estado de operação e atividade dos rádios.	UniFi_AP-AC-Pro_QSG.pdf	5	Hardware Overview LED
- Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação.	UniFi_AC_APs_DS.pdf	10	Mounting Wall/Ceiling (Kits Included)
- Implementar associação dinâmica de regras de acesso e de QoS por usuário, com base nos parâmetros da etapa de autenticação.	UniFi_AC_APs_DS.pdf	10	Advanced QoS Per-User Rate Limiting
- Possibilitar roaming layer 2 (modelo OSI) com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VOIP, streaming de vídeo, videoconferência.	UniFi - Fast Roaming – Ubiquiti Support and Help Center.pdf	1	As wireless devices improve in power and portability, exceptional on-the-go performance is expected from devices such as tablets, cell phones, and mobile VoIP.
- Implementar criptografia do tráfego local.	UniFi_AC_APs_DS.pdf	10	Wireless Security WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)

- Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.	UniFi_Controller_V5_UG.pdf	23	WPA-Personal WPA or Wi-Fi Protected Access was developed as an encryption method stronger than WEP WPA-Personal requires a passphrase to connect to the wireless network
- Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento.	Conforme Proposta Comercial	N/A	N/A
- A solução ofertada deve possuir homologação junto à ANATEL conforme a resolução nº 242, de 30 de novembro de 2000. A exigência de certificação de Produtos de Telecomunicação classificáveis nas Categorias I, II e III do art. 4o da Resolução Anatel 242/2000 é pré-requisito obrigatório para fins de comercialização e utilização no país, para atendimento ao disposto no parágrafo único do art. 20 da Resolução 242 da Anatel. Todas as certificações necessárias devem estar disponíveis publicamente nos sítio eletrônico da agência reguladora conforme endereço eletrônico http://sistemas.anatel.gov.br/sgch/	5ae31c1bbfc33.pdf	1	Modelo - Nome Comercial (s): UAP-AC-PRO (*) - (UAP-AC-PRO (*))

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 09 - BATERIA DE NOBREAK - REPOSIÇÃO	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- VRLA (Chumbo Ácida Selada Regulada por Válvula	1555958987folder-UNIPOWER_2019_web.pdf	2	A linha excede todos os requisitos da ANATEL, atestando o desempenho excepcional das baterias UNIPOWER® VRLA certificado pelo CPqD.
- Vida útil: 02 anos.	1555958987folder-UNIPOWER_2019_web.pdf	2	As baterias UNIPOWER® têm capacidade extra para suportar condições extremas de descarga em aplicações cíclicas ou em flutuação, sendo consideradas baterias de alta integridade, com vida útil projetada para mais de 10 anos, Certificado ANATEL 570.
- Tensão Nominal: 12V.	1555958987folder-UNIPOWER_2019_web.pdf	2	UP1270 E
- Capacidade C20: 7AH.	1555958987folder-UNIPOWER_2019_web.pdf	2	UP1270 E
- Terminal: tipo Faston 187 - Posição D.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Tipo Terminal Faston 187
- Temperatura: +15ºC a 50ºC.	ManualTecnicoBateriaUnipower.pdf	6	Armazenagem A bateria quando armazenada completamente descarregada por um longo período sofre o processo de “sulfatação”. Quanto mais avançado o grau de “sulfatação” da bateria menor é a capacidade de armazenar energia da bateria.Atabela abaixo mostra o tempo máximo de armazenagem em diferentes temperaturas ambientes.
- Dimensões aproximadas do produto: 15,1 x 6,5 x 10,0cm.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Comprimento Largura Altura
- Peso aproximado do produto: 1,860Kg.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Peso (kg)
- Garantia do fornecedor: 12 meses.	Conforme Proposta Comercial	N/A	N/A
- Tecnologia AGM com eletrôlito absorvido.	1555958987folder-UNIPOWER_2019_web.pdf	1	Eletrólito Absorvido em Manta de Fibra de Vidro (AGM) Baixa resistência interna e maior eficiência em altas correntes de descargas. Por que escolher as baterias VRLA UNIPOWER®? UNIPOWER®, marca comercial da UNICOBA Baterias, está presente no mercado desde 1978 e conquistou a liderança absoluta em baterias seladas VRLA com produtos de alta qualidade, tecnologia de ponta e portfólio incomparáve
- Livre de Manutenção.	Conforme Proposta Comercial	N/A	N/A
- Vaso em resina ABS especial com elevada resistência mecânica.	1555958987folder-UNIPOWER_2019_web.pdf	1	CAIXA EM ABS Mais robustez, maior proteção para os componentes internos
- Atende o guia EUROBAT.	Conforme Proposta Comercial	N/A	N/A
- São seguras para o transporte aéreo (IATA-A67).	Conforme Proposta Comercial	N/A	N/A

CERTIFICADO DE CONFORMIDADE
CERTIFICATE OF CONFORMITY

Certificado No. / *Certificate No.* **UL-BR 21.0860**

Emissão / *Date of issue* 14 de Abril de 2021 / April 14, 2021

Página / *Page* **1/6**

Certificado de conformidade válido somente acompanhado das páginas de 1 até 6

Certificate of conformity valid with pages from 1 to 6

Fornecedor / *Supplier* (100592254)	**LENOVO TECNOLOGIA (BRASIL) LTDA** ESTRADA MUNICIPAL JOSE COSTA DE MESQUITA, 200 MÓDULOS 5 A 10, CHACARA ALVORADA, INDAIATUBA - SP CEP 13337-200, BRAZIL CNPJ - 07.275.920/0001-61
Produto Certificado / *Certified Product*	**Servidor** / **Server**
Família de Produto / Product's Family	ThinkSystem
Modelo - Tipo / *Model - Type*	SR530 Machine type 7X07XXXXX, 7X08XXXXX ("X" can be any alphanumeric character or blank)
Código de barras / *Barcode*	N/A
Descrição (Nome comercial) / *Description (Brand Name)*	LENOVO
Marca Comercial / *Trademark*	LENOVO
Quantidade Importada / *Quantity Imported*	N/A
Unidade de medida / *Measurement Unit*	N/A
Lote ou No. de Série / *Lot or Serial Number*	N/A
Número e Data da Licença de Importação / *Number and Import License Date*	N/A
Normas Aplicáveis / *Applicable standards*	IEC 60950-1:2005 + A1:2009 + A2:2013; CISPR 22: 2010; CISPR 32: 2015; CISPR 24: 2010; IEC 61000-3-2:2014, IEC 61000-3-3:2013, IEC 61000-4-2: 2008; IEC 61000-4-3: 2006 + A1: 2007 + A2: 2010; IEC 61000-4-4: 2012; IEC 61000-4-5: 2014; IEC 61000-4-6: 2013; IEC 61000-4-8: 2009; IEC 61000-4-11:2004
Programa de Certificação ou Portaria / *Certification Program or Decree*	PORTARIA NO. 170/2012 / DECREE NO. 170/2012 PORTARIA NO. 407/2015 / DECREE NO. 407/2015 PORTARIA NO. 48/2017 / DECREE NO. 48/2017
Relatório de Avaliação e Ensaios / Assessment and *Test Report #*	BR2334, Vol. 1, Sec. 67
Concessão Para /*Consession for*	Ostentar o Selo de Identificação da Conformidade do Sistema Brasileiro de Avaliação da Conformidade (SBAC) sobre o(s) produto(s) relacionado(s) neste certificado. *Bearing the Conformity Identification Seal of the Brazilian System of Evaluation of Conformity (SBAC) on the product covered by this certificate.*
Revisão / *Revision date*	-
Validade / *Expire date*	13 de Abril de 2024 / April 13, 2024

Pedro Mottola
Program Owner

UL do Brasil Certificações , organismo acreditado pela Coordenação Geral de Acreditação do INMETRO – CGCRE, segundo o registro Nº OCP-0029 confirma que o produto está em conformidade com a(s) Norma(s) e programas ou Portarias acima descritas.
UL do Brasil Certificações , Certification Body accredited by Coordenação Geral de Acreditação do INMETRO - CGCRE according to the register Nr OCP-0029 confirms that the product is in compliance with the standards and certification Programs or Decrees above mentioned.

Organismo de Certificação / ***Certification Body***

UL do Brasil Certificações
Av. Engenheiro Luís Carlos Berrini, 105 – 24º Andar
São Paulo – SP – Brasil - 04571-010
T: 55.11.3049.8300 / W: brazil.ul.com

CERTIFICADO DE CONFORMIDADE
CERTIFICATE OF CONFORMITY

Certificado No. / *Certificate No.* **UL-BR 21.0860**

Emissão / *Date of issue* 14 de Abril de 2021 / April 14, 2021

Certificado de conformidade válido somente acompanhado das páginas de 1 até 6
Certificate of conformity valid with pages from 1 to 6

Solicitante / *Applicant* (100592254)
LENOVO TECNOLOGIA (BRASIL) LTDA
ESTRADA MUNICIPAL JOSE COSTA DE MESQUITA, 200
MÓDULOS 5 A 10, CHACARA ALVORADA, INDAIATUBA - SP
CEP 13337-200, BRAZIL
CNPJ - 07.275.920/0001-61

Fábrica / Factory (100592254)
LENOVO TECNOLOGIA (BRASIL) LTDA
ESTRADA MUNICIPAL JOSE COSTA DE MESQUITA, 200
MÓDULOS 5 A 10, CHACARA ALVORADA, INDAIATUBA - SP
CEP 13337-200, BRAZIL
CNPJ - 07.275.920/0001-61

POTÊNCIA SONORA (dBA) E CLASSIFICAÇÃO / *NOISE POWER AND CLASSIFICATION:* N/A

MARCAÇÃO / *MARKING:* Marca do fabricante, modelo e características elétricas.

CARACTERÍSTICAS NOMINAIS / *RATINGS:*

1) 100-127/200-240 Vac, 50/60 Hz, 6.2/3.0 A
2) 100-127/200-240 Vac, 50/60 Hz, 8.4/4.1 A
3) 200-240 Vac, 50/60 Hz, 4.0 A

Class I

LISTA DE ACESSÓRIOS / *LIST OF ACCESSORIES:* N/A

MODELO DE CERTIFICAÇÃO / *CERTIFICATION MODEL:* 5

VERSÃO DO PROJETO DO PRODUTO / *PRODUCT DESIGN VERSION:* N/A

LISTA DE COMPONENTES CRÍTICOS / *LIST OF CRITICAL COMPONENTS:*

Componente/*Component*	Fabricante/ *Manufacturer*	Tipo/Modelo *Type/Model*	Características técnicas/ *Technical data*	Norma/ *Standard*	Marca de conformidade/ *Mark(s) of conformity*
Cord set (Optional)	Interchangable	Interchangable	---	NBR 14136, NBR NM 60884-1	INMETRO
Building-in power supply unit (one or two provided)	Delta Electronics, Inc.	DPS-550AB-24XX (X = 0-9, A-Z or blank)	I/P: 100-127Vac, 50/60 Hz, 6.2 A or 200-240 Vac, 50/60 Hz, 3.0 A or 240 Vdc, 2.5 A, 5000 m, 55 ˚C. O/P: +12.2 Vdc, 45.1 A; +12.2Vaux, 3 A; Max. output power 550 W	IEC 60950-1: 2005+A1+A2, EN 60950-1: 2006+A11+A1+A12+A2, UL 60950-1	CB by TUV Rh, UL recognized
- alternate	Delta Electronics, Inc.	DPS-750AB-37XX (X = 0-9, A-Z or blank)	I/P: 200-240Vac, 50/60 Hz, 4.0 A or 240Vdc, 3.3 A, 5000 m, 55 ˚C. O/P: +12.2 Vdc, 61.5 A; +12.2Vaux, 3 A; Max. output power 750 W	IEC 60950-1: 2005+A1+A2, EN 60950-1: 2006+A11+A1+A12+A2, UL 60950-1	CB by TUV Rh, UL recognized

Organismo de Certificação / ***Certification Body***
UL do Brasil Certificações
Av. Engenheiro Luís Carlos Berrini, 105 – 24º Andar
São Paulo – SP – Brasil - 04571-010
T: 55.11.3049.8300 / W: brazil.ul.com

CERTIFICADO DE CONFORMIDADE
CERTIFICATE OF CONFORMITY

Certificado No. / *Certificate No.* **UL-BR 21.0860**

Emissão / *Date of issue* 14 de Abril de 2021 / April 14, 2021

Certificado de conformidade válido somente acompanhado das páginas de 1 até 6
Certificate of conformity valid with pages from 1 to 6

Componente/*Component*	Fabricante/ *Manufacturer*	Tipo/Modelo *Type/Model*	Características técnicas/ *Technical data*	Norma/ *Standard*	Marca de conformidade/ *Mark(s) of conformity*
- alternate	Acbel Polytech Inc.	FSF030	I/P: 100-127/200-240 Vac, 50/60 Hz, 6.2/3.0 A or 240 Vdc, 2.5 A, 5000 m, 55 ˚C. O/P: +12.2 Vdc, 45.1 A; +12.2Vaux, 3 A; Max. output power 550 W	IEC 60950-1: 2005+A1+A2, EN 60950-1: 2006+A11+A1+A12+A2, UL 60950-1	CB by TUV Rh, UL recognized
- alternate	Acbel Polytech Inc.	FSF055	I/P: 100-127/200-240 Vac, 50/60 Hz, 8.4/4.1 A or 240 Vdc, 3.5 A, 5000 m, 55 ˚C. O/P: +12.2 Vdc, 61.5 A; +12.2Vaux, 3 A; Max. output power 750 W	IEC 60950-1: 2005+A1+A2, EN 60950-1: 2006+A11+A1+A12+A2, UL 60950-1	CB by TUV Rh, UL recognized
- alternate	Acbel Polytech Inc.	FSF061	I/P: 200-240Vac, 50/60 Hz, 4.0 A or 240Vdc, 3.3 A, 5000 m, 55 ˚C. O/P: +12.2 Vdc, 61.5 A; +12.2Vaux, 3 A; Max. output power 750 W	IEC 60950-1: 2005+A1+A2, EN 60950-1: 2006+A11+A1+A12+A2, UL 60950-1	CB by TUV Rh, UL recognized
- alternate	Astec International Ltd.	700-014187-XXXX (XXXX can be blank or any alphanumeric character which have no any affection to product safety)	I/P: 100-127Vac, 50/60 Hz, 6.2 A or 200-240 Vac, 50/60 Hz, 3.0 A or 240 Vdc, 2.5 A, 5000 m, 55 °C. O/P: +12.2 Vdc, 45.1 A; +12.2Vaux, 3 A; Max. output power 550 W	IEC 60950-1: 2005+A1+A2, EN 60950-1: 2006+A11+A1+A12+A2, UL 60950-1	CB by TUV SUD, UL recognized
- alternate	Astec International Ltd.	700-014188-XXXX (XXXX can be blank or any alphanumeric character which have no any affection to product safety)	I/P: 100-127Vac, 50/60 Hz, 8.4 A or 200-240 Vac, 50/60 Hz, 4.1 A or 240 Vdc, 3.5 A, 5000 m, 55 ˚C. O/P: +12.2 Vdc, 61.5 A; +12.2Vaux, 3 A; Max. output power 750 W	IEC 60950-1: 2005+A1+A2, EN 60950-1: 2006+A11+A1+A12+A2, UL 60950-1	CB by TUV SUD, UL recognized
Hard Disk Drive (max. eight provided) (optional)	Seagate Technology LLC	2.5 Series, 3.5 Series, ST with additional suffixes, ST3 with additional suffixes, ST9 with additional suffixes	ST3 or 3.5 Series or ST with additional suffixes: 5/12, 1.5 A max. / 1.5 A max. (drives will be marked with actual current ratings); ST9 or 2.5 Series or ST with additional suffixes: +5 Vdc, 1.5 A max. (drives will be marked with actual current ratings)	IEC 60950-1: 2005+A1+A2, EN 60950-1:2006+A11+A1+A12+A2	CB by UL

Organismo de Certificação / ***Certification Body***
UL do Brasil Certificações
Av. Engenheiro Luís Carlos Berrini, 105 – 24º Andar
São Paulo – SP – Brasil - 04571-010
T: 55.11.3049.8300 / W: brazil.ul.com

CERTIFICADO DE CONFORMIDADE
CERTIFICATE OF CONFORMITY

Certificado No. / *Certificate No.* **UL-BR 21.0860**

Emissão / *Date of issue* 14 de Abril de 2021 / April 14, 2021

Certificado de conformidade válido somente acompanhado das páginas de 1 até 6
Certificate of conformity valid with pages from 1 to 6

Componente/*Component*	Fabricante/ *Manufacturer*	Tipo/Modelo *Type/Model*	Características técnicas/ *Technical data*	Norma/ *Standard*	Marca de conformidade/ *Mark(s) of conformity*
- alternate	Interchangeable	Interchangeable	5 Vdc or 12 Vdc, max. 1.5 A	IEC 60950-1: 2005+A1+A2, EN 60950-1:2006+A11+A1+A12+A2	S, VDE or other EU certification marks
Solid State Drive (max. eight provided) (optional)	Interchangeable	Interchangeable	3.3 Vdc or 5 Vdc or 12 Vdc	Applicable parts of IEC 60950-1	Tested in appliance
System fan (six provided)	Delta Electronics, Inc.	FFB0412EN-00	12 Vdc, 2.1 A, min. 22.76 CFM	EN 60950-1:2006 +A11+A1+A12+A2, UL 507	TUV Rh, UL recognized
- alternate	Asia Vital Components Co., Ltd.	DBPG0428B2UP003	12 Vdc, 1.2 A, min. 24.99 CFM	EN 60950-1:2006 +A11+A1+A12+A2, UL 507	TUV SUD, UL recognized
- alternate	Interchangeable	Interchangeable	12 Vdc, max. 2.1 A, min. 22.76 CFM	EN 60950-1:2006 +A11+A1+A12+A2	S, VDE or other EU certification marks
Polyswitch (for USB2.0 and USB3.0 ports)	Bourns, Inc.	MFMSMF250/16	16 Vdc, Ih= 2.5A, It= 5.0 A	EN 60730-1, UL 1434	TÜV Rh, UL recognized
- alternate	Littelfuse Inc.	1812L260THXXYYYYY	8 Vdc, Ih= 2.6A, It= 5.2 A	EN 60730-1, UL 1434	TÜV Rh, UL recognized
- alternate	Interchangeable	Interchangeable	8 or 16 Vdc, Ih=max. 2.6 A, It=max. 5.2 A	IEC/EN 60730-1	S, VDE or other EU certification marks
Polyswitch (for VGA port)	Bourns, Inc.	MF-MSMF160	8 Vdc, Ih = 1.6 A, It = 2.8 A	EN 60730-1, UL 1434	TÜV Rh, UL recognized
- alternate	Littelfuse Inc.	1812L150THXXYYYYY	8 Vdc, Ih= 1.5 A, It= 3.0 A	EN 60730-1, UL 1434	TÜV Rh, UL recognized
- alternate	Interchangeable	Interchangeable	8 Vdc, Ih= max. 1.6 A, It= max. 3.0 A	IEC/EN 60730-1	S, VDE or other EU certification marks
Current fuse (for HDD power board)	Littelfuse Inc.	448	125 Vac/Vdc, 8 A	Applicable parts of IEC 60950-1, UL 248	UL recognized
- alternate	Cooper Bussmann LLC	6125FFxxx-R, CB61FxA	125 Vac/Vdc, 8 A	Applicable parts of IEC 60950-1, UL 248	UL recognized
RTC battery (Lithium type)	Vic-Dawn Enterprise Co Ltd	CR2032	Max. abnormal charging current 10 mA	Applicable parts of IEC 60950-1, UL 1642	UL recognized
- alternate	Shun Wo New Power Battery Technology Ltd	CR2032	Max. abnormal charging current 10 mA	Applicable parts of IEC 60950-1, UL 1642	UL recognized

Organismo de Certificação / ***Certification Body***
UL do Brasil Certificações
Av. Engenheiro Luís Carlos Berrini, 105 – 24º Andar
São Paulo – SP – Brasil - 04571-010
T: 55.11.3049.8300 / W: brazil.ul.com

CERTIFICADO DE CONFORMIDADE
CERTIFICATE OF CONFORMITY

Certificado No. / *Certificate No.* **UL-BR 21.0860**

Emissão / *Date of issue* 14 de Abril de 2021 / April 14, 2021

Certificado de conformidade válido somente acompanhado das páginas de 1 até 6

Certificate of conformity valid with pages from 1 to 6

Componente/*Component*	Fabricante/ *Manufacturer*	Tipo/Modelo *Type/Model*	Características técnicas/ *Technical data*	Norma/ *Standard*	Marca de conformidade/ *Mark(s) of conformity*
- alternate	Wuhan Lixing (Torch) Power Source Co Ltd	CR2032	Max. abnormal charging current 10 mA	Applicable parts of IEC 60950-1, UL 1642	UL recognized
- alternate	Hitachi Maxell Ltd	CR2032	Max. abnormal charging current 10 mA	Applicable parts of IEC 60950-1, UL 1642	UL recognized
- alternate	Sony Energy Devices Corp	CR2032	Max. abnormal charging current 10 mA	Applicable parts of IEC 60950-1, UL 1642	UL recognized
- alternate	Interchangeable	CR2032	Max. abnormal charging current 10 mA	Applicable parts of IEC 60950-1, UL 1642	UL recognized
Metal enclosure	Interchangeable	Interchangeable	Metal alloy	Applicable parts of IEC 60950-1	Tested in appliance
Plastic Material List:					
Parts of front bezel	Interchangeable	Interchangeable	Min. HB	Applicable parts of IEC 60950-1, UL 94	UL recognized
Internal plastic cover under DC fans	Interchangeable	Interchangeable	Min. V-2	Applicable parts of IEC 60950-1, UL 94	UL recognized
PCB	Tripod (Wuxi) Electronic Co Ltd	2-9	V-0, 130 ˚C	Applicable parts of IEC 60950-1, UL 94, UL 796	UL recognized
- alternate	Interchangeable	Interchangeable	Min. V-1, min. 105 ˚C	Applicable parts of IEC 60950-1, UL 94, UL 796	UL recognized
I/O connectors	Interchangeable	Interchangeable	Min. V-2	Applicable parts of IEC 60950-1	Tested in appliance

Organismo de Certificação / ***Certification Body***

UL do Brasil Certificações
Av. Engenheiro Luís Carlos Berrini, 105 – 24º Andar
São Paulo – SP – Brasil - 04571-010
T: 55.11.3049.8300 / W: brazil.ul.com

CERTIFICADO DE CONFORMIDADE
CERTIFICATE OF CONFORMITY

Certificado No. / *Certificate No.* **UL-BR 21.0860**

Emissão / *Date of issue* 14 de Abril de 2021 / April 14, 2021

Certificado de conformidade válido somente acompanhado das páginas de 1 até 6
Certificate of conformity valid with pages from 1 to 6

DOCUMENTOS / *DOCUMENTS:*

Título / *Title*	**Número** / *Number*	**Revisão** / *Revision*	**Data emissão** / *Issuing Date*	**Data de Realização** / Performance *Date*
<<**Dados da Auditoria** / Audit data >> ***Supplier & Factory*** LENOVO TECNOLOGIA (BRASIL) LTDA	BR3334	0	2021-03-19	N/A
Relatório de ensaio emitido por / *Test report issued by* Intertek Testing Services Taiwan Ltd.	170400052TWN-001	0	2017-04-18	N/A
Relatório de ensaio emitido por / *Test report issued by* International Standards Laboratory	ISL-17LE334CE	0	2017-06-09	N/A
Relatório de ensaio emitido por / *Test report issued by* International Standards Laboratory	ISL-17LE334FA	0	2017-06-20	N/A

OBSERVAÇÕES / *OBSERVATIONS:*

1. **A validade deste Certificado está condicionada à realização das avaliações de manutenção e tratamento de possíveis não conformidades de acordo com as orientações da UL do Brasil Certificações e previstas nos procedimentos específicos. Para verificação da condição atualizada de regularidade deste Certificado de Conformidade deve ser consultado o banco de dados de produtos e serviços certificados do Inmetro.**
   The validation of this certificate depends on the surveillance inspections performing and Non conformity treatments, according to UL do Brasil Certificações procedures. To verify the updated condition of regularity of this Conformity Certificate shall be consulted the certified products and services Inmetro database.
2. **Este certificado aplica-se aos equipamentos (produtos) idênticos ao protótipo avaliado e certificado, manufaturados na(s) unidade (s) fabril (is) mencionada (S) acima.**
   This certificate applies to the products that are identical to the prototype investigated, certified and manufactured at the production site mentioned in this certificate.
3. **Qualquer alteração no produto, incluindo a marcação, invalidará o presente certificado, salvo se o solicitante informar por escrito à UL do Brasil Certificações sobre esta modificação, a qual procederá à avaliação e decidirá quanto à continuidade da validade do certificado.**
   Any non-authorized changes performed in the product, including marking, will invalidate this certificate. UL do Brasil Certificações must be notified about any desired change. This notification will be analyzed by UL do Brasil Certificações that will decide about certificate force.

Histórico de Revisões / *Revisiosn Description:*

14 de Abril de 2021 / April 14, 2021	Emissão inicial com recertificação do certificado UL-BR 18.0133 / *Initial Issue with renewall of certificate UL-BR 18.0133.*
A última revisão substitui e cancela as anteriores *The last review replaces and cancels the previous ones*	

Organismo de Certificação / ***Certification Body***
UL do Brasil Certificações
Av. Engenheiro Luís Carlos Berrini, 105 – 24º Andar
São Paulo – SP – Brasil - 04571-010
T: 55.11.3049.8300 / W: brazil.ul.com

SPEC® CPU2017 Integer Rate Result

Copyright 2017-2019 Standard Performance Evaluation Corporation

Lenovo Global Technology

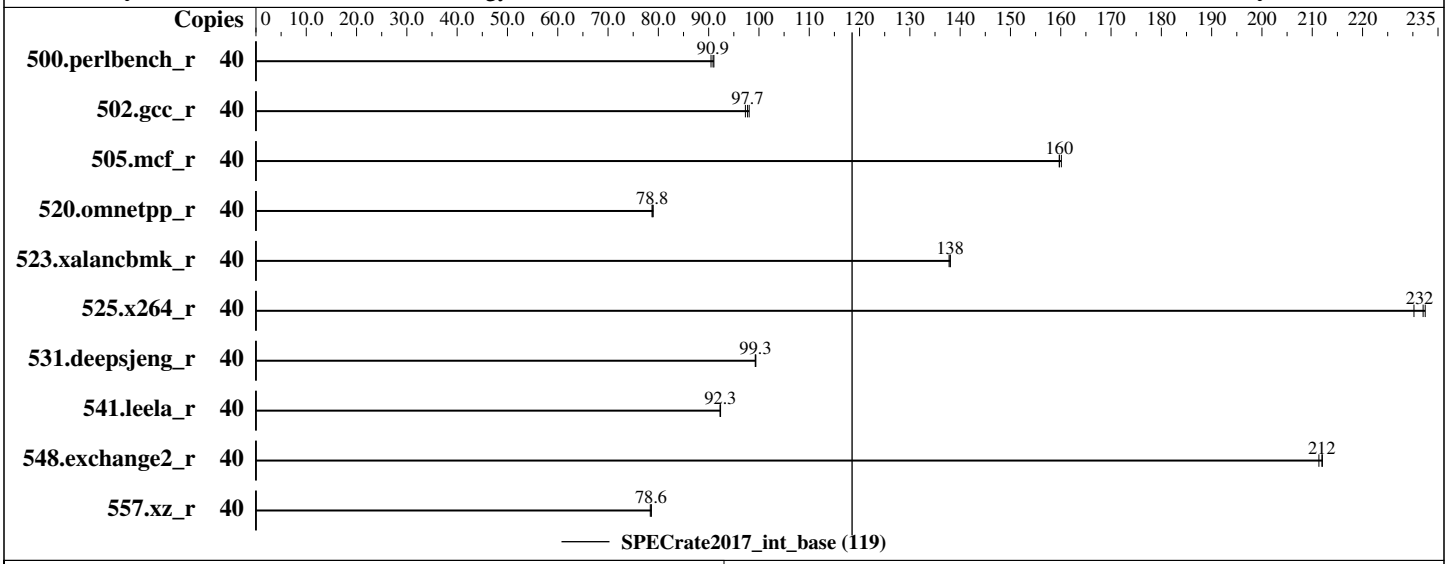
ThinkSystem SR530
(2.50 GHz, Intel Xeon Gold 5215)

SPECrate2017_int_base = 119

SPECrate2017_int_peak = Not Run

CPU2017 License: 9017
Test Sponsor: Lenovo Global Technology
Tested by: Lenovo Global Technology

Test Date: May-2019
Hardware Availability: Apr-2019
Software Availability: Dec-2018



Hardware

CPU Name:	Intel Xeon Gold 5215
Max MHz.:	3400
Nominal:	2500
Enabled:	20 cores, 2 chips, 2 threads/core
Orderable:	1,2 chips
Cache L1:	32 KB I + 32 KB D on chip per core
L2:	1 MB I+D on chip per core
L3:	13.75 MB I+D on chip per chip
Other:	None
Memory:	192 GB (12 x 16 GB 2Rx8 PC4-2933Y-R, running at 2666)
Storage:	1 x 960 GB SATA SSD
Other:	None

Software

OS:	SUSE Linux Enterprise Server 12 SP4 (x86_64) Kernel 4.12.14-94.41-default
Compiler:	C/C++: Version 19.0.1.144 of Intel C/C++ Compiler Build 20181018 for Linux; Fortran: Version 19.0.1.144 of Intel Fortran Compiler Build 20181018 for Linux
Parallel:	No
Firmware:	Lenovo BIOS Version TEE135L 2.10 released Jan-2019
File System:	xfs
System State:	Run level 3 (multi-user)
Base Pointers:	64-bit
Peak Pointers:	Not Applicable
Other:	None

Results Table

Benchmark	Base							Peak						
	Copies	Seconds	Ratio	Seconds	Ratio	Seconds	Ratio	Copies	Seconds	Ratio	Seconds	Ratio	Seconds	Ratio
500.perlbench_r	40	704	90.5	**701**	**90.9**	699	91.0							
502.gcc_r	40	582	97.3	**580**	**97.7**	578	98.1							
505.mcf_r	40	405	160	404	160	**405**	**160**							
520.omnetpp_r	40	664	79.0	**666**	**78.8**	666	78.8							
523.xalancbmk_r	40	306	138	**306**	**138**	307	138							
525.x264_r	40	304	230	**302**	**232**	301	232							
531.deepsjeng_r	40	461	99.4	**462**	**99.3**	462	99.3							
541.leela_r	40	717	92.4	718	92.3	**717**	**92.3**							
548.exchange2_r	40	496	211	494	212	**495**	**212**							
557.xz_r	40	551	78.4	**550**	**78.6**	550	78.6							

SPECrate2017_int_base = 119

SPECrate2017_int_peak = Not Run

Results appear in the order in which they were run. Bold underlined text indicates a median measurement.

Submit Notes

```
The numactl mechanism was used to bind copies to processors. The config file option 'submit'
was used to generate numactl commands to bind each copy to a specific processor.
For details, please see the config file.
```

Operating System Notes

```
Stack size set to unlimited using "ulimit -s unlimited"
```

General Notes

```
Environment variables set by runcpu before the start of the run:
LD_LIBRARY_PATH = "/home/cpu2017-1.0.5-ic19.0u1/lib/intel64"

 Binaries compiled on a system with 1x Intel Core i9-7900X CPU + 32GB RAM
 memory using Redhat Enterprise Linux 7.5
 Transparent Huge Pages enabled by default
 Prior to runcpu invocation
 Filesystem page cache synced and cleared with:
 sync; echo 3>       /proc/sys/vm/drop_caches
 runcpu command invoked through numactl i.e.:
 numactl --interleave=all runcpu <etc>
NA: The test sponsor attests, as of date of publication, that CVE-2017-5754 (Meltdown)
is mitigated in the system as tested and documented.
Yes: The test sponsor attests, as of date of publication, that CVE-2017-5753 (Spectre variant 1)
is mitigated in the system as tested and documented.
Yes: The test sponsor attests, as of date of publication, that CVE-2017-5715 (Spectre variant 2)
```

(Continued on next page)

General Notes (Continued)

```
is mitigated in the system as tested and documented.
Yes: The test sponsor attests, as of date of publication, that CVE-2018-3640 (Spectre variant 3a)
is mitigated in the system as tested and documented.
Yes: The test sponsor attests, as of date of publication, that CVE-2018-3639 (Spectre variant 4)
is mitigated in the system as tested and documented.
```

Platform Notes

```
BIOS configuration:
Choose Operating Mode set to Maximum Performance
Choose Operating Mode set to Custom Mode
Memory Power Management set to Automatic
MONITOR/MWAIT set to Enable
 Sysinfo program /home/cpu2017-1.0.5-ic19.0u1/bin/sysinfo
 Rev: r5974 of 2018-05-19 9bcde8f2999c33d61f64985e45859ea9
 running on linux-zitb Sun May  5 22:57:49 2019

 SUT (System Under Test) info as seen by some common utilities.
 For more information on this section, see
    https://www.spec.org/cpu2017/Docs/config.html#sysinfo

 From /proc/cpuinfo
    model name : Intel(R) Xeon(R) Gold 5215 CPU @ 2.50GHz
       2  "physical id"s (chips)
       40 "processors"
    cores, siblings (Caution: counting these is hw and system dependent. The following
    excerpts from /proc/cpuinfo might not be reliable.  Use with caution.)
       cpu cores : 10
       siblings  : 20
       physical 0: cores 0 1 2 3 4 8 9 10 11 12
       physical 1: cores 0 1 2 3 4 8 9 10 11 12

 From lscpu:
      Architecture:          x86_64
      CPU op-mode(s):        32-bit, 64-bit
      Byte Order:            Little Endian
      CPU(s):                40
      On-line CPU(s) list:   0-39
      Thread(s) per core:    2
      Core(s) per socket:    10
      Socket(s):             2
      NUMA node(s):          2
      Vendor ID:             GenuineIntel
      CPU family:            6
      Model:                 85
      Model name:            Intel(R) Xeon(R) Gold 5215 CPU @ 2.50GHz
```

(Continued on next page)

Platform Notes (Continued)

```
      Stepping:              6
      CPU MHz:               2500.000
      CPU max MHz:           3400.0000
      CPU min MHz:           1000.0000
      BogoMIPS:              5000.00
      Virtualization:        VT-x
      L1d cache:             32K
      L1i cache:             32K
      L2 cache:              1024K
      L3 cache:              14080K
      NUMA node0 CPU(s):     0-9,20-29
      NUMA node1 CPU(s):     10-19,30-39
      Flags:                 fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
      pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp
      lm constant_tsc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc cpuid
      aperfmperf pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 ssse3 sdbg fma cx16
      xtpr pdcm pcid dca sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave
      avx f16c rdrand lahf_lm abm 3dnowprefetch cpuid_fault epb cat_l3 cdp_l3
      invpcid_single ssbd mba ibrs ibpb stibp tpr_shadow vnmi flexpriority ept vpid
      fsgsbase tsc_adjust bmi1 hle avx2 smep bmi2 erms invpcid rtm cqm mpx rdt_a avx512f
      avx512dq rdseed adx smap clflushopt clwb intel_pt avx512cd avx512bw avx512vl
      xsaveopt xsavec xgetbv1 xsaves cqm_llc cqm_occup_llc cqm_mbm_total cqm_mbm_local
      dtherm ida arat pln pts pku ospke avx512_vnni flush_l1d arch_capabilities

/proc/cpuinfo cache data
   cache size : 14080 KB

From numactl --hardware  WARNING: a numactl 'node' might or might not correspond to a
physical chip.
  available: 2 nodes (0-1)
  node 0 cpus: 0 1 2 3 4 5 6 7 8 9 20 21 22 23 24 25 26 27 28 29
  node 0 size: 96346 MB
  node 0 free: 95722 MB
  node 1 cpus: 10 11 12 13 14 15 16 17 18 19 30 31 32 33 34 35 36 37 38 39
  node 1 size: 96712 MB
  node 1 free: 96314 MB
  node distances:
  node   0   1
    0:  10  21
    1:  21  10

From /proc/meminfo
   MemTotal:       197692248 kB
   HugePages_Total:       0
   Hugepagesize:       2048 kB

From /etc/*release* /etc/*version*
```

(Continued on next page)

Platform Notes (Continued)

```
    SuSE-release:
       SUSE Linux Enterprise Server 12 (x86_64)
       VERSION = 12
       PATCHLEVEL = 4
       # This file is deprecated and will be removed in a future service pack or release.
       # Please check /etc/os-release for details about this release.
    os-release:
       NAME="SLES"
       VERSION="12-SP4"
       VERSION_ID="12.4"
       PRETTY_NAME="SUSE Linux Enterprise Server 12 SP4"
       ID="sles"
       ANSI_COLOR="0;32"
       CPE_NAME="cpe:/o:suse:sles:12:sp4"

  uname -a:
     Linux linux-zitb 4.12.14-94.41-default #1 SMP Wed Oct 31 12:25:04 UTC 2018 (3090901)
     x86_64 x86_64 x86_64 GNU/Linux

  Kernel self-reported vulnerability status:

  CVE-2017-5754 (Meltdown):          Not affected
  CVE-2017-5753 (Spectre variant 1): Mitigation: __user pointer sanitization
  CVE-2017-5715 (Spectre variant 2): Mitigation: Indirect Branch Restricted Speculation,
  IBPB, IBRS_FW

  run-level 3 May 5 22:43

  SPEC is set to: /home/cpu2017-1.0.5-ic19.0u1
     Filesystem     Type  Size  Used Avail Use% Mounted on
     /dev/sda3      xfs   892G   50G  842G   6% /

  Additional information from dmidecode follows.  WARNING: Use caution when you interpret
  this section. The 'dmidecode' program reads system data which is "intended to allow
  hardware to be accurately determined", but the intent may not be met, as there are
  frequent changes to hardware, firmware, and the "DMTF SMBIOS" standard.
    BIOS Lenovo -[TEE135L-2.10]- 01/10/2019
    Memory:
     12x SK Hynix HMA82GR7CJR8N-WM 16 GB 2 rank 2933, configured at 2666

  (End of data from sysinfo program)
```

Compiler Version Notes

```
==============================================================================
 CC  500.perlbench_r(base) 502.gcc_r(base) 505.mcf_r(base) 525.x264_r(base)
```

(Continued on next page)

Compiler Version Notes (Continued)

```
      557.xz_r(base)
------------------------------------------------------------------------------
Intel(R) C Intel(R) 64 Compiler for applications running on Intel(R) 64,
  Version 19.0.1.144 Build 20181018
Copyright (C) 1985-2018 Intel Corporation.  All rights reserved.
------------------------------------------------------------------------------

==============================================================================
 CXXC 520.omnetpp_r(base) 523.xalancbmk_r(base) 531.deepsjeng_r(base)
      541.leela_r(base)
------------------------------------------------------------------------------
Intel(R) C++ Intel(R) 64 Compiler for applications running on Intel(R) 64,
  Version 19.0.1.144 Build 20181018
Copyright (C) 1985-2018 Intel Corporation.  All rights reserved.
------------------------------------------------------------------------------

==============================================================================
 FC  548.exchange2_r(base)
------------------------------------------------------------------------------
Intel(R) Fortran Intel(R) 64 Compiler for applications running on Intel(R)
  64, Version 19.0.1.144 Build 20181018
Copyright (C) 1985-2018 Intel Corporation.  All rights reserved.
------------------------------------------------------------------------------
```

Base Compiler Invocation

C benchmarks:
icc -m64 -std=c11

C++ benchmarks:
icpc -m64

Fortran benchmarks:
ifort -m64

Base Portability Flags

500.perlbench_r: -DSPEC_LP64 -DSPEC_LINUX_X64
502.gcc_r: -DSPEC_LP64
505.mcf_r: -DSPEC_LP64
520.omnetpp_r: -DSPEC_LP64
523.xalancbmk_r: -DSPEC_LP64 -DSPEC_LINUX
525.x264_r: -DSPEC_LP64

(Continued on next page)

Base Portability Flags (Continued)

531.deepsjeng_r: -DSPEC_LP64
541.leela_r: -DSPEC_LP64
548.exchange2_r: -DSPEC_LP64
557.xz_r: -DSPEC_LP64

Base Optimization Flags

C benchmarks:
-Wl,-z,muldefs -xCORE-AVX512 -ipo -O3 -no-prec-div
-qopt-mem-layout-trans=4
-L/usr/local/IntelCompiler19/compilers_and_libraries_2019.1.144/linux/compiler/lib/intel64
-lqkmalloc

C++ benchmarks:
-Wl,-z,muldefs -xCORE-AVX512 -ipo -O3 -no-prec-div
-qopt-mem-layout-trans=4
-L/usr/local/IntelCompiler19/compilers_and_libraries_2019.1.144/linux/compiler/lib/intel64
-lqkmalloc

Fortran benchmarks:
-Wl,-z,muldefs -xCORE-AVX512 -ipo -O3 -no-prec-div
-qopt-mem-layout-trans=4 -nostandard-realloc-lhs -align array32byte
-L/usr/local/IntelCompiler19/compilers_and_libraries_2019.1.144/linux/compiler/lib/intel64
-lqkmalloc

The flags files that were used to format this result can be browsed at
http://www.spec.org/cpu2017/flags/Intel-ic18.0-official-linux64.2019-04-02.html
http://www.spec.org/cpu2017/flags/Lenovo-Platform-SPECcpu2017-Flags-V1.2-CLX-A.html

You can also download the XML flags sources by saving the following links:
http://www.spec.org/cpu2017/flags/Intel-ic18.0-official-linux64.2019-04-02.xml
http://www.spec.org/cpu2017/flags/Lenovo-Platform-SPECcpu2017-Flags-V1.2-CLX-A.xml

SPEC is a registered trademark of the Standard Performance Evaluation Corporation. All other brand and product names appearing in this result are trademarks or registered trademarks of their respective holders.

For questions about this result, please contact the tester. For other inquiries, please contact info@spec.org.

Tested with SPEC CPU2017 v1.0.5 on 2019-05-05 10:57:48-0400.
Report generated on 2019-05-29 16:46:54 by CPU2017 PDF formatter v6067.
Originally published on 2019-05-29.

CERTIFICATE

Certificate Number: 111969.00
With One Page Addendum

The Quality Management System and implementation of:

Lenovo Group, LTD

With Headquarters at:
8001 Development Drive
Morrisville, NC 27560
United States

meets the requirements of the standard:

ISO 9001:2015

Scope of Certification:

Design, development, manufacturing, distribution, fulfillment, services, marketing, and sales of computer products and devices, data center products, mobile devices, smart devices, and accessories.

Certificate Expires:	June 30, 2022
Certificate Issued:	July 1, 2019
Certified Since:	July 1, 2016

Dr. Cem O. Onus
Managing Director, Business Assurance
DEKRA Certification, Inc.
1120 Welsh Road, Suite 210
North Wales, PA 19454 USA
(215) 997-4519
dekra-certification.us

ADDENDUM

Certificate Number: 111969.00
Addendum Page One of One

Standard: ISO 9001:2015

The Quality Management System and implementation of:

Lenovo Group, LTD

Site Address	Scope Per Site:
HQ: 8001 Development Drive; Morrisville, NC 27560 USA	*Responsibility of the company's overall QMS through the management of documentation/changes, management review, corrective actions, internal audit, planning/evaluation and compliance to applicable requirements.*
8001 Development Drive; Morrisville, NC 27560 USA	*Design, development, fulfillment, services, marketing, and sales of computer products and devices, data center products, mobile devices, smart devices, and accessories.*
19/1A, & 2A Edayar, Cuddalore Main Road, Edayar Palayam Village – Pondicherry, India	*Manufacturing of computer products and devices.*
Apodaca (Monterrey), Mexico; Boulevard Escobed No 316, Apodaca Industrial Park, PO 66600	*Manufacturing of computer products and devices, and data center products.*
Estrada Municipal José Costa de Mesquita, 200 – Chácara Alvorada – Indaiatuba/SP, Brazil	*Manufacturing of computer products and devices, and data center products.*
6540 Franz Warner Parkway; Whitsett, NC 27377 USA	*Manufacturing, distribution, fulfillment and services of computer products and devices, data center products, mobile devices, smart devices, and accessories.*
Digital Park, Einsteinova 851 01; Bratislava, Slovakia	*Fulfillment, services, marketing, and sales of computer products and devices, data center products, mobile devices, smart devices, and accessories.*
Minatomiral Center Building; 2F 3-6-1; Minatomiral, Nishi-Ku; Yokohama, Japan	*Design and development of computer products and devices.*

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

管理体系认证证书

证书编号：01116Q30209R3L(F1)
OID 编号：1.2.156.1.2.01116Q30209R3L(F1)

兹 证 明

联想(北京)有限公司

（社会信用代码：91110108700000458B）

（北京市海淀区上地信息产业基地创业路 6 号，100085）

质量管理体系符合标准：

GB/T 19001-2016/ISO9001:2015《质量管理体系 要求》

本 证 书 覆 盖 下 述 范 围：

台式电脑、显示器、笔记本电脑、服务器及存储系列产品、打印机、移动存储、多媒体数码产品 PC 周边设备系列产品、移动用户终端、便携式计算机、智能电视接收机的设计、开发、生产和服务；服务器系统软件的设计、开发、生产、服务

该 认 证 范 围 覆 盖 场 所 见：

见质量认证证书附件

（本证书有效性依据发证机构的定期监督获得保持，证书有效性信息请登录 www.cc.cesi.cn 进行查询）
（本证书信息可在国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 上查询）
注：认证注册范围不包括未获得有效的国家规定的相关行政许可，资质许可的产品服务范围

总 经 理

发证日期：2016 年 11 月 17 日
换证日期：2017 年 12 月 1 日
有效期至：2019 年 11 月 16 日

北京赛西认证有限责任公司

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C011-M

地址：北京市东城区安定门东大街 1 号　　客服电话：400-071-9000　　网址：www.cc.cesi.cn

CERTIFICATE OF MANAGEMENT SYSTEM CERTIFICATION

Certificate No: 01116Q30209R3L(F1)
OID No: 1.2.156.1.2.01116Q30209R3L(F1)

This is to certify that the Quality Management Systems of

LENOVO (BEIJING) CO., LTD.

(Certificate of Social Credit Code : 91110108700000458B)
(NO.6 CHUANGYE ROAD, SHANGDI INFORMATION INDUSTRY BASE, HAIDIAN DISTRICT, BEIJING, CHINA, 100085)

has complied with the requirements of

GB/T 19001-2016/ISO9001:2015

Quality management systems-Requirements

This certificate is valid for the following scope:

THE DESIGN, DEVELOPMENT, MANUFACTURING AND SERVICE OF DESKTOP, MONITOR, NOTEBOOK, SERVER AND STORAGE PRODUCT SERIES, PRINTER, MOBILE STORAGE, MULTIMEADIA DIGITAL PRODUCT, PC OPTIONS, MOBILE TERMINAL DEVICE, PORTABLE PC, SMART TV RECEIVERS, AND SYSTEM SOFTWARES OF SERVER

THE LOCATION COVERED BY THE CERTIFICATION IS:
SEE THE ATTACHMENT OF QUALITY MANAGEMENT SYSTEM CERTIFICATE

THE VALIDITY OF THIS CERTIFICATE DEPENDS ON THE CONSEQUENCE OF THE ANNUALLY SURVEILLANCE EXECUTED BY THE CERTIFICATION BODY
PLEASE ACCESS www.cc.cesi.cn OR www.cnca.gov.cn FOR CHECKING VALIDITY OF THE CERTIFICATE
Note: The scope of product services without the related administrative permits and qualifications is not included in the scope of certification registration.

General Manager

Issue Date:2016-11-17
Exchange Date:2017-12-01
Valid Until:2019-11-16

CESI Certification Co., Ltd.

MEMBER OF MULTILATERAL RECOGNITION ARRAN GEMENT IAF

CNAS

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C011-M

Add: No.1Andingmen Dongdajie Dongchengqu,Beijing,China Tel: 400-071-9000 Http://www.cc.cesi.cn

发证日期：2016 年 11 月 17 日
Issue Date:2016-11-17
换证日期：2017 年 12 月 1 日
Exchange Date:2017-12-01
有效期至：2019 年 11 月 16 日
Valid Until:2019-11-16

质量认证证书附件

QUALITY MANAGEMENT SYSTEMS CERTIFICATE APPENDIX

证书编号：**01116Q30209R3L(F1)**
Certificate No：**01116Q30209R3L(F1)**
OID 编号：**1.2.156.1.2. 01116Q30209R3L(F1)**
OID No：**1.2.156.1.2. 01116Q30209R3L(F1)**

名称：联想(北京)有限公司
Name of Body: LENOVO (BEIJING) CO., LTD.

认证范围覆盖场所：

1. 北京市海淀区上地信息产业基地创业路 6 号
2. 北京市海淀区上地信息产业基地创业路 8 号 2 号楼
3. 北京市海淀区上地西路 6 号
4. 上海市浦东新区松涛路 696 号
5. 中国（上海）自由贸易试验区芬菊路 199 号 68 号厂房
6. 上海市浦东新区上丰路 955 号 2# 厂房
7. 上海市张江科技园区春晓路 289 号张江大厦 7A,9A,10A,11A 层
8. 广东省惠州市惠阳经济开发区联想科技园 E 栋
9. 四川省成都市高新区西区天健路 88 号 B1,B2 生产厂房和办公楼
10. 辽宁省大连市沙河口五一路 267 号大连软件园 17 号楼 4 层 401B
11. 广东省深圳市南山区高新技术产业园区南一道 16 号联想研发大厦 4-11 层
12. 广东省深圳市福田区福田保税区桃花路 30 号
13. 福建省厦门市火炬高新区信息光电园岐山北二路 999 号
14. 湖北省武汉市东湖新技术开发区高新四路 19 号

THE LOCATION COVERED BY THE CERTIFICATION IS:

1. NO. 6 CHUANGYE ROAD, SHANGDI INFORMATION INDUSTRY BASE, HAIDIAN DISTRICT, BEIJING, CHINA
2. NO. 2 BUILDING, NO. 8 CHUANGYE ROAD, SHANGDI INFORMATION INDUSTRY BASE, HAIDIAN DISTRICT, BEIJING, CHINA
3. NO. 6 SHANGDI WEST ROAD, HAIDIAN DISTRICT, BEIJING, CHINA
4. NO. 696 SONGTAO ROAD, PUDONG NEW DISTRICT, SHANGHAI, CHINA
5. NO. 68 BUILDING 199 FENJU ROAD FREE-TRADE-ZONE SHANGHAI, CHINA
6. NO. 2 BUILDING, NO. 955 SHANGFENG ROAD, PUDONG NEW DISTRICT, SHANGHAI, CHINA
7. 7A, 9A, 10A, 11A, ZHANGJIANG BUILDING, NO. 289 CHUNXIAO ROAD, ZHANGJIANG TECHNOLOGY ZONE, SHANGHAI, CHINA
8. E BUILDING, LENOVO SCIENCE&TECHNOLOGY PARK, HUIYANG ECONOMIC DEVELOPMENT ZONE, HUIZHOU, GUANGDONG, CHINA
9. NO. B1, B2 AND OFFICE BUILDING, NO. 88 TIANJIAN ROAD WEST GAOXIN DISTRICT CHENGDU, SICHUAN, CHINA.
10. 401B LENOVO, NO. 17 BUILDING, DALIAN SOFTWARE PARK, NO. 267 WUYI ROAD, SHAHEKOU DISTRICT, DALIAN CITY, LIAONING, CHINA.
11. 4-11F LENOVO R&D CENTRE, NO. 16 NANYI ROAD, HI-TECH INDUSTRIAL PARK, NANSHAN DISTRICT, SHENZHEN, GUANGDONG, CHINA
12. NO.30 TAO HUA ROAD, FUTIAN FREE TRADE ZONE, FUTIAN DISTRICT SHENZHEN, GUANGDONG, CHINA
13. NO. 999 QISHAN NORTH 2ND ROAD, INFORMATION & OPTOELECTRONICS PARK, TORCH HI-TECH INDUSTRY DEVELOPMENT ZONE, XIAMEN, CHINA
14. NO. 19 GAOXIN 4TH ROAD, EAST LAKE HIGH-TECH ZONE, WUHAN, CHINA

管理体系认证证书

证书编号：01116Q30231R0M (F1)
OID 编号：1.2.156.1.2.01116Q30231R0M (F1)

兹 证 明

联想（北京）信息技术有限公司

（社会信用代码：91110108397173806M）

（北京市海淀区上地信息产业基地创业路 6 号 3406 房间，100085）

质量管理体系符合标准：

GB/T 19001-2016/ISO9001:2015《质量管理体系 要求》

本 证 书 覆 盖 下 述 范 围：

服务器的设计、开发、生产（外包）和服务

服务器系统软件的设计、开发和服务

该 认 证 范 围 覆 盖 场 所：

北京市海淀区上地信息产业基地创业路 6 号
上海市张江科技园区春晓路 289 号张江大厦 7A, 9A, 10A, 11A 层
台湾台北市南港区三重路 66 号 4, 5, 8 楼

（本证书有效性依据发证机构的定期监督获得保持，证书有效性信息请登录 www.cc.cesi.cn 进行查询）
（本证书信息可在国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 上查询）
注：认证注册范围不包括未获得有效的国家规定的相关行政许可，资质许可的产品服务范围

总 经 理

发证日期：2016 年 12 月 16 日
换证日期：2018 年 1 月 1 日
有效期至：2019 年 12 月 15 日

北京赛西认证有限责任公司

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C011-M

地址：北京市东城区安定门东大街 1 号　　客服电话：400-071-9000　　网址：www.cc.cesi.cn

CERTIFICATE OF MANAGEMENT SYSTEM CERTIFICATION

Certificate No: 01116Q30231R0M (F1)
OID No: 1.2.156.1.2.01116Q30231R0M (F1)

This is to certify that the Quality Management Systems of

LENOVO (BEIJING) INFORMATION TECHNOLOGY CO., LTD.

(Certificate of Social Credit Code : 91110108397173806M)
(3406 ROOM IN NO. 6 CHUANGYE ROAD, SHANGDI INFORMATION INDUSTRY BASE, HAIDIAN DISTRICT, BEIJING CHINA, 100085)

has complied with the requirements of

GB/T 19001-2016/ISO9001:2015

Quality management systems-Requirements

This certificate is valid for the following scope:

THE DESIGN, DEVELOPMENT, MANUFACTURING(OUTSOURCING) AND SERVICE OF SERVER, THE DESIGN, DEVELOPMENT AND SERVICE OF SYSTEM SOFTWARES OF SERVER

THE LOCATION COVERED BY THE CERTIFICATION IS:
NO. 6 CHUANGYE ROAD, SHANGDI INFORMATION INDUSTRY BASE, HAIDIAN DISTRICT, BEIJING CHINA
7A, 9A, 10A, 11A, ZHANGJIANG BUILDING, No. 289 CHUNXIAO ROAD, ZHANGJIANG TECHNOLOGY ZONE, SHANGHAI, CHINA
4F, 5F, 8F, No. 66 SAN CHONG ROAD, NAN GANG DISTRICT, TAIPEI CITY, TAIWAN

THE VALIDITY OF THIS CERTIFICATE DEPENDS ON THE CONSEQUENCE OF THE ANNUALLY SURVEILLANCE EXECUTED BY THE CERTIFICATION BODY
PLEASE ACCESS www.cc.cesi.cn OR www.cnca.gov.cn FOR CHECKING VALIDITY OF THE CERTIFICATE
Note: The scope of product services without the related administrative permits and qualifications is not included in the scope of certification registration.

General Manager

Issue Date:2016-12-16
Exchange Date:2018-01-01
Valid Until:2019-12-15

CESI Certification Co., Ltd.

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C011-M

Add: No.1Andingmen Dongdajie Dongchengqu,Beijing,China Tel: 400-071-9000 Http://www.cc.cesi.cn

管理体系认证证书

证书编号：01116Q30231R0M-1
OID 编号：1.2.156.1.2.01116Q30231R0M-1

兹 证 明

台湾联想环球科技股份有限公司

（台湾台北市南港区三重路 66 号 8 楼）

质量管理体系符合标准：

GB/T 19001-2016/ISO9001:2015《质量管理体系 要求》

本 证 书 覆 盖 下 述 范 围：

服务器的设计、开发和服务

该 认 证 范 围 覆 盖 场 所：

台湾台北市南港区三重路 66 号 4, 5, 8 楼

（本证书有效性依据发证机构的定期监督获得保持，证书有效性信息请登录 www.cc.cesi.cn 进行查询）
（本证书信息可在国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 上查询）
注：认证注册范围不包括未获得有效的国家规定的相关行政许可，资质许可的产品服务范围

总 经 理

发证日期：2018 年 1 月 1 日

有效期至：2019 年 12 月 15 日

北京赛西认证有限责任公司

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C011-M

地址：北京市东城区安定门东大街 1 号　　客服电话：400-071-9000　　网址：www.cc.cesi.cn

CERTIFICATE OF MANAGEMENT SYSTEM CERTIFICATION

Certificate No: 01116Q30231R0M-1
OID No: 1.2.156.1.2.01116Q30231R0M-1

This is to certify that the Quality Management Systems of

LENOVO GLOBAL TECHNOLOGY (TAIWAN) LTD.
(8F, No. 66 SAN CHONG ROAD, NAN GANG DISTRICT, TAIPEI CITY, TAIWAN)

has complied with the requirements of

GB/T 19001-2016/ISO9001:2015

Quality management systems-Requirements

This certificate is valid for the following scope:

THE DESIGN, DEVELOPMENT AND SERVICE OF SERVER

THE LOCATION COVERED BY THE CERTIFICATION IS:
4F, 5F, 8F, No. 66 SAN CHONG ROAD, NAN GANG DISTRICT, TAIPEI CITY, TAIWAN

THE VALIDITY OF THIS CERTIFICATE DEPENDS ON THE CONSEQUENCE OF THE ANNUALLY SURVEILLANCE EXECUTED BY THE CERTIFICATION BODY
PLEASE ACCESS www.cc.cesi.cn OR www.cnca.gov.cn FOR CHECKING VALIDITY OF THE CERTIFICATE
Note: The scope of product services without the related administrative permits and qualifications is not included in the scope of certification registration.

General Manager

Issue Date:2018-01-01

Valid Until:2019-12-15

CESI Certification Co., Ltd.

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C011-M

Add: No.1Andingmen Dongdajie Dongchengqu,Beijing,China Tel: 400-071-9000 Http://www.cc.cesi.cn

CERTIFICATE

Certificate Number: 111969.00
With One Page Addendum

The Quality Management System and implementation of:

Lenovo Group, LTD

With Headquarters at:
8001 Development Drive
Morrisville, NC 27560
United States

meets the requirements of the standard:

ISO 9001:2015

Scope of Certification:

Design, development, manufacturing, distribution, fulfillment, services, marketing, and sales of computer products and devices, data center products, mobile devices, smart devices, and accessories.

Certificate Expires:	June 30, 2022
Certificate Issued:	July 1, 2019
Certified Since:	July 1, 2016

Dr. Cem O. Onus
Managing Director, Business Assurance
DEKRA Certification, Inc.
1120 Welsh Road, Suite 210
North Wales, PA 19454 USA
(215) 997-4519
dekra-certification.us

ADDENDUM

Certificate Number: 111969.00
Addendum Page One of One

Standard: ISO 9001:2015

The Quality Management System and implementation of:

Lenovo Group, LTD

Site Address	Scope Per Site:
HQ: 8001 Development Drive; Morrisville, NC 27560 USA	*Responsibility of the company's overall QMS through the management of documentation/changes, management review, corrective actions, internal audit, planning/evaluation and compliance to applicable requirements.*
8001 Development Drive; Morrisville, NC 27560 USA	*Design, development, fulfillment, services, marketing, and sales of computer products and devices, data center products, mobile devices, smart devices, and accessories.*
19/1A, & 2A Edayar, Cuddalore Main Road, Edayar Palayam Village – Pondicherry, India	*Manufacturing of computer products and devices.*
Apodaca (Monterrey), Mexico; Boulevard Escobed No 316, Apodaca Industrial Park, PO 66600	*Manufacturing of computer products and devices, and data center products.*
Estrada Municipal José Costa de Mesquita, 200 – Chácara Alvorada – Indaiatuba/SP, Brazil	*Manufacturing of computer products and devices, and data center products.*
6540 Franz Warner Parkway; Whitsett, NC 27377 USA	*Manufacturing, distribution, fulfillment and services of computer products and devices, data center products, mobile devices, smart devices, and accessories.*
Digital Park, Einsteinova 851 01; Bratislava, Slovakia	*Fulfillment, services, marketing, and sales of computer products and devices, data center products, mobile devices, smart devices, and accessories.*
Minatomiral Center Building; 2F 3-6-1; Minatomiral, Nishi-Ku; Yokohama, Japan	*Design and development of computer products and devices.*

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

Intel X722 Integrated 10 GbE Controller for Lenovo ThinkSystem

Product Guide

The Intel Ethernet Connection X722 is a network controller embedded into the Intel C624 "Lewisburg" PCH chipset of Lenovo ThinkSystem servers. The controller connects to available 10 GbE and 1 Gigabit Ethernet LAN-on-motherboard (LOM) adapter cards and onboard connectors to provide a comprehensive 1 GbE / 10 GbE networking solution for ThinkSystem customers.

ThinkSystem servers support either 10 Gb Ethernet copper or optical connections, or Gigabit Ethernet connections depending on the server model.

The following figure shows the ThinkSystem 10Gb 4-port SFP+ LOM adapter which provides four SFP+ cages for optical or direct-attach copper (DAC) connectivity.



Figure 1. ThinkSystem 10Gb 4-port SFP+ LOM adapter (Port 1 at the top)

Did you know?

The Intel Ethernet Connection X722 shares the same driver package as the Intel X710 adapters making driver management easier for existing customers.

ThinkSystem LOM adapters are cost-effective adapters that take advantage of the X722 controller embedded in Intel Xeon Processor Scalable Family chipset and offer the flexibility advantages of a PCIe adapter while supporting integrated networking features, such as Wake-on-LAN and direct connectivity to the XClarity Controller management processor for NC-SI-compliant systems management.

Part number information

The following table provides the ordering part numbers and feature codes for the ThinkSystem LOM adapters.

Table 1. Supported LOM adapters

Part number	Feature code	Description	Ports
Gigabit Ethernet			
7ZT7A00544	AUKG	ThinkSystem 1Gb 2-port RJ45 LOM	2x RJ45
7ZT7A00545	AUKH	ThinkSystem 1Gb 4-port RJ45 LOM	4x RJ45
10 Gb Ethernet			
7ZT7A00546	AUKJ	ThinkSystem 10Gb 2-port SFP+ LOM	2x SFP+
7ZT7A00547	AUKK	ThinkSystem 10Gb 4-port SFP+ LOM	4x SFP+
7ZT7A00548	AUKL	ThinkSystem 10Gb 2-port Base-T LOM	2x RJ45 (10GBASE-T)
7ZT7A00549	AUKM	ThinkSystem 10Gb 4-port Base-T LOM	4x RJ45 (10GBASE-T)
EIOM modules for D2 Enclosure for use with SD530 servers			
7M17A04001	AUYA	ThinkSystem D2 10Gb 8-port Base-T (RJ45)	8x RJ45
7M17A04000	AUY9	ThinkSystem D2 10Gb 8-port SFP+	8x SFP+

Note: The SFP+ LOM adapters ship without any SFP+ transceivers or direct attach cables. These items must be ordered separately as described in the following section.

The following figure shows the ThinkSystem 10Gb 4-port Base-T LOM adapter which provides four RJ45 10GBASE-T ports.

Tip: Ports are numbered sequentially starting with Port 1 at the top of the adapter (furthest away from the edge connector)

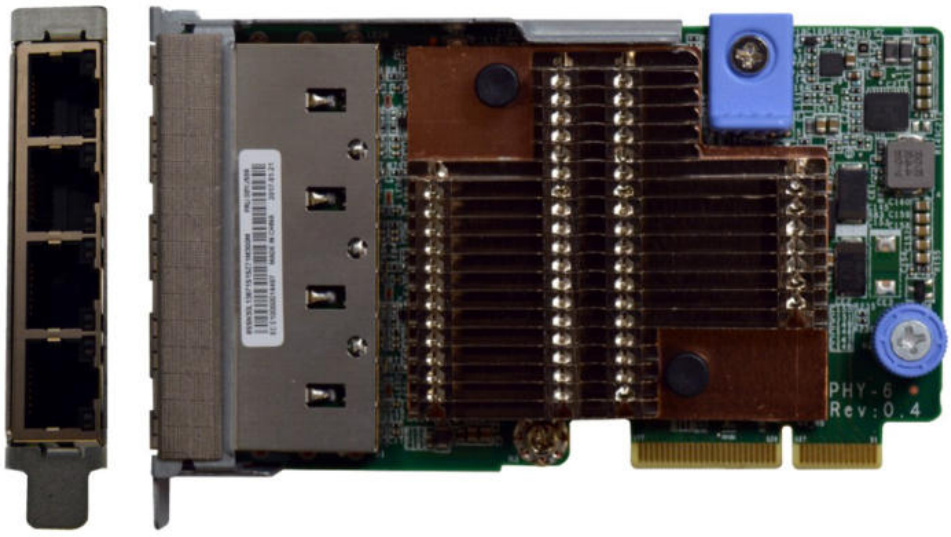


Figure 2. ThinkSystem 10Gb 4-port Base-T LOM

Supported transceivers and cables

The 2-port and 4-port SFP+ LOM adapters have empty SFP+ cages that support SFP+ SR and LR transceivers as listed in the following table.

Table 2. Supported SFP+ transceivers - 2-port and 4-port SFP+ LOM adapters

Part number	Feature code	Description
49Y4216	0069	Brocade 10Gb SFP+ SR Optical Transceiver
46C3447	5053	SFP+ SR Transceiver (10Gb)
90Y9412	A1PM	SFP+ LR Transceiver
00FE331	B0RJ	10GBASE-LR SFP+Transceiver

The ThinkSystem D2 10Gb 8-port SFP+ module, 7M17A04000, supports SFP+ SR and LR transceivers as listed in the following table.

Table 3. Supported SFP+ transceivers - D2 10Gb 8-port SFP+ EIOM module

Part number	Feature code	Description
46C3447	5053	SFP+ SR Transceiver (10Gb)
90Y9412	A1PM	SFP+ LR Transceiver

The following table lists the fiber optic cables and Active Optical Cables supported by the SFP+ adapters.

Table 4. Optical cables

Part number	Feature code	Description
LC-LC OM3 Fiber Optic Cables (requires transceivers)		
00MN499	ASR5	Lenovo 0.5m LC-LC OM3 MMF Cable
00MN502	ASR6	Lenovo 1m LC-LC OM3 MMF Cable
00MN505	ASR7	Lenovo 3m LC-LC OM3 MMF Cable
00MN508	ASR8	Lenovo 5m LC-LC OM3 MMF Cable
00MN511	ASR9	Lenovo 10m LC-LC OM3 MMF Cable
00MN514	ASRA	Lenovo 15m LC-LC OM3 MMF Cable
00MN517	ASRB	Lenovo 25m LC-LC OM3 MMF Cable
00MN520	ASRC	Lenovo 30m LC-LC OM3 MMF Cable
SFP+ 10Gb Active Optical Cables		
00YL634	ATYX	Lenovo 1M SFP+ to SFP+ Active Optical Cable
00YL637	ATYY	Lenovo 3M SFP+ to SFP+ Active Optical Cable
00YL640	ATYZ	Lenovo 5M SFP+ to SFP+ Active Optical Cable
00YL643	ATZ0	Lenovo 7M SFP+ to SFP+ Active Optical Cable
00YL646	ATZ1	Lenovo 15M SFP+ to SFP+ Active Optical Cable
00YL649	ATZ2	Lenovo 20M SFP+ to SFP+ Active Optical Cable

The following table lists the direct-attach copper (DAC) cables supported by the SFP+ adapters.

Table 5. Copper cables

Part number	Feature code	Description
SFP+ Passive DAC Cables		
00D6288	A3RG	0.5m Passive DAC SFP+ Cable
90Y9427	A1PH	1m Passive DAC SFP+ Cable
00AY764	A51N	1.5m Passive DAC SFP+ Cable
00AY765	A51P	2m Passive DAC SFP+ Cable
90Y9430	A1PJ	3m Passive DAC SFP+ Cable
90Y9433	A1PK	5m Passive DAC SFP+ Cable
SFP+ Active DAC Cables		
00VX111	AT2R	Lenovo 1m Active DAC SFP+ Cables
00VX114	AT2S	Lenovo 3m Active DAC SFP+ Cables
00VX117	AT2T	Lenovo 5m Active DAC SFP+ Cables
SFP28 25Gb Passive DAC Cables		
7Z57A03557	AV1W	Lenovo 1m Passive 25G SFP28 DAC Cable
7Z57A03558	AV1X	Lenovo 3m Passive 25G SFP28 DAC Cable
7Z57A03559	AV1Y	Lenovo 5m Passive 25G SFP28 DAC Cable

The following table lists the Category 6 (CAT 6) cables supported by the 1Gb and 10Gb RJ45 adapters.

Table 6. CAT6 cables

Part number	Feature code	Description
CAT6 Green Cables		
00WE123	AVFW	0.75m CAT6 Green Cable
00WE127	AVFX	1.0m CAT6 Green Cable
00WE131	AVFY	1.25m CAT6 Green Cable
00WE135	AVFZ	1.5m CAT6 Green Cable
00WE139	AVG0	3m CAT6 Green Cable
90Y3718	A1MT	10m CAT6 Green Cable
90Y3727	A1MW	25m CAT6 Green Cable
CAT6 Blue Cables		
90Y3721	A1MU	10m CAT6 Blue Cable
90Y3730	A1MX	25m CAT6 Blue Cable
CAT6 Yellow Cables		
90Y3724	A1MV	25m CAT6 Yellow Cable

The following table lists the supported Category 5e (CAT 5e) cables supported by the 1Gb RJ45 adapters

Table 7. CAT5e cables

Part number	Feature code	Description
CAT5e Blue Cables		
40K5679	3801	0.6m Blue Cat5e Cable
00WE111	AVFT	0.75m Blue Cat5e Cable
00WE115	AVFU	1.0m Blue Cat5e Cable
00WE119	AVFV	1.25m Blue Cat5e Cable
40K8785	3802	1.5m Blue Cat5e Cable
40K5581	3803	3m Blue Cat5e Cable
40K8927	3804	10m Blue Cat5e Cable
40K8930	3805	25m Blue Cat5e Cable
CAT5e Green Cables		
40K5563	3796	0.6m Green Cat5e Cable
00WE099	AVFQ	0.75m Green Cat5e Cable
00WE103	AVFR	1.0m Green Cat5e Cable
00WE107	AVFS	1.25m Green Cat5e Cable
40K5643	3797	1.5m Green Cat5e Cable
40K5793	3798	3m Green Cat5e Cable
40K5794	3799	10m Green Cat5e Cable
40K8869	3800	25m Green Cat5e Cable
CAT5e Yellow Cables		
40K8933	3791	0.6m Yellow Cat5e Cable
40K8951	3792	1.5m Yellow Cat5e Cable
40K8957	3793	3m Yellow Cat5e Cable
40K8801	3794	10m Yellow Cat5e Cable
40K8807	3795	25m Yellow Cat5e Cable

The following figure shows the ThinkSystem 10Gb 2-port Base-T LOM adapter which provides two RJ45 10GBASE-T ports.

Tip: Ports 1 is at further away from the edge connector and Port 2 is at the bottom, closer to the edge connector.



Figure 3. ThinkSystem 10Gb 2-port Base-T LOM

Features

The Intel X722 controller is optimized for data center, cloud, and mobile applications and includes the following features:

- VXLAN, NVGRE and GENEVE Hardware Offloads: These stateless offloads preserve application performance for overlay networks. With these offloads, it is possible to distribute network traffic across CPU cores. At the same time, the controller offloads LSO, GSO, and checksum from the host software, which reduces CPU overhead.
- Low latency: Intel Ethernet Flow Director delivers hardware-based application steering and Intel Data Direct I/O makes the processor cache the primary destination and source of I/O data rather than main memory.
- Virtualization performance: With Intel Virtualization Technology (VT), the controller delivers outstanding I/O performance in virtualized server environments. The controller reduces I/O bottlenecks by providing intelligent offloads for networking traffic per virtual machine (VM), which enables near-line rate speeds for small packets and supports almost an unlimited amount of isolated traffic flows so that you can scale your cloud environment.
- Next-generation VMDq: The controller support up to 128 VMDq VMs and offer enhanced Quality of Service (QoS) feature by providing weighted round-robin servicing for the Tx data. The controller offloads the data-sorting functionality from the hypervisor to the network silicon, which improves data throughput and CPU usage.
- SR-IOV implementation: Provides an implementation of the PCI-SIG standard for I/O Virtualization. The physical configuration of each port is divided into multiple virtual ports. Each virtual port is assigned to an individual VM directly by bypassing the virtual switch in the Hypervisor, which results in near-native performance.
- iWarp RDMA support implements kernel bypass and direct data placement and allows for more efficient high-speed networking by eliminating queues and network related interrupts

- VM load balancing: Provides traffic load balancing (Tx and Rx) across VMs that are bound to the team interface. It also provides fault tolerance of a switch, port, or cable.
- Auto-detect (PnP) feature for the LOM adapters, enabling you to change LOM adapters (eg from a 1Gb LOM to 10 Gb LOM) and the network interface will automatically reconfigure during the boot process

The following figure shows the ThinkSystem 10Gb 2-port SFP+ LOM adapter which provides two SFP+ cages for optical or direct-attach copper (DAC) connectivity.

Tip: Ports 1 is at further away from the edge connector and Port 2 is at the bottom, closer to the edge connector.

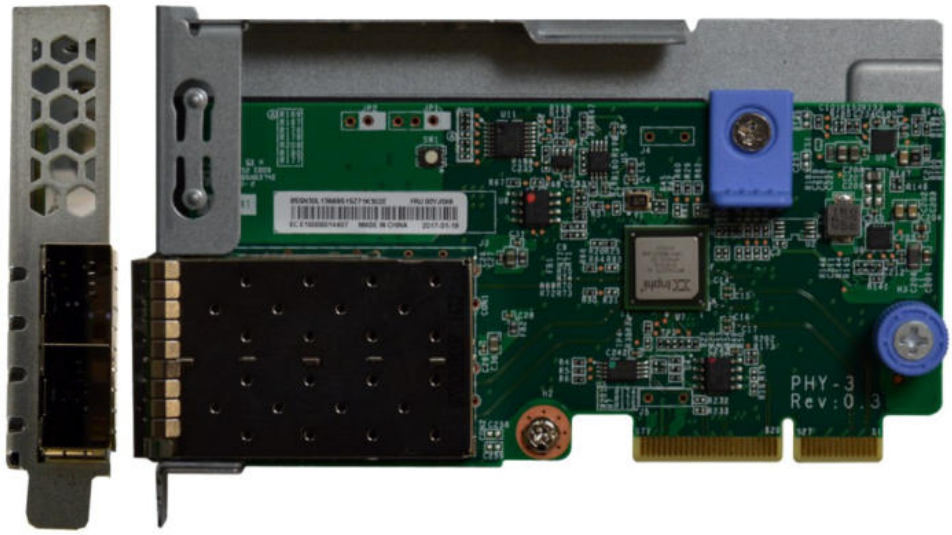


Figure 4. ThinkSystem 10Gb 2-port SFP+ LOM adapter

Specifications

The ThinkSystem LOM adapters support 1 Gb and 10 Gb Ethernet speeds as shown in the following table.

Note: None of the adapters support 100 Mbps and 10 Mbps Ethernet speeds.

Table 8. Supported network speeds

Part number	Description	10Gb	1Gb	100Mb	10Mb
Gigabit Ethernet					
7ZT7A00544	ThinkSystem 1Gb 2-port RJ45 LOM	No	Yes	No	No
7ZT7A00545	ThinkSystem 1Gb 4-port RJ45 LOM	No	Yes	No	No
10 Gb Ethernet					
7ZT7A00546	ThinkSystem 10Gb 2-port SFP+ LOM	Yes	No	No	No
7ZT7A00547	ThinkSystem 10Gb 4-port SFP+ LOM	Yes	No	No	No
7ZT7A00548	ThinkSystem 10Gb 2-port 10GBASE-T LOM	Yes	Yes	No	No
7ZT7A00549	ThinkSystem 10Gb 4-port 10GBASE-T LOM	Yes	Yes	No	No
EIOM modules for D2 Enclosure for use with SD530 servers					
7M17A04000	ThinkSystem D2 10Gb 8-port SFP+	Yes	No	No	No
7M17A04001	ThinkSystem D2 10Gb 8-port 10GBASE-T	Yes	Yes	No	No

The Intel Ethernet Connection X722 has the following specifications:

- Adapter connectors:
  - Gigabit adapters: RJ45 connectors
  - 10 GbE 10GBASE-T adapters: RJ45 connectors
  - 10 GbE SFP+ adapters: Empty SFP+ cages supporting SFP+ transceivers or DAC cables
- Host interface:
  - PCI Power Management/ACPI Extensions
  - TLP Processing Hint (TPH) Support
  - MSI-X Support - up to 1168 MSI-X vectors
- Virtualization features:
  - Microsoft Network Virtualization that uses Generic Routing Encapsulation (NVGRE)
  - VMware Virtual Extensible LAN (VXLAN)
  - GENEVE support
  - Intel Virtual Technology (VT) with VMDq for virtualization
  - VMware NetQueue and Microsoft VMQ support
  - VEB enhancement
  - SR-IOV support - 4 physical functions, 128 virtual functions
  - Virtual Bridging Support: VEPA/802.1Qbg
  - iWarp RDMA support

  Note: These virtualization features are only supported at 10 Gbps speeds
- Management features:
  - Advanced filtering capabilities (IPv4, IPv6)
  - SNMP
  - RMON statistic counters
  - Wake on LAN support (first port only)
  - NC-SI for XClarity Controller (XCC) shared management port connectivity only through port 1
  - Intel PROSet Utility for easy configuration and management

- Additional features:
  - IPv4 and IPv6 support
  - Jumbo Frame Support: 9728 bytes
  - VLAN support
  - Flow Control
  - 1588 Time Synchronization Support
  - Data Plane Development Kit (DPDK) support
- TCP/IP Layer 2 features:
  - Receive Side Scaling (RSS)
  - Large Send Offload (LSO)
  - TCP/UDP/IP/SCTP Checksum Offload
  - IPv4, IPv6
  - Supports iSCSI as an iSCSI software initiator
- Teaming support:
  - 10Gb LOM adapters support teaming with the X710 and other 10Gb adapters
  - 1Gb LOM adapters support teaming with the I350 and other 1Gb adapters
  - Adapter Fault Tolerance (AFT)
  - Switch Fault Tolerance (SFT)
  - Adaptive Load Balancing (ALB)
  - VM Load Balancing (VMLB)
  - IEEE 802.3ad (link aggregation control protocol)

  Note: Teaming is not vendor specific
- IEEE 802.1Q VLAN support with VLAN tag insertion, with stripping and packet filtering for up to 4096 VLAN tags.
- IEEE 802.3x flow control support
- IEEE 802.1p Class of Service (CoS)/QoS
  Note: QoS is only supported at 10 Gbps speeds
- Support for Advanced Packet Filtering
- UEFI and legacy PXE boot

The following figure shows the ThinkSystem 1Gb 4-port RJ45 LOM adapter which provides four RJ45 Gigabit Ethernet ports.

Tip: Ports are numbered sequentially starting with Port 1 at the top of the adapter (furthest away from the edge connector)



Figure 5. ThinkSystem 1Gb 4-port RJ45 LOM

Standards supported

The X722 controller supports the following IEEE standards:

- IEEE 802.1p CoS traffic prioritization
- IEEE 802.1Q VLAN tagging
- IEEE 802.3ad Link Aggregation Control Protocol
- IEEE 802.3x Full-duplex flow control
- IEEE 1588, 802.1as Time Sync

10 GbE standards:

- IEEE 802.3ae 10GBASE-SR short range fiber optics 10 Gb Ethernet
- 10GSFP+Cu SFP+ Direct Attach copper
- IEEE 802.3ab 1000BASE-T copper twisted pair Gigabit Ethernet
- IEEE 802.3an 10GBASE-T copper twisted pair 10 Gb Ethernet

Server support

The ThinkSystem LOM adapters are supported in the servers listed in the following table.

As shown in the table, some ThinkSystem servers do not support the LOM adapters even though they offer Intel Ethernet Connection X722:

- The ST550 tower server has two onboard Gigabit ports that connect to the X722 controller
- The SD530 dense server routes two 10 GbE connections form the X722 controller to the Ethernet ports in the EIOM network modules in the D2 Enclosure.
- The SN550 and SN850 Blade servers use use a Fabric Connector ("Periscope connector") to route four 10 GbE connections to the midplane of the Flex System Enterprise Chassis.

The following tables list the ThinkSystem servers that are compatible.

Table 9. ThinkSystem server support (Part 1)

		Intel 2S								AMD			
Part number	**Description**	**ST550 (7X09/7X10)**	**SR530 (7X07/7X08)**	**SR550 (7X03/7X04)**	**SR570 (7Y02/7Y03)**	**SR590 (7X98/7X99)**	**SR630 (7X01/7X02)**	**SR650 (7X05/7X06)**	**SR670 (7Y36/37/38)**	**SR635 (7Y98/7Y99)**	**SR655 (7Y00/7Z01)**	**SR645 (7D2Y/7D2X)**	**SR665 (7D2W/7D2V)**
Gigabit Ethernet													
None	Integrated 2-port 1Gb RJ45	N	Y	Y	Y	Y	N	N	N	N	N	N	N
7ZT7A00544	ThinkSystem 1Gb 2-port RJ45 LOM	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N
7ZT7A00545	ThinkSystem 1Gb 4-port RJ45 LOM	N	N	N	N	N	Y	Y	N	N	N	N	N
10 Gb Ethernet													
7ZT7A00546	ThinkSystem 10Gb 2-port SFP+ LOM	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N
7ZT7A00547	ThinkSystem 10Gb 4-port SFP+ LOM	N	N	N	N	N	Y	Y	N	N	N	N	N
7ZT7A00548	ThinkSystem 10Gb 2-port Base-T LOM	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N
7ZT7A00549	ThinkSystem 10Gb 4-port Base-T LOM	N	N	N	N	N	Y	Y	N	N	N	N	N
EIOM modules for D2 Enclosure for use with SD530 servers													
7M17A04001	ThinkSystem D2 10Gb 8 port EIOM Base T RJ45	N	N	N	N	N	N	N	N	N	N	N	N
7M17A04000	ThinkSystem D2 10Gb 8 port EIOM SFP+	N	N	N	N	N	N	N	N	N	N	N	N

Table 10. ThinkSystem server support (Part 2)

Part number	Description	E	1S Intel				4S Intel						Dense/ Blade			
		SE350 (7Z46/7D1X)	ST50 (7Y48/7Y50)	ST250 (7Y45/7Y46)	SR150 (7Y54)	SR250 (7Y51/7Y52)	SR850 (7X18/7X19)	SR850P (7D2F/2D2G)	SR860 (7X69/7X70)	SR950 (7X11/12/13)	SR850 V2 (7D31/32/33)	SR860 V2 (7Z59/7Z60)	SD530 (7X21)	SD650 (7X58)	SN550 (7X16)	SN850 (7X15)
Gigabit Ethernet																
7ZT7A00544	ThinkSystem 1Gb 2-port RJ45 LOM	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N
7ZT7A00545	ThinkSystem 1Gb 4-port RJ45 LOM	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N
10 Gb Ethernet																
7ZT7A00546	ThinkSystem 10Gb 2-port SFP+ LOM	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N
7ZT7A00547	ThinkSystem 10Gb 4-port SFP+ LOM	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N
7ZT7A00548	ThinkSystem 10Gb 2-port Base-T LOM	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N
7ZT7A00549	ThinkSystem 10Gb 4-port Base-T LOM	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N
EIOM modules for D2 Enclosure for use with SD530 servers																
7M17A04001	ThinkSystem D2 10Gb 8 port EIOM Base T RJ45	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N
7M17A04000	ThinkSystem D2 10Gb 8 port EIOM SFP+	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N
Integrated LOM for blade servers																
None	Integrated 4-port 10 Gb (requires Fabric Connector)	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y

The following figure shows the ThinkSystem 1Gb 2-port RJ45 LOM adapter which provides two RJ45 Gigabit Ethernet ports.

Tip: Ports 1 is at further away from the edge connector and Port 2 is at the bottom, closer to the edge connector.



Figure 6. ThinkSystem 1Gb 2-port RJ45 LOM

Cabling requirements

The network cables that can be used with the adapters are described in the following sections.

- 10GBASE-SR (supported with the 10 GbE SFP+ SR transceivers listed in Table 2)
  850 nm communication that uses multimode fiber cable (50 µ or 62.5 µ) up to 300 m that uses an LC duplex connector
- 10GSFP+Cu (supported with the SFP+ DAC cables listed in Table 3)

Operating system support

The following tables list the supported operating systems for the adapters.

- ThinkSystem 1Gb 2-Port RJ45 LOM, 7ZT7A00544
- ThinkSystem 1Gb 4-Port RJ45 LOM, 7ZT7A00545
- ThinkSystem 2-Port SFP+ LOM, 7ZT7A00546
- ThinkSystem 10Gb 4-Port SFP+ LOM, 7ZT7A00547
- ThinkSystem 10Gb 2-Port Base-T LOM, 7ZT7A00548
- ThinkSystem 10Gb 4-Port Base-T LOM, 7ZT7A00549
- ThinkSystem D2 10Gb 8-port EIOM Base-T (RJ45), 7M17A04001
- ThinkSystem D2 10Gb 8-port EIOM SFP+, 7M17A04000

Tip: These tables are automatically generated based on data from Lenovo ServerProven.

Table 11. Operating system support for ThinkSystem 1Gb 2-Port RJ45 LOM, 7ZT7A00544

Operating systems	SR530 (Gen 2)	SR550 (Gen 2)	SR570 (Gen 2)	SR590 (Gen 2)	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR530 (Gen 1)	SR550 (Gen 1)	SR570 (Gen 1)	SR590 (Gen 1)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
Microsoft Windows Server 2012 R2	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2016	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2019	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1709	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1803	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.10	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.9	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.3	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
Red Hat Enterprise Linux 7.4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.5	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.7	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.8	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 11 SP4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP2	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
SUSE Linux Enterprise Server 12 SP3	N	N	N	N	N	N	N	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.0 U3	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
VMware vSphere Hypervisor (ESXi) 6.5 U1	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Operating systems	SR530 (Gen 2)	SR550 (Gen 2)	SR570 (Gen 2)	SR590 (Gen 2)	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR530 (Gen 1)	SR550 (Gen 1)	SR570 (Gen 1)	SR590 (Gen 1)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
VMware vSphere Hypervisor (ESXi) 6.7	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 12. Operating system support for ThinkSystem 1Gb 4-Port RJ45 LOM, 7ZT7A00545

Operating systems	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
Microsoft Windows Server 2012 R2	N	N	N	N	N	N	Y	Y	Y	Y	Y
Microsoft Windows Server 2016	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2019	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1709	N	N	N	N	N	N	Y	Y	Y	Y	Y
Microsoft Windows Server version 1803	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.10	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.9	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.3	N	N	N	N	N	N	Y	Y	Y	N	Y
Red Hat Enterprise Linux 7.4	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.5	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.7	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.8	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 11 SP4	N	N	N	N	N	N	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP2	N	N	N	N	N	N	Y	Y	Y	N	Y
SUSE Linux Enterprise Server 12 SP3	N	N	N	Y	N	N	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Operating systems	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
SUSE Linux Enterprise Server 12 SP5 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.0 U3	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5	N	N	N	N	N	N	Y	Y	Y	N	Y
VMware vSphere Hypervisor (ESXi) 6.5 U1	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 13. Operating system support for ThinkSystem 10Gb 2-Port SFP+ LOM, 7ZT7A00546

Operating systems	SR530 (Gen 2)	SR550 (Gen 2)	SR570 (Gen 2)	SR590 (Gen 2)	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR530 (Gen 1)	SR550 (Gen 1)	SR570 (Gen 1)	SR590 (Gen 1)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
Microsoft Windows Server 2012 R2	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2016	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2019	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1709	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1803	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.10	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.9	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.3	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
Red Hat Enterprise Linux 7.4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.5	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.7	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Operating systems	SR530 (Gen 2)	SR550 (Gen 2)	SR570 (Gen 2)	SR590 (Gen 2)	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR530 (Gen 1)	SR550 (Gen 1)	SR570 (Gen 1)	SR590 (Gen 1)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
Red Hat Enterprise Linux 7.8	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 11 SP4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP2	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
SUSE Linux Enterprise Server 12 SP3	N	N	N	N	N	N	N	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.0 U3	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
VMware vSphere Hypervisor (ESXi) 6.5 U1	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 14. Operating system support for ThinkSystem 10Gb 4-Port SFP+ LOM, 7ZT7A00547

Operating systems	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
Microsoft Windows Server 2012 R2	N	N	N	N	N	N	Y	Y	Y	Y	Y
Microsoft Windows Server 2016	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2019	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1709	N	N	N	N	N	N	Y	Y	Y	Y	Y
Microsoft Windows Server version 1803	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.10	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.9	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.3	N	N	N	N	N	N	Y	Y	Y	N	Y
Red Hat Enterprise Linux 7.4	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.5	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.7	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.8	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 11 SP4	N	N	N	N	N	N	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP2	N	N	N	N	N	N	Y	Y	Y	N	Y
SUSE Linux Enterprise Server 12 SP3	N	N	N	Y	N	N	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.0 U3	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5	N	N	N	N	N	N	Y	Y	Y	N	Y
VMware vSphere Hypervisor (ESXi) 6.5 U1	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Operating systems	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
VMware vSphere Hypervisor (ESXi) 6.7	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 15. Operating system support for ThinkSystem 10Gb 2-Port Base-T LOM, 7ZT7A00548

Operating systems	SR530 (Gen 2)	SR550 (Gen 2)	SR570 (Gen 2)	SR590 (Gen 2)	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR530 (Gen 1)	SR550 (Gen 1)	SR570 (Gen 1)	SR590 (Gen 1)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
Microsoft Windows Server 2012 R2	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2016	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2019	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1709	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1803	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.10	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.9	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.3	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
Red Hat Enterprise Linux 7.4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.5	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.7	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.8	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 11 SP4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP2	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
SUSE Linux Enterprise Server 12 SP3	N	N	N	N	N	N	N	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Operating systems	SR530 (Gen 2)	SR550 (Gen 2)	SR570 (Gen 2)	SR590 (Gen 2)	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR530 (Gen 1)	SR550 (Gen 1)	SR570 (Gen 1)	SR590 (Gen 1)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
SUSE Linux Enterprise Server 12 SP5 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.0 U3	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y	N	Y
VMware vSphere Hypervisor (ESXi) 6.5 U1	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 16. Operating system support for ThinkSystem 10Gb 4-Port Base-T LOM, 7ZT7A00549

Operating systems	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
Microsoft Windows Server 2012 R2	N	N	N	N	N	N	Y	Y	Y	Y	Y
Microsoft Windows Server 2016	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2019	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server version 1709	N	N	N	N	N	N	Y	Y	Y	Y	Y
Microsoft Windows Server version 1803	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.10	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 6.9	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.3	N	N	N	N	N	N	Y	Y	Y	N	Y
Red Hat Enterprise Linux 7.4	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.5	N	N	N	N	N	N	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.6	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.7	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Operating systems	SR630 (Gen 2)	SR650 (Gen 2)	SR850 (Gen 2)	SR850P	SR860 (Gen 2)	SR950 (Gen 2)	SR630 (Gen 1)	SR650 (Gen 1)	SR850 (Gen 1)	SR860 (Gen 1)	SR950 (Gen 1)
Red Hat Enterprise Linux 7.8	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 7.9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 11 SP4	N	N	N	N	N	N	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP2	N	N	N	N	N	N	Y	Y	Y	N	Y
SUSE Linux Enterprise Server 12 SP3	N	N	N	Y	N	N	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP4 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 12 SP5 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP1 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP2 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 with Xen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.0 U3	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5	N	N	N	N	N	N	Y	Y	Y	N	Y
VMware vSphere Hypervisor (ESXi) 6.5 U1	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7	N	N	N	N	N	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 17. Operating system support for ThinkSystem D2 10Gb 8-port EIOM Base-T (RJ45), 7M17A04001

Operating systems	D2 Enclosure, 7X20	D2 Modular Encl, 7X22
Microsoft Windows Server 2012 R2	Y	N
Microsoft Windows Server 2016	Y	N
Microsoft Windows Server 2019	Y	Y
Microsoft Windows Server version 1803	Y	Y
Red Hat Enterprise Linux 6.10	Y	Y
Red Hat Enterprise Linux 6.9	Y	N
Red Hat Enterprise Linux 7.3	Y	N
Red Hat Enterprise Linux 7.4	Y	N
Red Hat Enterprise Linux 7.5	Y	Y
Red Hat Enterprise Linux 7.6	Y	Y
Red Hat Enterprise Linux 7.7	Y	Y
Red Hat Enterprise Linux 7.8	Y	Y
Red Hat Enterprise Linux 7.9	Y	Y
Red Hat Enterprise Linux 8.0	Y	Y
Red Hat Enterprise Linux 8.1	Y	Y
Red Hat Enterprise Linux 8.2	Y	Y
Red Hat Enterprise Linux 8.3	Y	Y
SUSE Linux Enterprise Server 11 SP4	Y	N
SUSE Linux Enterprise Server 12 SP2	Y	N
SUSE Linux Enterprise Server 12 SP3	Y	N
SUSE Linux Enterprise Server 12 SP4	Y	Y
SUSE Linux Enterprise Server 12 SP4 with Xen	Y	Y
SUSE Linux Enterprise Server 12 SP5	Y	Y
SUSE Linux Enterprise Server 12 SP5 with Xen	Y	Y
SUSE Linux Enterprise Server 15	Y	Y
SUSE Linux Enterprise Server 15 SP1	Y	Y
SUSE Linux Enterprise Server 15 SP1 with Xen	Y	Y
SUSE Linux Enterprise Server 15 SP2	Y	Y
SUSE Linux Enterprise Server 15 SP2 with Xen	Y	Y
SUSE Linux Enterprise Server 15 with Xen	Y	Y
VMware vSphere Hypervisor (ESXi) 6.0 U3	Y	N
VMware vSphere Hypervisor (ESXi) 6.5	Y	N
VMware vSphere Hypervisor (ESXi) 6.5 U1	Y	N

Operating systems	D2 Enclosure, 7X20	D2 Modular Encl, 7X22
VMware vSphere Hypervisor (ESXi) 6.5 U2	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U3	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U1	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U2	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U3	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U1	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U2	Y	Y

Table 18. Operating system support for ThinkSystem D2 10Gb 8-port EIOM SFP+, 7M17A04000

Operating systems	D2 Enclosure, 7X20	D2 Modular Encl, 7X22
Microsoft Windows Server 2012 R2	Y	N
Microsoft Windows Server 2016	Y	N
Microsoft Windows Server 2019	Y	Y
Microsoft Windows Server version 1803	Y	Y
Red Hat Enterprise Linux 6.10	Y	Y
Red Hat Enterprise Linux 6.9	Y	N
Red Hat Enterprise Linux 7.3	Y	N
Red Hat Enterprise Linux 7.4	Y	N
Red Hat Enterprise Linux 7.5	Y	Y
Red Hat Enterprise Linux 7.6	Y	Y
Red Hat Enterprise Linux 7.7	Y	Y
Red Hat Enterprise Linux 7.8	Y	Y
Red Hat Enterprise Linux 7.9	Y	Y
Red Hat Enterprise Linux 8.0	Y	Y
Red Hat Enterprise Linux 8.1	Y	Y
Red Hat Enterprise Linux 8.2	Y	Y
Red Hat Enterprise Linux 8.3	Y	Y

Operating systems	D2 Enclosure, 7X20	D2 Modular Encl, 7X22
SUSE Linux Enterprise Server 11 SP4	Y	N
SUSE Linux Enterprise Server 12 SP2	Y	N
SUSE Linux Enterprise Server 12 SP3	Y	N
SUSE Linux Enterprise Server 12 SP4	Y	Y
SUSE Linux Enterprise Server 12 SP4 with Xen	Y	Y
SUSE Linux Enterprise Server 12 SP5	Y	Y
SUSE Linux Enterprise Server 12 SP5 with Xen	Y	Y
SUSE Linux Enterprise Server 15	Y	Y
SUSE Linux Enterprise Server 15 SP1	Y	Y
SUSE Linux Enterprise Server 15 SP1 with Xen	Y	Y
SUSE Linux Enterprise Server 15 SP2	Y	Y
SUSE Linux Enterprise Server 15 SP2 with Xen	Y	Y
SUSE Linux Enterprise Server 15 with Xen	Y	Y
VMware vSphere Hypervisor (ESXi) 6.0 U3	Y	N
VMware vSphere Hypervisor (ESXi) 6.5	Y	N
VMware vSphere Hypervisor (ESXi) 6.5 U1	Y	N
VMware vSphere Hypervisor (ESXi) 6.5 U2	Y	Y
VMware vSphere Hypervisor (ESXi) 6.5 U3	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U1	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U2	Y	Y
VMware vSphere Hypervisor (ESXi) 6.7 U3	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U1	Y	Y
VMware vSphere Hypervisor (ESXi) 7.0 U2	Y	Y

Warranty

One-year limited warranty. When installed in a supported server, these adapters assume the system’s base warranty and any warranty upgrade.

Agency approvals

The LOM adapters conform to the following standards:

- UL recognized to UL60950-1 2nd Edition
- FCC Rules, Part 15, Class A
- Australian EMC Framework (RCM)
- Japan VCCI, Class A
- Industry Canada, ICES-003, Class A
- EU (CE Mark)
- Korea KC-RRA, Class A
- China RoHS compliant

Related publications

For more information, see the following resources:

- Lenovo ThinkSystem networking options product web page
  https://lenovopress.com/lp0765-networking-options-for-thinksystem-servers
- Lenovo ServerProven compatibility information for network adapters:
  http://www.lenovo.com/us/en/serverproven
- Lenovo ThinkSystem product publications:
  http://thinksystem.lenovofiles.com/help/index.jsp

Related product families

Product families related to this document are the following:

- 1 Gb Ethernet Connectivity
- 10 Gb Ethernet Connectivity
- Ethernet Adapters

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2021. All rights reserved.

This document, LP0654, was created or updated on October 13, 2020.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  http://lenovopress.com/LP0654
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at http://lenovopress.com/LP0654.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
Flex System
RackSwitch
ServerProven®
ThinkSystem
XClarity®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Lenovo ThinkSystem SR530 Server (Xeon SP Gen 2)

Product Guide

Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.

Featuring the second generation of the Intel Xeon Processor Scalable Family (Xeon SP Gen 2), the SR530 server offers a balance of performance, capacity and value. The SR530 server supports up to two processors, up to 768 GB of 2933 MHz TruDDR4 memory, 8x 2.5-inch or 4x 3.5-inch drive bays with an extensive choice of SAS/SATA SSDs and SAS/SATA HDDs, and flexible I/O expansion options with a LOM slot and up to 3x PCIe slots.

The SR530 server offers basic software RAID or advanced hardware RAID protection and a wide range of networking options, including embedded LOM, selectable LOM, ML2, and PCIe network adapters. The next-generation Lenovo XClarity Controller, which is built into the SR530 server, provides advanced service processor control, monitoring, and alerting functions.

The following figure shows the ThinkSystem SR530 server with 3.5-inch front hot-swap drives. Other drive configurations are also available.



Figure 1. Lenovo ThinkSystem SR530 with 3.5-inch hot-swap drives

Did you know?

The SR530 server delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies that can deliver 96% (Titanium) or 94% (Platinum) efficiency at 50% load when connected to a 200 - 240 V AC power source.

The SR530 server is designed to meet ASHRAE A4 standards (up to 45 °C) in select configurations, which enable customers to lower energy costs, while still maintaining world-class reliability.

Key features

The SR530 server offers a balance of processing power, expandability, and cost for small and medium businesses up to the large enterprise. Ease of use and comprehensive systems management tools help make deployment easier and efficient design improves your business environment and helps save operational costs.

Scalability and performance

The SR530 server offers numerous features to boost performance, improve scalability, and reduce costs:

- Improves productivity by offering superior system performance with the second generation of the Intel Xeon Processor Scalable Family with up to 22-core processors, up to 30.25 MB of last level cache (LLC), up to 2933 MHz memory speeds, and up to 10.4 GT/s Ultra Path Interconnect (UPI) links.
    - Support for up to two processors, 44 cores, and 88 threads allows to maximize the concurrent execution of multithreaded applications.
    - Intelligent and adaptive system performance with energy efficient Intel Turbo Boost 2.0 Technology allows CPU cores to run at maximum speeds during peak workloads by temporarily going beyond processor thermal design power (TDP).
    - Intel Hyper-Threading Technology boosts performance for multithreaded applications by enabling simultaneous multithreading within each processor core, up to two threads per core.
    - Intel Virtualization Technology integrates hardware-level virtualization hooks that allow operating system vendors to better utilize the hardware for virtualization workloads.
    - Intel Speed Select Technology provides improvements in server utilization and guaranteed per-core performance service levels with more granular control over processor performance.
    - Intel Deep Learning Boost (Vector Neural Network Instruction set [VNNI]) is designed to deliver significant, more efficient Deep Learning (Inference) acceleration for high-performance Artificial Intelligence (AI) workloads.
    - Intel Advanced Vector Extensions 512 (AVX-512) enable acceleration of enterprise-class and high performance computing (HPC) workloads.
- Helps maximize system performance for data intensive applications with up to 2933 MHz memory speeds and up to 768 GB of memory capacity.
- Offers flexible and scalable internal storage in a 1U rack form factor with up to 8x 2.5-inch drives for performance-optimized configurations or up to 4x 3.5-inch drives for capacity-optimized configurations, providing a wide selection of SAS/SATA HDDs/SSDs.
- Provides I/O scalability with a LOM slot and up to three PCI Express (PCIe) 3.0 I/O expansion slots in a 1U rack form factor.
- Reduces I/O latency and increases overall system performance with Intel Integrated I/O Technology that embeds the PCI Express 3.0 controller into the Intel Xeon Processor Scalable Family.

Availability and serviceability

The SR530 server provides many features to simplify serviceability and increase system uptime:

- Offers protection in the event of a non-correctable memory failure with Single Device Data Correction (SDDC, also known as Chipkill, requires x4-based DIMMs), Adaptive Double Device Data Correction (ADDDC, also known as Redundant Bit Steering [RBS], requires x4-based DIMMs and Intel Xeon Gold or Platinum processors), memory mirroring, and memory rank sparing.
- Provides easy access to upgrades and serviceable parts (such as processors, memory DIMMs, and adapter cards) with tool-less cover removal.
- Offers affordable data protection with software RAID and Simple Swap drives and advanced hardware RAID data redundancy with hot-swap drives.
- Provides availability for applications with redundant hot-swap power supplies and redundant non-hot-swap fans.
- Speeds up troubleshooting tasks to reduce service time with diagnostics built into the XClarity Provisioning Manager.

- Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
- Continuously monitors system parameters, triggers alerts, and performs recovery actions in case of failure to minimize downtime with Built-in XClarity Controller (XCC).
- Provides quick access to system status, firmware, network, health, and alerts information via Virtual Operator Panel from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access.

Manageability and security

Powerful systems management features simplify local and remote management of the SR530 server and deliver enterprise-class data protection:

- Provides advanced service processor control, monitoring, and alerting functions with XClarity Controller, a next generation service processor.
- Improves Unified Extensible Firmware Interface (UEFI) system setup, configuration, updates, simplified error handling, and operating system deployment with the embedded XClarity Provisioning Manager.
- Offers XClarity Essentials software tools that can help you set up, use, and maintain the server.
- Increases uptime, reduces costs, and improves productivity through advanced server management capabilities with Lenovo XClarity Administrator that provides comprehensive hardware management.
- Provides on-the-go monitoring and management of devices in XClarity Administrator from anywhere with the Lenovo XClarity mobile app, which can help improve efficiency and reduce downtime risks.
- Centralizes infrastructure resource management with Lenovo XClarity Integrators for VMware vCenter and Microsoft System Center, extending XClarity Administrator features to virtualization management software tools and enabling users to deploy and manage infrastructure end-to-end.
- Offers advanced cryptographic functionality (such as digital signatures and remote attestation) with an integrated Trusted Platform Module (TPM) or optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC).
- Keeps user data safe with Lenovo Business Vantage, a security software tool suite designed to work with the Trusted Cryptographic Module (available only in PRC).
- Offers enterprise-class data protection with advanced RAID and optional self-encrypting drives.
- Provides faster, stronger encryption with industry-standard AES NI support.
- Helps prevent certain classes of malicious buffer overflow attacks with Intel Execute Disable Bit functionality, when combined with a supporting operating system.
- Enhances security through hardware-based resistance to malicious software attacks with Intel Trusted Execution Technology, allowing an application to run in its own isolated space, protected from all other software running on a system.

Energy efficiency

The SR530 server offers the following energy-efficiency features to save energy, reduce operational costs, increase energy availability, and contribute to the green environment:

- Delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies.
- Enables customers to lower energy costs with design to meet ASHRAE A4 standards in select configurations.
- Reduces power drawn with Intel Intelligent Power Capability that powers individual processor elements on and off as needed.
- Helps reduce power consumption with variable speed fans.
- Helps achieve lower heat output and reduced cooling needs with Lenovo XClarity Energy Manager that provides advanced data center power notification, analysis, and policy-based management.

Components and connectors

The following figure shows the front of the SR530 server with four 3.5-inch drive bays.

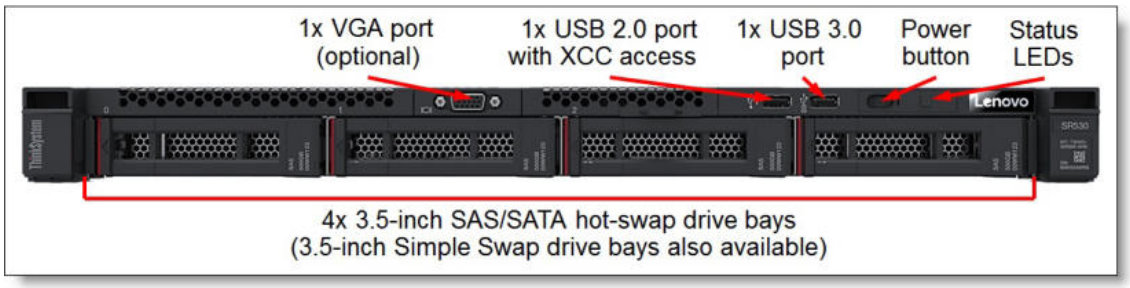


Figure 2. Front view of the SR530: 4x 3.5-inch drive bays

The following figure shows the front of the SR530 server with eight 2.5-inch drive bays.

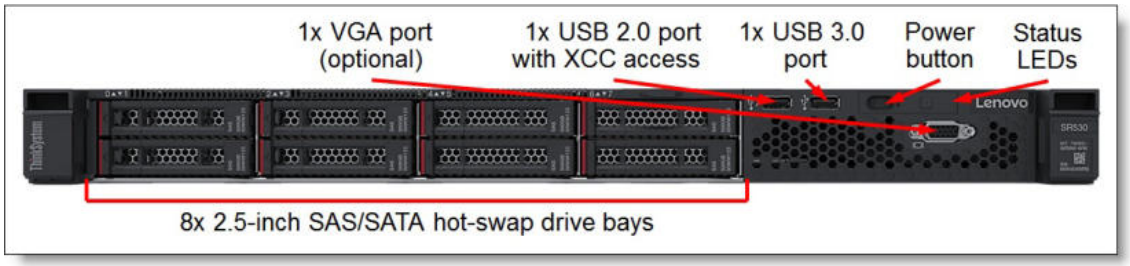


Figure 3. Front view of the SR530: 8x 2.5-inch drive bays

The front of the SR530 server includes the following components:

- Up to 8x 2.5-inch or 4x 3.5-inch hot-swap drive bays, or 4x 3.5-inch Simple Swap drive bays.
- One VGA port (optional).
- One USB 3.0 port.
- One USB 2.0 port with XClarity Controller access.
- Power button.
- Status LEDs.

The following figure shows the rear of the SR530 server with three PCIe low profile slots.

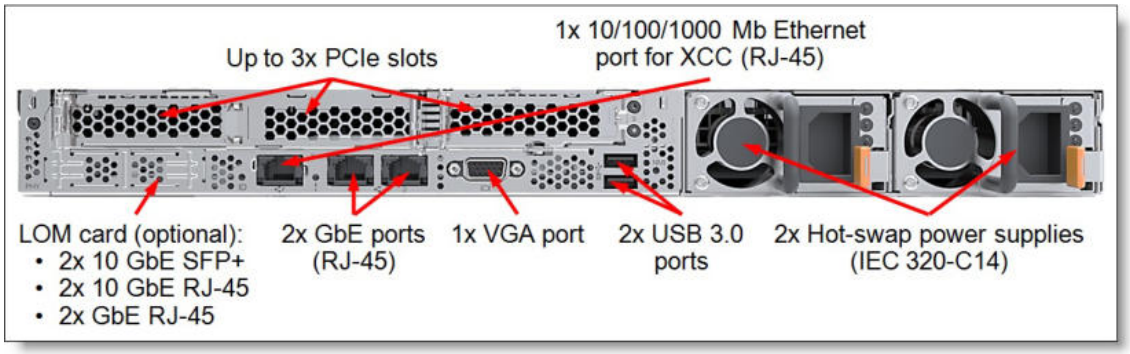


Figure 4. Rear view of the SR530

The rear of the SR530 server includes the following components:

- Up to three PCIe expansion slots (depending on the riser cards selected).
- One LOM card slot.
- One 1 GbE port for XClarity Controller.
- One VGA port.
- Two USB 3.0 ports.
- Up to two hot-swap power supplies.

The following figure shows the locations of key components inside the SR530 server.

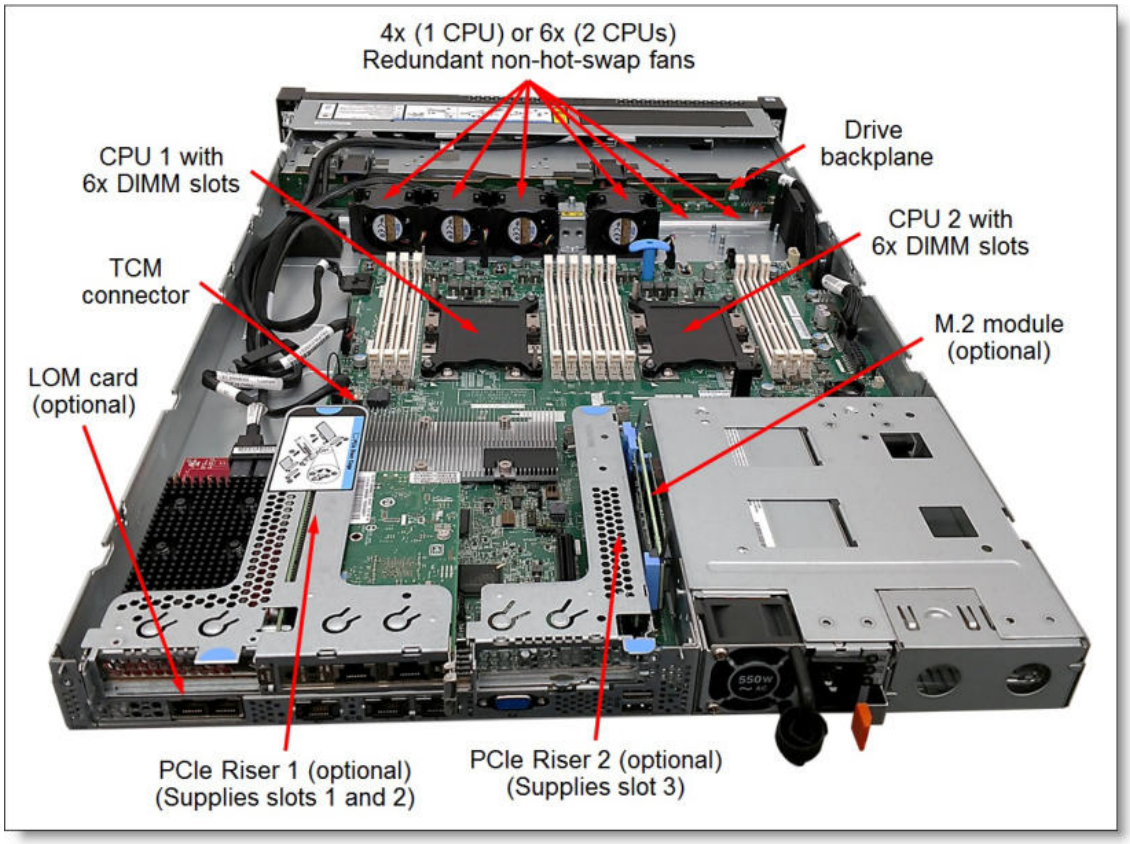


Figure 5. Internal view of the SR530

The following key components are located inside the SR530 server:

- Up to two processors.
- 12 DIMM slots (6 DIMM slots per processor).
- Drive backplanes.
- One M.2 module connector.
- One LOM card connector.
- Two slots for PCIe riser cards.
- One TCM connector.
- Four (one processor) or six (two processors) non-hot-swap system fans.

System specifications

The following table lists the system specifications for the SR530 server.

Table 1. SR530 system specifications

Attribute	Specification
Machine types	7X07 - 1 year warranty 7X08 - 3 year warranty
Form factor	1U rack-mount.
Processor	Up to two Intel Xeon Gen 2 Bronze, Silver, Gold, or Platinum processors: • Up to 22 cores (1.9 GHz core speeds) • Up to 3.8 GHz core speeds (4 cores) • Two UPI links up to 10.4 GT/s each • Up to 30.25 MB cache • Up to 2933 MHz memory speed

Attribute	Specification
Chipset	Intel C622.
Memory	Up to 12 DIMM sockets (6 DIMMs per processor; six memory channels per processor with one DIMM per channel) with support for the following TruDDR4 RDIMM types and capacities: • 8 GB, 16 GB, 32 GB, and 64 GB 2933 MHz. • 16 GB and 32 GB 2666 MHz.
Memory protection	Error correction code (ECC), SDDC (for x4-based memory DIMMs), ADDDC (for x4-based memory DIMMs, requires Intel Xeon Gold or Platinum processors), memory mirroring, memory rank sparing, patrol scrubbing, and demand scrubbing.
Memory capacity	Up to 768 GB with 12x 64 GB RDIMMs (Up to 384 GB per processor).
Drive bays	• 4 LFF SATA Simple Swap drive bays • 4 LFF SAS/SATA hot-swap drive bays • 8 SFF SAS/SATA hot-swap drive bays

Internal storage capacity	• 2.5-inch drives:
	  ◦ 122.88TB using 8x 15.36TB 2.5-inch SAS/SATA SSDs
	  ◦ 19.2TB using 8x 2.4TB 2.5-inch HDDs
	• 3.5-inch drives:
	  ◦ 72TB using 4x 18TB 3.5-inch HDDs
	  ◦ 30.72TB using 4x 7.68TB 3.5-inch SAS/SATA SSDs

Storage controller	6 Gbps SATA
	• Non-RAID: Onboard SATA AHCI
	• RAID 0/1/10/5: Onboard SATA RAID (Intel RSTe)
	
	12 Gbps SAS/6 Gbps SATA RAID
	• RAID 0/1/10/5/50:
	  ◦ RAID 530-8i
	  ◦ RAID 730-8i 1GB Cache
	• RAID 0/1/10/5/50/6/60:
	  ◦ RAID 730-8i 2GB Flash
	  ◦ RAID 930-8i 2GB Flash
	  ◦ RAID 930-16i 4GB or 8GB Flash
	
	12 Gbps SAS/6 Gbps SATA non-RAID: 430-8i HBA

Optical drive bays	None. Support for an external USB DVD RW Optical Disk Drive (SeeOptical drives).

Network interfaces	• 2x Integrated 1 GbE RJ-45 ports (no 10/100 Mb support)
	• Onboard LOM slot for up to two additional 1/10 Gb Ethernet ports:
	  ◦ 2x 1 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE SFP+ ports (no 10/100 Mb support)
	• Optional Mezzanine LOM (ML2) slot for dual-port 10 GbE cards with SFP+ or RJ-45 connectors.
	• 1x RJ-45 10/100/1000 Mb Ethernet systems management port.

I/O expansion slots	Up to three slots depending on the riser cards installed. The slots are as follows: • Slot 1: PCIe 3.0 x8; low profile • Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length • Slot 3: PCIe 3.0 x8 or x16; low profile PCIe x16 slot 3 requires the second processor to be installed.
Ports	• Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. • Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
Cooling	Four (one processor) or six (two processors) non-hot-swap system fans with N+1 redundancy.
Power supply	Up to two redundant hot-swap 550 W or 750 W (100 - 240 V) High Efficiency Platinum or 750 W (200 - 240 V) High Efficiency Titanium AC power supplies. HVDC support (PRC only).

Attribute	Specification
Video	Matrox G200 with 16 MB memory integrated into the XClarity Controller. Maximum resolution is 1920x1200 at 60 Hz with 32 bits per pixel.
Hot-swap parts	Drives (select models) and power supplies.
Systems management	XClarity Controller (XCC) Standard, Advanced, or Enterprise (Pilot 4 chip), proactive platform alerts, XClarity Provisioning Manager, XClarity Essentials, XClarity Administrator, XClarity Integrators for VMware vCenter and Microsoft System Center, XClarity Energy Manager, Capacity Planner.
Security features	Power-on password, administrator's password, secure firmware updates, Trusted Platform Module (TPM) 1.2 or 2.0 (configurable UEFI setting). Optional lockable front bezel. Optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC). Optional Lenovo Business Vantage security software (available only in PRC).
Operating systems	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. See the Operating systems section for specifics.
Warranty	One-year (7X07) or three-year (7X08) customer-replaceable unit (CRU) and onsite limited warranty with 9x5 Next Business Day Parts Delivered.
Service and support	Optional service upgrades are available through Lenovo Services: 2-hour or 4-hour response time, 6-hour or 24-hour committed service repair, warranty extension up to 5 years, 1-year or 2-year post-warranty extensions, YourDrive Your Data, Enterprise Software Support, and Basic Hardware Installation Services.
Dimensions	Width: 435 mm (17.1 in.), height: 43 mm (1.7 in.), depth: 750 mm (29.5 in.). See Physical specifications for details.
Weight	Minimum configuration: 10.2 kg (22.5 lb), maximum: 16 kg (35.3 lb)

Models

ThinkSystem SR530 models can be configured by using the Lenovo Data Center Solution Configurator (DCSC).

Configure-to-order (CTO) models are used to create models with factory-integrated server customizations. For CTO models, two base CTO models are available for the SR530 as listed in the following table, CTO1WW and CTOLWW:

- The CTO1WW base CTO model is for general business and is selectable by choosing **General Purpose** mode in DCSC.
- The CTOLWW base model is intended for High Performance Computing (HPC) and Artificial Intelligence (AI) configurations and solutions, including configurations for Lenovo Scalable Infrastructure (LeSI), and is enabled using either the **HPC & AI LeSI Solutions** mode or **HPC & AI ThinkSystem Hardware** mode in DCSC. CTOLWW configurations can also be built using System x and Cluster Solutions Configurator (x-config).

Preconfigured server models may also be available for the SR530, however these are region-specific; that is, each region may define their own server models, and not all server models are available in every region.

The following table lists the base CTO models of the ThinkSystem SR530 server.

Table 2. Base CTO models

Description	Machine Type/Model General purpose	Machine Type/Model for HPC and AI
ThinkSystem SR530 - 3 year Warranty	7X08CTO1WW	7X08CTOLWW
ThinkSystem SR530 - 1 year Warranty	7X07CTO1WW	7X07CTOLWW

The following table lists the base chassis for CTO models of the SR530 server.

Table 3. Base chassis for CTO models

Feature code	Description
AV0T	ThinkSystem SR530 3.5" Chassis with 4 Bays
AV0S	ThinkSystem SR530 2.5" Chassis with 8 Bays

All models of the SR530 server are shipped with the following items:

- *Rack Installation Guide*
- *Electronic Publications Flyer*

Models table conventions: The model tables shown in this section use the following conventions:

- XClarity Controller: "S" = Standard, "A" = Advanced, "E" = Enterprise.
- Front VGA port: "Y" = Included; "N" = Not included, optional.
- Tool-less Rail Kit: "Y" = Included; "N" = Not included, optional.
- Cable Management Arm (CMA): "Y" = Included; "N" = Not included, optional.
- Power cord:
  - "R1" = 1.5 m C13-C14 rack power cable.
  - "R2" = 2.8 m C13-C14 rack power cable.
  - "L2" = 2.8 m line cord.
  - "N" = Not included; see Power supplies and cables for the ordering information.

The following tables list the models of the SR530 server for the following regions:

- Brazil
- Latin America (except Brazil)
- Europe, Middle East, and Africa (EMEA)
- India
- Hong Kong, Taiwan, Korea
- Japan
- Association of Southeast Asian Nations (ASEAN)
- Australia and New Zealand

Table 4. SR530 server models: Brazil

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Brazil													
7X08A0A1BR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
TopSeller models - Brazil													
7X08100QBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x SATA AHCI	4 / 4 SS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A0A2BR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
7X08A09YBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09ZBR	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0APBR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 5. SR530 server models: Latin America (except Brazil)

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
TopSeller models - Latin America (except Brazil)													
7X08A09WLA	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09XLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0AQLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	Y	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 6. SR530 server models: EMEA

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - EMEA													
7X08A0ACEA	1x 3206R 8C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	R2
7X08A075EA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AZEA	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	None	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	N	R2
7X08A0ADEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AHEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A078EA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A06WEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A07FEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AEEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AJEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A07CEA	1x 4214 12C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AKEA	1x 4214R 12C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A070EA	1x 4216 16C 100W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0ALEA	1x 5218R 20C 125W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 7. SR530 server models: India

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - India													
7X08A08TSG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07USG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A07WSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A084SG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07YSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A079SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06VSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07SSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07JSG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ASG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08PSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A098SG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A077SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A095SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07RSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08VSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08WSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06USG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A094SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A089SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ESG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08KSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 8. SR530 server models: Hong Kong, Taiwan, Korea

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Hong Kong, Taiwan, Korea													
7X08A09CCN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085CN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08100VCN	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	Y	N	Y
7X08A071CN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YCN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09BCN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080CN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CCN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A082CN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09DCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07NCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A088CN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GCN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A087CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08MCN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092CN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06XCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07KCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 9. SR530 server models: Japan

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Japan													
7X08A0AWJP	1x 5218R 20C 125W 2.1GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
TopSeller models - Japan													
7X08A08AJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08DJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08EJP	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07HJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08SJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08QJP	1x 4214 12C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07QJP	1x 4215 8C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07LJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07MJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08HJP	1x 5215 10C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08FJP	1x 5217 8C 115W 3.0GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08YJP	1x 5218 16C 125W 2.3GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A090JP	1x 5220 18C 125W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08UJP	1x 5222 4C 105W 3.8GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A096JP	1x 6230 20C 125W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A0AXJP	1x 3206R 8C 85W 1.9GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AYJP	1x 4210R 10C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AVJP	1x 4214R 12C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 10. SR530 server models: ASEAN

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - ASEAN													
7X08A099SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A086SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A081SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ZSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A083SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A093SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07VSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ESG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RSG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A073SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A097SG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07PSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07TSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09FSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A091SG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 11. SR530 server models: Australia and New Zealand

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Australia and New Zealand (1-year warranty)													
7X07A00VAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	None	No bays / 8 HS SFF	Open bay	Open slot	None	1x 550W	S	Y	Y	N	R2
Relationship models - Australia and New Zealand (3-year warranty)													
7X08A099AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A071AU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YAU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XAU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080AU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A0B0AU	1x 4216 16C 100W 2.1GHz	1x 32GB(x4) 2933MHz	1x RAID 930-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W Platinum	E	Y	Y	N	Y
7X08A07VAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07EAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076AU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BAU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LAU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092AU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A06XAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
TopSeller models - Australia and New Zealand (3-year warranty)													
7X08A09GAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09HAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09LAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09KAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09NAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09MAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09JAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Processors

The SR530 server supports one or two Intel Xeon Bronze, Silver, Gold, or Platinum processors of up to 125 W TDP. The following table lists the specifications of the processors for the SR530 server.

Processor specifications table abbreviations:

- UPI: Ultra Path Interconnect
- TDP: Thermal Design Power
- HT: Hyper-Threading
- TB: Turbo Boost 2.0
- VT-x: Virtualization Technology
- VT-d: Virtualization Technology for Directed I/O
- SST-PP: Speed Select Technology - Performance Profile
- FMA: Fused-Multiply Add (AVX-512)
- RAS: Reliability, Availability, and Serviceability
    - Std: Standard RAS
    - Adv: Advanced RAS

Table 12. Processor specifications

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
Intel Xeon Bronze processors														
3204	6 / 6	1.9 / 1.9 GHz	8.25 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	Std

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
3206R	8 / 8	1.9 / 1.9 GHz	11 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	
Intel Xeon Silver processors														
4208	8 / 16	2.1 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4209T	8 / 16	2.2 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	70 W	Y	Y	Y	Y	N	1	Std
4210	10 / 20	2.2 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4210R	10 / 20	2.4 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4214R	12 / 24	2.4 / 3.5 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214Y	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	Y	1	Std
	10 / 20	2.3 / 3.2 GHz												
	8 / 16	2.4 / 3.2 GHz												
4215	8 / 16	2.5 / 3.5 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4216	16 / 32	2.1 / 3.2 GHz	22 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
Intel Xeon Gold processors														
5215	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	1 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5215L	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	4.5 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5217	8 / 16	3.0 / 3.7 GHz	11 MB	2666 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	1	Adv
5218	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218B	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218R	20 / 40	2.1 / 4.0 GHz	27.5 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218T	16 / 32	2.1 / 3.8 GHz	22 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5220	18 / 36	2.2 / 3.9 GHz	24.75 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220S	18 / 36	2.7 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220T	18 / 36	1.9 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5222	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv
6209U	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	N/A	125 W	Y	Y	Y	Y	N	2	Adv
6222V	20 / 40	1.8 / 3.6 GHz	27.5 MB	2400 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	2	Adv
6226	12 / 24	2.7 / 3.7 GHz	19.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230N	20 / 40	2.3 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230T	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6238T	22 / 44	1.9 / 3.7 GHz	30.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
Intel Xeon Platinum processors														
8253	16 / 32	2.2 / 3.0 GHz	22 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
8256	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv

Configuration notes:

- The Intel Xeon Gold 5218 and 5218B processors have similar specifications; however, they use different silicon designs and cannot be mixed in the same system.
- The processors that support SST-PP offer three distinct operating points that are defined by a core count with a base speed associated with that core count. The operating point is static, it is selected during the boot process and cannot be changed at runtime.

For the SR530 server models that come with one processor, the second processor can be ordered, if required (see the following table for ordering information). The second processor must be of the same model as the first processor. The second processor option includes a processor and a heatsink; two additional system fans are not included and need to be purchased with the second processor (see Cooling for details).

Table 13. Processor options

Description	Part number	Feature code*
Intel Xeon Bronze processors		
SR530/SR570/SR630 Intel Xeon Bronze 3204 6C 85W 1.9GHz Processor w/o FAN	4XG7A37939	B4HU
SR530/SR570/SR630 Intel Xeon Bronze 3206R 8C 85W 1.9GHz Processor w/o FAN	4XG7A37990	B7N3
Intel Xeon Silver processors		
SR530/SR570/SR630 Intel Xeon Silver 4208 8C 85W 2.1GHz Processor w/o FAN	4XG7A37936	B4HT
SR530/SR570/SR630 Intel Xeon Silver 4209T 8C 70W 2.2GHz Processor w/o FAN	4XG7A37945	B4P4
SR530/SR570/SR630 Intel Xeon Silver 4210 10C 85W 2.2GHz Processor w/o FAN	4XG7A37933	B4HS
SR530/SR570/SR630 Intel Xeon Silver 4210R 10C 100W 2.4GHz Processor w/o FAN	4XG7A37988	B7N5
SR530/SR570/SR630 Intel Xeon Silver 4214 12C 85W 2.2GHz Processor w/o FAN	4XG7A37930	B4HR
SR530/SR570/SR630 Intel Xeon Silver 4214R 12C 100W 2.4GHz Processor w/o FAN	4XG7A37987	B7N6
SR530/SR570/SR630 Intel Xeon Silver 4214Y 12/10/8C 85W 2.2GHz Processor w/o FAN	4XG7A37942	B4NW
SR530/SR570/SR630 Intel Xeon Silver 4215 8C 85W 2.5GHz Processor w/o FAN	4XG7A37927	B4HQ
SR530/SR570/SR630 Intel Xeon Silver 4216 16C 100W 2.1GHz Processor w/o FAN	4XG7A37924	B4HP
Intel Xeon Gold processors		
SR530/SR570/SR630 Intel Xeon Gold 5215 10C 85W 2.5GHz Processor w/o FAN	4XG7A37917	B4HN
SR530/SR570/SR630 Intel Xeon Gold 5215L 10C 85W 2.5GHz Processor w/o FAN	4XG7A37911	B4P9
SR530/SR570 Intel Xeon Gold 5217 8C 115W 3.0GHz Processor w/o FAN	4XG7A37921	B4HM
SR530/SR570/SR630 Intel Xeon Gold 5218 16C 125W 2.3GHz Processor w/o FAN	4XG7A37896	B4HL
SR530/SR570/SR630 Intel Xeon Gold 5218B 16C 125W 2.3GHz Processor w/o FAN	4XG7A37959	B6BS
SR530/SR570/SR630 Intel Xeon Gold 5218R 20C 125W 2.1GHz Processor w/o FAN	4XG7A63296	BAZS
SR530/SR570 Intel Xeon Gold 5218T 16C 105W 2.1GHz Processor w/o FAN	4XG7A38017	B4P3
SR530/SR570/SR630 Intel Xeon Gold 5220 18C 125W 2.2GHz Processor w/o FAN	4XG7A37893	B4HK
SR530/SR570/SR630 Intel Xeon Gold 5220S 18C 125W 2.7GHz Processor w/o FAN	4XG7A38018	B6CW
SR530/SR570 Intel Xeon Gold 5220T 18C 105W 1.9GHz Processor w/o FAN	4XG7A38004	B6CQ
SR530/SR570 Intel Xeon Gold 5222 4C 105W 3.8GHz Processor w/o FAN	4XG7A37953	B5S1
Intel Xeon Gold 6209U 20C 125W 2.1GHz Processor	None**	B6CX
SR530/SR570/SR630 Intel Xeon Gold 6222V 20C 115W 1.8GHz Processor w/o FAN	4XG7A38022	B6CV
SR530/SR570/SR630 Intel Xeon Gold 6226 12C 125W 2.7GHz Processor w/o FAN	4XG7A38020	B6CL
SR530/SR570/SR630 Intel Xeon Gold 6230 20C 125W 2.1GHz Processor w/o FAN	4XG7A37890	B4HJ
SR530/SR570 Intel Xeon Gold 6230N 20C 125W 2.3GHz Processor w/o FAN	4XG7A38029	B5RY
SR530/SR570 Intel Xeon Gold 6230T 20C 125W 2.1GHz Processor w/o FAN	4XG7A38007	B6CP
SR530/SR570 Intel Xeon Gold 6238T 22C 125W 1.9GHz Processor w/o FAN	4XG7A37908	B4P2
Intel Xeon Platinum processors		
SR530/SR570/SR630 Intel Xeon Platinum 8253 16C 125W 2.2GHz Processor w/o FAN	4XG7A37899	B5RZ
SR530/SR570 Intel Xeon Platinum 8256 4C 105W 3.8GHz Processor w/o FAN	4XG7A37949	B5S2

* For CTO configurations, the feature code represents a processor, and fans and heatsinks are derived by the configuration tool.
** Factory-installed only; no field upgrade. Supported in the uniprocessor configurations only.

Memory

The SR530 server supports up to 6 TruDDR4 memory RDIMMs when one processor is installed and up to 12 RDIMMs when two processors are installed for a total of up to 768 GB of memory capacity (up to 384 TB per processor). Each processor has six memory channels, and there is a one DIMM per channel.

Lenovo TruDDR4 memory uses the highest-quality components sourced from Tier 1 DRAM suppliers and only memory that meets strict requirements is selected. It is compatibility tested and tuned on every ThinkSystem server to maximize performance and reliability.

TruDDR4 memory has a unique signature programmed into the DIMM, which enables Lenovo servers to verify whether the memory installed is qualified and supported. Lenovo qualified and supported TruDDR4 memory is covered by Lenovo warranty, and service and support provided worldwide.

The following memory protection technologies are supported by the processor's integrated memory controllers:

- ECC
- SDDC (for x4-based memory DIMMs)
- ADDDC (for x4-based memory DIMMs; Gold and Platinum processors only)
- Memory mirroring
- Memory rank sparing
- Patrol scrubbing
- Demand scrubbing

The following table lists memory options available for the SR530 server.

Table 14. Memory options

Description	Part number	Feature code	Maximum quantity*
RDIMMs - 2933 MHz			
ThinkSystem 8GB TruDDR4 2933MHz (1Rx8 1.2V) RDIMM	4ZC7A08706	B4H1	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (1Rx4 1.2V) RDIMM	4ZC7A08707	B4LY	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (2Rx8 1.2V) RDIMM	4ZC7A08708	B4H2	6 / 12
ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08709	B4H3	6 / 12
ThinkSystem 64GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08710	B4H4	6 / 12
RDIMMs - 2666 MHz			
ThinkSystem 16GB TruDDR4 2666 MHz (1Rx4 1.2V) RDIMM	7X77A01302	AUNB	6 / 12
ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM	7X77A01303	AUNC	6 / 12
ThinkSystem 32GB TruDDR4 2666 MHz (2Rx4 1.2V) RDIMM	7X77A01304	AUND	6 / 12

* The maximum quantity shown is with one processor / two processors.

Configuration notes:

- All RDIMMs in the server operate at the same speed, which is determined as the lowest value of:
  - RDIMM rated speed (2666 MHz or 2933 MHz).
  - Memory speed supported by the specific processor (2133 MHz, 2400 MHz, 2666 MHz, or 2933 MHz).

  Note: Maximum memory speed can be achieved when Max performance mode is enabled in UEFI.
- Mixing RDIMMs of different ranks (single- or dual-rank), DRAM chip types (x4 or x8), speeds (2666 MHz or 2933 MHz), and capacities (8 GB, 16 GB, 32 GB, or 64 GB) is supported in the independent channel mode (the default operational mode).
- For server configurations with memory protection, the following rules apply:
  - Single Device Data Correction (SDDC) works only in the independent channel mode and supports only x4-based memory DIMMs.
  - Adaptive Double Device Data Correction (ADDDC) works with x4-based memory DIMMs and requires two DIMM ranks per channel, Intel Xeon Gold or Platinum processors, and the Closed Page memory access mode.
  - If memory mirroring is used, then DIMMs must be installed in quantities of 2 or 4 per processor for mirroring across two memory channels, or in quantities of 3 or 6 per processor for mirroring across three memory channels. Mixing two- and three-channel mirroring in the server is allowed (one processor uses two-channel mirroring, and another processor uses three-channel mirroring). All DIMMs in the server must be identical in type and size.
  - If memory rank sparing is used, then a minimum of two ranks must be installed per populated channel (a least one dual-rank or quad-rank DIMM; single-rank DIMMs are not supported). With rank sparing, one rank in each populated channel is reserved as spare memory for other ranks on the same channel. All DIMMs in the server must be identical in type and size.
  - SDDC, memory mirroring, and memory rank sparing modes are mutually exclusive. Only one operational memory mode can be enabled on the server.

Internal storage

The SR530 server supports the following internal drive bay configurations:

1. 4 LFF SATA Simple Swap drive bays
2. 4 LFF SAS/SATA hot-swap drive bays
3. 8 SFF SAS/SATA hot-swap drive bays

In addition, the SR530 server models can be configured with one or two internal M.2 SATA SSDs. The server also supports configurations without drive bays.

The following figure shows the internal drive bay configurations.

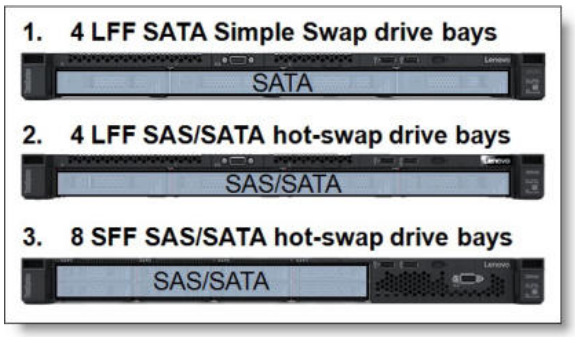


Figure 6. Internal drive bay configurations

The following table lists the internal storage options for the SR530 server.

Table 15. Internal storage options

Description	Part number	Feature code	Maximum quantity
Factory-installed backplane kits			
ThinkSystem 1U 3.5" SATA/SAS 4-Bay Backplane	None*	AUW8	1
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane	None*	AUWB	1
Backplane kit field upgrade options			
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane Kit	7XH7A05896	None**	1
M.2 enablement kits			
ThinkSystem M.2 Enablement Kit	7Y37A01092	AUMU	1
ThinkSystem M.2 with Mirroring Enablement Kit	7Y37A01093	AUMV	1

* These backplane kits can be factory-installed in standard or custom (CTO or Special Bid) models, and they might not have an option part number assigned.
** Field upgrade only; used for upgrading models without any drive bays to 8x 2.5" SAS/SATA hot-swap drive bays.

M.2 Enablement Kit configuration notes:

- The M.2 Enablement Kit (7Y37A01092) supports one M.2 SATA SSD which is connected to the SATA port on the Intel Platform Controller Hub (PCH).
- The M.2 with Mirroring Enablement Kit (7Y37A01093) is connected to the Intel PCH via the PCIe link, and the kit supports two M.2 SATA SSDs that can be configured in a RAID-1 or RAID-0 drive group, or they can operate as two separate drives.

The following tables list supported internal storage configurations with the SAS/SATA backplanes.

Table 16. Internal storage configurations

Drive bay configuration	Backplane kit type and quantity		Storage controller type and quantity*
	4x 3.5" SATA/SAS	8x 2.5" SATA/SAS	
4x 3.5" chassis (Feature code AV0T)			
4x 3.5-in. SATA Simple Swap	0	0	Onboard AHCI (non-RAID) / Intel RSTe (RAID) (4)
4x 3.5-in. SAS/SATA hot-swap	1	0	1x RAID 530-8i/730-8i 1GB (4)
			1x RAID 730-8i 2GB/930-8i (4)
			1x 430-8i HBA (4)
8x 2.5" chassis (Feature code AV0S)			
8x 2.5-in. SAS/SATA hot-swap	0	1	1x RAID 530-8i/730-8i 1GB (8)
			1x RAID 730-8i 2GB/930-8i/930-16i (8)
			1x 430-8i HBA (8)

* The number in brackets (x) specifies the quantity of drive bays connected to each of the controllers.

Configuration note: Models without any drive bays are based on the 8x 2.5" chassis (feature code AV0S), and they support adding drive bays by using the 2.5" 8-drive backplane kit (7XH7A05896).

Controllers for internal storage

The following table lists the storage controllers and options for internal storage of the SR530 server.

Table 17. RAID controllers and HBAs for internal storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
6 Gbps SATA controllers				
Onboard AHCI (non-RAID) / Intel RSTe (RAID)	Onboard*	Onboard*	1	-
12 Gb SAS/SATA RAID controllers				
ThinkSystem RAID 530-8i PCIe 12Gb Adapter	7Y37A01082	AUNG	1	1
ThinkSystem RAID 730-8i 1GB Cache PCIe 12Gb Adapter	7Y37A01083	AUNH	1	1
ThinkSystem RAID 730-8i 2GB Flash PCIe 12Gb Adapter	4Y37A09722	B4RQ	1	1
ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter	7Y37A01084	AUNJ	1	1
ThinkSystem RAID 930-16i 4GB Flash PCIe 12Gb Adapter	7Y37A01085	AUNK	1	1
ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter	4Y37A09721	B31E	1	1
12 Gb SAS/SATA non-RAID HBAs				
ThinkSystem 430-8i SAS/SATA 12Gb HBA	7Y37A01088	AUNL	1	1

* The onboard SATA controller integrated into the Intel C622 Platform Controller Hub (PCH) supports non-RAID (JBOD) AHCI mode or a hardware-assist, software RAID feature (Intel Rapid Storage Technology Enterprise [RSTe]).

Configuration note: Low profile SAS RAID controllers and HBAs for internal storage are supported in the PCIe x8 slot 1 supplied by the riser card 1.

The following table summarizes features of supported SAS/SATA storage controllers.

Table 18. Storage controller features and specifications (LP = Low profile, FHHL = Full-height half-length)

Feature	Intel RSTe	RAID 530-8i	RAID 730-8i 1GB	RAID 730-8i 2GB	RAID 930-8i	RAID 930-16i	430-8i HBA
Form factor	Onboard	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP
SAS controller	None	SAS3408	SAS3108	SAS3108	SAS3508	SAS3516	SAS3408
Host interface	PCH	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	6 Gb SATA	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	8	8	8	16	8
Connector type	SATA x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4
Number of connectors	2	2	2	2	2	4	2
Drive interface	SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD	HDD, SSD, SED	HDD, SSD	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED*
Hot-swap drive support	No	Yes	Yes	Yes	Yes	Yes	Yes
Number of drives	8	8	8	8	8	16^	8
RAID levels	0/1/10/5	0/1/10/5/50	0/1/10/5/50	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	None
JBOD mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cache	None	None	1 GB	2 GB	2 GB	4 GB; 8 GB	None
Cache protection	None	None	None	Flash backup (Included)	Flash backup (Included)	Flash backup (Included)	None
SED key management (SafeStore)	No	Yes	No	Yes	Yes	Yes	No
SSD I/O acceleration (FastPath)	No	Yes	No	Yes	Yes	Yes	No
SSD Caching (CacheCade Pro 2.0)	No	No	No	No	No**	No**	No
Consistency check	Yes	Yes	Yes	Yes	Yes	Yes	No
Patrol read	Yes	Yes	Yes	Yes	Yes	Yes	No
Online capacity expansion	Yes	Yes	Yes	Yes	Yes	Yes	No
Online RAID level migration	Yes	Yes	Yes	Yes	Yes	Yes	No
Global Hot Spare	Yes	Yes	Yes	Yes	Yes	Yes	No
Auto-rebuild	Yes	Yes	Yes	Yes	Yes	Yes	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
^ Up to 8 drives is supported by the RAID 930-16i in the SR530 server.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

Important: The onboard Intel RSTe is not supported by virtualization hypervisors, including VMware vSphere (ESXi), Linux KVM, Xen, and Microsoft Hyper-V.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Drives for internal storage

The following tables list the hard disk drive and solid-state drive options for the internal disk storage of the server.

2.5-inch hot-swap drives:

- 2.5-inch hot-swap 12 Gb SAS HDDs
- 2.5-inch hot-swap 6 Gb SATA HDDs
- 2.5-inch hot-swap 12 Gb SAS SSDs
- 2.5-inch hot-swap 6 Gb SATA SSDs

3.5-inch hot-swap drives:

- 3.5-inch hot-swap 12 Gb SAS HDDs
- 3.5-inch hot-swap 6 Gb SATA HDDs
- 3.5-inch hot-swap 12 Gb SAS SSDs
- 3.5-inch hot-swap 6 Gb SATA SSDs

Simple-swap drives:

- 3.5-inch simple-swap 6 Gb SATA HDDs

M.2 drives:

- M.2 SATA drives

M.2 drive support: The use of M.2 drives requires an additional adapter as described in the Internal storage section.

Table 19. 2.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00024	AULY	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00025	AULZ	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00026	AUM0	ThinkSystem 2.5" 900GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00027	AUM1	ThinkSystem 2.5" 1.2TB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00028	AUM2	ThinkSystem 2.5" 1.8TB 10K SAS 12Gb Hot Swap 512e HDD	8
7XB7A00069	B0YS	ThinkSystem 2.5" 2.4TB 10K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00021	AULV	ThinkSystem 2.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00022	AULW	ThinkSystem 2.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00023	AULX	ThinkSystem 2.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00034	AUM6	ThinkSystem 2.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00035	AUM7	ThinkSystem 2.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
2.5-inch hot-swap SED HDDs - 12 Gb SAS 10K			
7XB7A00030	AUM4	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD SED	8
7XB7A00031	AUM5	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD SED	8

Table 20. 2.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00036	AUUE	ThinkSystem 2.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	8
7XB7A00037	AUUJ	ThinkSystem 2.5" 2TB 7.2K SATA 6Gb Hot Swap 512e HDD	8

Table 21. 2.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17062	B8HU	ThinkSystem 2.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17063	B8J4	ThinkSystem 2.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17064	B8JD	ThinkSystem 2.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17065	B8JA	ThinkSystem 2.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13654	B4A1	ThinkSystem 2.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13655	B4A2	ThinkSystem 2.5" PM1645 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A38175	B91A	ThinkSystem 2.5" PM1643a 960GB Entry SAS 12Gb Hot Swap SSD	8
4XB7A38176	B91B	ThinkSystem 2.5" PM1643a 1.92TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17054	B91C	ThinkSystem 2.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17055	B91D	ThinkSystem 2.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17056	BC4R	ThinkSystem 2.5" PM1643a 15.36TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A13645	B4A7	ThinkSystem 2.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	8

Table 22. 2.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17087	B8J1	ThinkSystem 2.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17088	B8HY	ThinkSystem 2.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17089	B8J6	ThinkSystem 2.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17090	B8JE	ThinkSystem 2.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17091	B8J7	ThinkSystem 2.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13633	B49L	ThinkSystem 2.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13634	B49M	ThinkSystem 2.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13635	B49N	ThinkSystem 2.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13636	B49P	ThinkSystem 2.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13637	B49Q	ThinkSystem 2.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10237	B488	ThinkSystem 2.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10239	B48A	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10240	B48B	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10241	B48C	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			

Part number	Feature	Description	Maximum supported
4XB7A38271	BCTC	ThinkSystem 2.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38272	BCTD	ThinkSystem 2.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38273	BCTE	ThinkSystem 2.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38274	BCTF	ThinkSystem 2.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38275	BCTG	ThinkSystem 2.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17075	B8HV	ThinkSystem 2.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17076	B8JM	ThinkSystem 2.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17077	B8HP	ThinkSystem 2.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17078	B8J5	ThinkSystem 2.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17079	B8JP	ThinkSystem 2.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17080	B8J2	ThinkSystem 2.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38185	B9AC	ThinkSystem 2.5" 5210 960GB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38144	B7EW	ThinkSystem 2.5" 5210 1.92TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38145	B7EX	ThinkSystem 2.5" 5210 3.84TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38146	B7EY	ThinkSystem 2.5" 5210 7.68TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A10247	B498	ThinkSystem 2.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10248	B499	ThinkSystem 2.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10249	B49A	ThinkSystem 2.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13622	B49B	ThinkSystem 2.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13623	B49C	ThinkSystem 2.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10195	B34H	ThinkSystem 2.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10196	B34J	ThinkSystem 2.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10197	B34K	ThinkSystem 2.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10198	B34L	ThinkSystem 2.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10199	B34M	ThinkSystem 2.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10200	B4D2	ThinkSystem 2.5" PM883 7.68TB Entry SATA 6Gb Hot Swap SSD	8
7SD7A05740	B0Z0	ThinkSystem 2.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10155	B2X4	ThinkSystem 2.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10157	B2X6	ThinkSystem 2.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	8

Table 23. 3.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00063	B1JJ	ThinkSystem 3.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	4
3.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00038	AUU2	ThinkSystem 3.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00039	AUU3	ThinkSystem 3.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00040	AUUC	ThinkSystem 3.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00041	AUU4	ThinkSystem 3.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00042	AUU5	ThinkSystem 3.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00043	AUU6	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00044	AUU7	ThinkSystem 3.5" 6TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00045	B0YR	ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00046	AUUG	ThinkSystem 3.5" 10TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00067	B117	ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13906	B496	ThinkSystem 3.5" 14TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13911	B7EZ	ThinkSystem 3.5" 16TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A38266	BCFP	ThinkSystem 3.5" 18TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap SED HDDs - 12 Gb NL SAS			
7XB7A00047	AUUH	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD FIPS	4

Table 24. 3.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00049	AUUF	ThinkSystem 3.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00050	AUUD	ThinkSystem 3.5" 2TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00051	AUU8	ThinkSystem 3.5" 4TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00052	AUUA	ThinkSystem 3.5" 6TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00053	AUU9	ThinkSystem 3.5" 8TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00054	AUUB	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00068	B118	ThinkSystem 3.5" 12TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13907	B497	ThinkSystem 3.5" 14TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13914	B7F0	ThinkSystem 3.5" 16TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A38130	BCFH	ThinkSystem 3.5" 18TB 7.2K SATA 6Gb Hot Swap 512e HDD	4

Table 25. 3.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17066	B8HT	ThinkSystem 3.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17043	B8JN	ThinkSystem 3.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17067	B8JK	ThinkSystem 3.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17068	B8JG	ThinkSystem 3.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A13658	B4A4	ThinkSystem 3.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A17058	B91E	ThinkSystem 3.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A17059	BEVK	ThinkSystem 3.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A13649	B4A8	ThinkSystem 3.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	4

Table 26. 3.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17096	B8JL	ThinkSystem 3.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17097	B8JF	ThinkSystem 3.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17098	B8J0	ThinkSystem 3.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17099	B8HR	ThinkSystem 3.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17100	B8HX	ThinkSystem 3.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13639	B49R	ThinkSystem 3.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13640	B49S	ThinkSystem 3.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13641	B49T	ThinkSystem 3.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13642	B49U	ThinkSystem 3.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13643	B49V	ThinkSystem 3.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10242	B48D	ThinkSystem 3.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10244	B48F	ThinkSystem 3.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10245	B48G	ThinkSystem 3.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10246	B48H	ThinkSystem 3.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			
4XB7A38276	BCTH	ThinkSystem 3.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38277	BCTJ	ThinkSystem 3.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38278	BCTK	ThinkSystem 3.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38279	BCTL	ThinkSystem 3.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38281	BCTM	ThinkSystem 3.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17081	B8JB	ThinkSystem 3.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17082	B8J9	ThinkSystem 3.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17083	B8JC	ThinkSystem 3.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17084	B8HZ	ThinkSystem 3.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17085	B8HQ	ThinkSystem 3.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17086	B8J3	ThinkSystem 3.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Part number	Feature	Description	Maximum supported
4XB7A13625	B49D	ThinkSystem 3.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13626	B49E	ThinkSystem 3.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13627	B49F	ThinkSystem 3.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13628	B49G	ThinkSystem 3.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13629	B49H	ThinkSystem 3.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17176	B6TM	ThinkSystem 3.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17177	B6TN	ThinkSystem 3.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17178	B6TP	ThinkSystem 3.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17179	B6JY	ThinkSystem 3.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17180	B6JZ	ThinkSystem 3.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	4
7SD7A05735	B0Z5	ThinkSystem 3.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10160	B2X9	ThinkSystem 3.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10162	B2XB	ThinkSystem 3.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Table 27. 3.5-inch simple-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch simple-swap HDDs - 6 Gb NL SATA			
7XB7A00055	AUZS	ThinkSystem 1TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00056	AUZT	ThinkSystem 2TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00057	AUZU	ThinkSystem 4TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00058	AXC7	ThinkSystem 6TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00059	AXC6	ThinkSystem 8TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00060	AXC8	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Simple Swap 512e HDD	4

Table 29. M.2 SATA drives

Part number	Feature	Description	Maximum supported
M.2 SSDs - 6 Gb SATA - Entry (<3 DWPD)			
7N47A00129	AUUL	ThinkSystem M.2 32GB SATA 6Gbps Non-Hot Swap SSD	2
7N47A00130	AUUV	ThinkSystem M.2 128GB SATA 6Gbps Non-Hot Swap SSD	2
7SD7A05703	B11V	ThinkSystem M.2 5100 480GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17071	B8HS	ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17073	B919	ThinkSystem M.2 5300 480GB SATA 6Gbps Non-Hot Swap SSD	2

Optical drives

The server supports the external USB optical drive listed in the following table.

Table 30. External optical drive

Part number	Feature code	Description
7XA7A05926	AVV8	ThinkSystem External USB DVD RW Optical Disk Drive

The drive is based on the Lenovo Slim DVD Burner DB65 drive and supports the following formats: DVD-RAM, DVD-RW, DVD+RW, DVD+R, DVD-R, DVD-ROM, CD-RW, CD-R, CD-ROM.

I/O expansion

The SR530 server supports one LOM card slot and up to three PCIe slots with different riser cards installed into two riser sockets on the system planar (one riser socket supports installation of one riser card).

The slot form factors are as follows:

- LOM card slot
- Slot 1: PCIe 3.0 x8; low profile
- Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length
- Slot 3: PCIe 3.0 x8 or x16; low profile

Configuration notes:

- PCIe x16 slot 3 requires the second processor to be installed.
- The COM Port Upgrade Kit is installed in place of one of the PCIe slots 1, 2, or 3.

The locations of the PCIe slots are shown in the following figure.

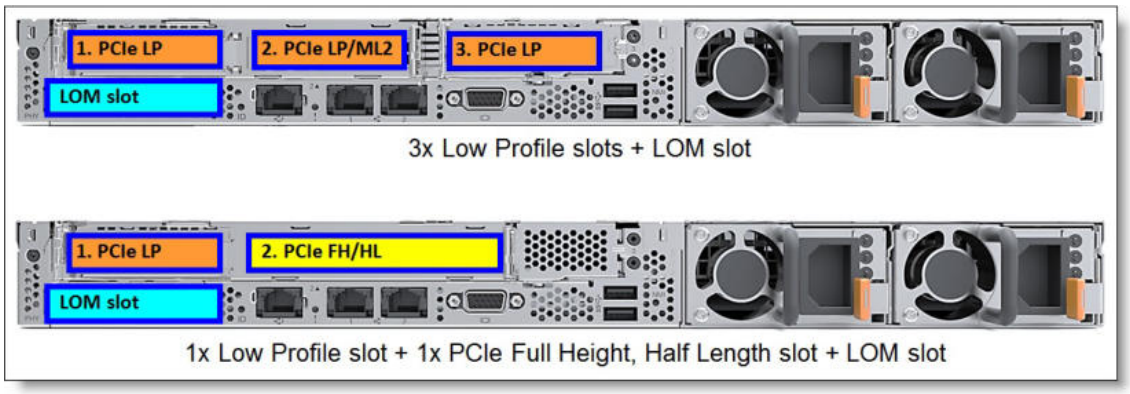


Figure 7. Slot locations

Riser 1 supplies slots 1 and 2, and Riser 2 supplies slot 3. The slots that are available for use depend on the number of riser cards that are installed and whether the second processor is installed, as shown in the following table.

Table 31. Slots available for use

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
None	None	LOM	-
None	PCIe x8	LOM, 3	-
None	PCIe x16	LOM	3
PCIe x8/x16 or PCIe x8/x8ML2	None	LOM, 1, 2	-
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x8	LOM, 1, 2, 3	-

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x16	LOM, 1, 2	3

The following table lists available PCIe riser card options.

Table 32. PCIe riser cards and miscellaneous options

Description	Part number	Feature code	Maximum quantity
x8 Riser Card 1 options (Riser card 1 supplies slots 1 and 2)			
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+LP Riser 1 Kit	7XH7A02682	AUWC	1
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+FH Riser 1 Kit	7XH7A05893	None*	1
ThinkSystem SR530/SR570 x8/x8ML2 PCIe LP+LP Riser 1 Kit	7XH7A05892	AV0X	1
Riser Card 2 option (Riser card 2 supplies slot 3)			
ThinkSystem SR530/SR570/SR630 x16 PCIe LP Riser 2 Kit	7XH7A02685	AUWA	1
ThinkSystem SR530/SR570 x8 PCIe LP Riser 2 Kit	7XH7A05891	AV0W	1
Serial port upgrade kit			
ThinkSystem COM Port Upgrade Kit	7Z17A02577	AUSL	1

* The LP+FH Riser 1 can be factory-installed by selecting the feature codes AUWC (LP+LP Riser 1) and AUWS (LP+FH Bracket).

The COM Port Upgrade Kit, part number 7Z17A02577, is used for mounting the external serial port on the rear of the SR530. This option includes the bracket and the cable. The COM Port option is mounted in place of one of the PCIe slots 1, 2, or 3.

Network adapters

The SR530 server has two onboard 1 GbE ports (no 10/100 Mb support) and up to two additional onboard 1/10 GbE network ports (no 10/100 Mb support) with optional LOM cards. Onboard ports and LOM cards use the Intel Ethernet Connection X722 1/10 GbE technology integrated into the Intel C622 Platform Controller Hub (PCH). The server also supports ML2 adapters that are installed in the custom ML2 slot provided by an ML2 riser card. The LOM cards support direct connectivity to the XClarity Controller via the Network Controller Sideband Interface (NSCI) for out-of-band systems management.

Note: ML2 network adapters do not support NSCI when used in the SR530 server.

The integrated Intel Ethernet Connection X722 has the following features:

- Two 1 Gb Ethernet ports (no 10/100 Mb Ethernet support)
- Two 1/10 Gb Ethernet capable ports (no 10/100 Mb Ethernet support)
- NIC Teaming (load balancing and failover)
- Data Center Bridging
- iWARP (RDMA over IP)
- VMDq and SR-IOV virtualization (10 Gb speeds only, 4 PFs, 128 VFs per device)
- IEEE 802.1q Virtual Local Area Networks (VLANs)
- NVGRE, VXLAN, IPinGRE, and MACinUDP network virtualization
- IEEE 802.1Qbg Edge Virtual Bridging
- TCP, IP, and UDP checksum offload
- Large Send Offload (LSO) and Generic Send Offload (GSO)
- Receive Side Scaling (RSS) for TCP and UDP traffic
- Jumbo frames up to 9.5 Kbytes

The following table lists the network adapters that are supported with the SR530 server.

Table 33. Network adapters

Description	Part number	Feature code	Max qty	I/O slots supported
LOM cards - 1 Gb Ethernet				
ThinkSystem 1Gb 2-port RJ45 LOM	7ZT7A00544	AUKG	1	LOM slot
LOM cards - 10 Gb Ethernet				
ThinkSystem 10Gb 2-port Base-T LOM	7ZT7A00548	AUKL	1	LOM slot
ThinkSystem 10Gb 2-port SFP+ LOM	7ZT7A00546	AUKJ	1*	LOM slot
ML2 adapters - 10 Gb Ethernet				
Broadcom NX-E ML2 10Gb 2-Port Base-T Ethernet Adapter	7ZT7A00497	AUKQ	1	2 (ML2)
Emulex VFA5.2 ML2 Dual Port 10GbE SFP+ Adapter	00AG560	AT7U	1*	2 (ML2)
Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	01CV770	AU7Z	1*	2 (ML2)
Intel X710-DA2 ML2 2x10GbE SFP+ Adapter	00JY940	ATRH	1*	2 (ML2)
PCIe Low Profile adapters - 1 Gb Ethernet				
Broadcom 5720 1GbE RJ45 2-Port PCIe Ethernet Adapter	7ZT7A00482	AUZX	3	1, 2, 3
Broadcom 5719 1GbE RJ45 4-Port PCIe Ethernet Adapter	7ZT7A00484	AUZV	3	1, 2, 3
ThinkSystem I350-F1 PCIe 1Gb 1-Port SFP Ethernet Adapter	7ZT7A00533	AUZZ	3	1, 2, 3
ThinkSystem I350-T2 PCIe 1Gb 2-Port RJ45 Ethernet Adapter	7ZT7A00534	AUZY	3	1, 2, 3
ThinkSystem I350-T4 PCIe 1Gb 4-Port RJ45 Ethernet Adapter	7ZT7A00535	AUZW	3	1, 2, 3
PCIe Low Profile adapters - 10 Gb Ethernet				
Broadcom 57416 10GBASE-T 2-Port PCIe Ethernet Adapter	7ZT7A00496	AUKP	3	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ PCIe Adapter	00AG570	AT7S	3*	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	00AG580	AT7T	3*	1, 2, 3
Intel X550-T2 Dual Port 10GBase-T Adapter	00MM860	ATPX	3	1, 2, 3
Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter	7ZT7A00537	AUKX	3*	1, 2, 3
QLogic QL41134 PCIe 10Gb 4-Port Base-T Ethernet Adapter	4XC7A08225	B31G	3	1, 2, 3
PCIe Full Height adapters - 10 Gb Ethernet				
Emulex OCe14104B-NX PCIe 10Gb 4-Port SFP+ Ethernet Adapter	7ZT7A00493	AUKN	1*	2
PCIe Low Profile adapters - 25 Gb Ethernet				
Broadcom 57412 10/25GbE SFP28 1-Port PCIe Ethernet Adapter	7ZT7A00505	AUKS	3*	1, 2, 3
Broadcom 57414 10/25GbE SFP28 2-port PCIe Ethernet Adapter	4XC7A08238	B5T0	3*	1, 2, 3
PCIe Low Profile adapters - Omni-Path				
Intel OPA 100 Series Single-port PCIe 3.0 x16 HFA	00WE027	AU0B	1 / 2#*	2, 3

The maximum quantity shown is with one processor / two processors.
* The adapter comes without transceivers or cables; for ordering transceivers or cables, see the adapter product guide

Configuration notes:

- ML2 network adapters are supported in the ML2 x8 slot 2 supplied by the x8/x8ML2 Riser Card 1 (7XH7A05892).
- PCIe full-height network adapters are supported in the full-height PCIe x16 slot 2 supplied by the PCIe x8/x16 LP+FH Riser Card 1 (7XH7A05893).
- Omni-Path adapters are supported in the low profile or full-height PCIe x16 slots supplied by the riser cards 1 and 2.
- PCIe Low Profile network adapters (except Omni-Path adapters) are supported in the low profile and full-height PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

- Some adapters require supported transceivers or DAC cables to be purchased for the adapter. The maximum number of transceivers or cables that are supported per adapter equals the quantity of the adapter ports, and all adapter ports must have the same type of the transceiver or cable selected.

For more information, see the list of Product Guides in the Ethernet Adapters category:
http://lenovopress.com/servers/options/ethernet#rt=product-guide

SAS adapters for external storage

The following table lists SAS RAID controllers and HBAs for external storage attachments that are supported by the SR530 server.

Table 34. SAS RAID adapters and HBAs for external storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
12 Gbps SAS RAID adapters				
ThinkSystem RAID 930-8e 4GB Flash PCIe 12Gb Adapter	7Y37A01087	AUNQ	2	1, 2, 3
12 Gbps SAS HBAs				
ThinkSystem 430-8e SAS/SATA 12Gb HBA	7Y37A01090	AUNR	2	1, 2, 3
ThinkSystem 430-16e SAS/SATA 12Gb HBA	7Y37A01091	AUNN	2	1, 2, 3

Configuration notes:

- Low profile SAS RAID controllers and HBAs for external storage are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.
- The total quantity of the RAID 730-8i 2GB, RAID 930-8i, RAID 930-16i, and RAID 930-8e controllers in a supported combination in the server must not exceed 2 (up to 2 supercapacitors can be mounted in the server).

The following table summarizes features of supported RAID controllers and HBAs for external storage.

Table 35. Features and specifications of the RAID controllers and HBAs for external storage

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
Form factor	PCIe LP	PCIe LP	PCIe LP
SAS controller chip	SAS3516	SAS3408	SAS3416
Host interface	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	16
Connector type	SFF-8644 x4	SFF-8644 x4	SFF-8644 x4
Number of connectors	2	2	4
Drive interface	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD, SSD, SED	HDD, SSD, SED*	HDD, SSD, SED*
Hot-swap drive support	Yes	Yes	Yes
Number of devices	240	1024	1024
RAID levels	0/1/10/5/50/6/60	None	None
JBOD mode	Yes	Yes	Yes
Cache	4 GB	None	None
Cache protection	Flash backup (Included)	None	None
SED key management (SafeStore)	Yes	No	No
SSD I/O acceleration (FastPath)	Yes	No	No

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
SSD Caching (CacheCade Pro 2.0)	No**	No	No
Consistency check	Yes	No	No
Patrol read	Yes	No	No
Online capacity expansion	Yes	No	No
Online RAID level migration	Yes	No	No
Global Hot Spare	Yes	No	No
Auto-rebuild	Yes	No	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Fibre Channel host bus adapters

The following table lists Fibre Channel HBAs supported by the SR530 server.

Table 36. Fibre Channel HBAs

Description	Part number	Feature code	Maximum quantity	I/O slots supported
16 Gb Fibre Channel - PCIe				
Emulex 16Gb Gen6 FC Single-port HBA	01CV830	ATZU	3	1, 2, 3
Emulex 16Gb Gen6 FC Dual-port HBA	01CV840	ATZV	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Single-port HBA	01CV750	ATZB	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Dual-port HBA	01CV760	ATZC	3	1, 2, 3
8 Gb Fibre Channel - PCIe (available only in PRC and Asia Pacific)				
Emulex LPe12002-M8-L PCIe 8Gb 2-Port SFP+ FC HBA	4XC7A08221	B0X0	3	1, 2, 3
Emulex LPe12000-M8-L PCIe 8Gb 1-Port SFP+ FC HBA	4XC7A08220	B0WZ	3	1, 2, 3

Configuration note: FC HBAs are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

For more information, see the list of Product Guides in the Host bus adapters category:
http://lenovopress.com/servers/options/hba#rt=product-guide

Cooling

The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.

The following table shows additional cooling options.

Table 37. Cooling options

Description	Part number	Feature code	Maximum quantity
ThinkSystem SR530 FAN Option Kit	4F17A12354	AV0N	1

Configuration note: The SR530 FAN Option Kit (4F17A12354) includes two system fans that are required for field upgrades that add a second processor to the server. If two processors are selected in the initial server configurations, two fans for the second processor are derived by the configurator.

Power supplies and cables

The SR530 server supports up to two redundant power supplies and is capable of N+N redundancy depending on the configuration. A second power supply can be added to the models that come with one power supply. The following table lists the power supply options.

Table 38. Power supplies

Description	Part number	Feature code	Maximum quantity
ThinkSystem 550W (230V/115V) Platinum Hot-Swap Power Supply	7N67A00882	AVV6	2
ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply	7N67A00883	AVV7	2
ThinkSystem 750W (230V) Titanium Hot-Swap Power Supply	7N67A00884	AVV5	2

Configuration notes:

- Minimum of 1 and maximum of 2 power supplies per system.
- If 2 are installed, power supplies must be identical.
- Power supplies support AC (Worldwide) and HVDC (PRC only) power sources.

Important: The Standalone Solution Configuration Tool (SSCT) and Lenovo Data Center Solution Configurator (DCSC) power supply selection rules allow a subset of possible configurations due to power restrictions. Configurations that cannot be built in SSCT or DCSC due to power restrictions may still be supported. To verify support and ensure that the right power supply is chosen for optimal performance, you should always validate your server configuration using the latest version of the Lenovo Capacity Planner: http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

The SR530 server ship standard with or without a power cord (model dependent). A hot-swap power supply option ships without a power cord. The following table lists the rack power cables and line cords that can be ordered for the SR530 server.

Table 39. Power cables

Description	Part number	Feature code
Rack power cables		
1.0m, 10A/125-250V, C13 to IEC 320-C14 Rack Power Cable	00Y3043	A4VP
1.5m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7937	6201
2.0m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08369	6570
2.8m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08366	6311

Description	Part number	Feature code
2.8m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08370	6400
2.8m, 10A/100-250V, C13 to IEC 320-C20 Rack Power Cable	39Y7938	6204
4.3m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7932	6263
4.3m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08371	6583
Line cords		
Argentina 2.8m, 10A/250V, C13 to IRAM 2073 Line Cord	39Y7930	6222
Argentina 4.3m, 10A/250V, C13 to IRAM 2073 Line Cord	81Y2384	6492
Australia/New Zealand 2.8m, 10A/250V, C13 to AS/NZS 3112 Line Cord	39Y7924	6211
Australia/New Zealand 4.3m, 10A/250V, C13 to AS/NZS 3112 Line Cord	81Y2383	6574
Brazil 2.8m, 10A/250V, C13 to NBR 14136 Line Cord	69Y1988	6532
Brazil 4.3m, 10A/250V, C13 to NBR14136 Line Cord	81Y2387	6404
China 1.8m, 10A/250V, C13 to GB 2099.1 Line Cord	4L67A69954	6361
China 2.8m, 10A/250V, C13 to GB 2099.1 Line Cord	39Y7928	6210
China 4.3m, 10A/250V, C13 to GB 2099.1 Line Cord	81Y2378	6580
Denmark 2.8m, 10A/250V, C13 to DK2-5a Line Cord	39Y7918	6213
Denmark 4.3m, 10A/250V, C13 to DK2-5a Line Cord	81Y2382	6575
Europe 2.8m, 10A/250V, C13 to CEE7-VII Line Cord	39Y7917	6212
Europe 4.3m, 10A/250V, C13 to CEE7-VII Line Cord	81Y2376	6572
India 2.8m, 10A/250V, C13 to IS 6538 Line Cord	39Y7927	6269
India 4.3m, 10A/250V, C13 to IS 6538 Line Cord	81Y2386	6567
Israel 2.8m, 10A/250V, C13 to SI 32 Line Cord	39Y7920	6218
Israel 4.3m, 10A/250V, C13 to SI 32 Line Cord	81Y2381	6579
Italy 2.8m, 10A/250V, C13 to CEI 23-16 Line Cord	39Y7921	6217
Italy 4.3m, 10A/250V, C13 to CEI 23-16 Line Cord	81Y2380	6493
Japan 2.8m, 12A/125V, C13 to JIS C-8303 Line cord	46M2593	6314
Japan 2.8m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08357	5472
Japan 4.3m, 12A/125V, C13 to JIS C-8303 Line Cord	39Y7926	6335
Japan 4.3m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08362	6495
Korea 2.8m, 12A/250V, C13 to KS C8305 Line Cord	39Y7925	6219
Korea 4.3m, 12A/250V, C13 to KS C8305 Line Cord	81Y2385	6494
South Africa 2.8m, 10A/250V, C13 to SABS 164 Line Cord	39Y7922	6214
South Africa 4.3m, 10A/250V, C13 to SABS 164 Line Cord	81Y2379	6576
Switzerland 2.8m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	39Y7919	6216
Switzerland 4.3m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	81Y2390	6578
Taiwan 2.8m, 10A/125V, C13 to CNS 10917-3 Line Cord	23R7158	6386
Taiwan 2.8m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2375	6317
Taiwan 2.8m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2374	6402
Taiwan 4.3m, 10A/125V, C13 to CNS 10917-3 Line Cord	4L67A08363	AX8B
Taiwan 4.3m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2389	6531
Taiwan 4.3m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2388	6530
United Kingdom 2.8m, 10A/250V, C13 to BS 1363/A Line Cord	39Y7923	6215
United Kingdom 4.3m, 10A/250V, C13 to BS 1363/A Line Cord	81Y2377	6577
United States 2.8m, 10A/125V, C13 to NEMA 5-15P Line Cord	90Y3016	6313

Description	Part number	Feature code
United States 2.8m, 10A/250V, C13 to NEMA 6-15P Line Cord	46M2592	A1RF
United States 2.8m, 13A/125V, C13 to NEMA 5-15P Line Cord	00WH545	6401
United States 4.3m, 10A/125V, C13 to NEMA 5-15P Line Cord	4L67A08359	6370
United States 4.3m, 10A/250V, C13 to NEMA 6-15P Line Cord	4L67A08361	6373
United States 4.3m, 13A/125V, C13 to NEMA 5-15P Line Cord	4L67A08360	AX8A

Systems management

The SR530 supports the following systems management tools:

- Lenovo XClarity Controller
- Lenovo XClarity Provisioning Manager
- Lenovo XClarity Essentials
- Lenovo XClarity Administrator
- Lenovo XClarity Integrators
- Lenovo XClarity Energy Manager
- Lenovo Capacity Planner

Lenovo XClarity Controller

The SR530 server contains Lenovo XClarity Controller (XCC), which provides advanced service-processor control, monitoring, and alerting functions. XClarity Controller offers three functional levels: Standard, Advanced, and Enterprise.

By default, the SR530 server includes XClarity Controller Standard features, and it can be upgraded to Advanced or Enterprise functionality by using the Features on Demand (FoD) upgrades.

XClarity Controller Standard offers the following capabilities:

- Gathering and viewing system information and inventory
- Monitoring system status and health
- Alerting and notifications
- Event logging
- Configuring network connectivity
- Configuring security
- Updating system firmware
- Configuring server settings and devices
- Real-time power usage monitoring
- Remotely controlling server power (Power on, Power off, Restart)
- Managing FoD activation keys
- Redirecting serial console via IPMI
- Capturing the video display contents when an operating system hang condition is detected

XClarity Controller Advanced Upgrade adds the following functionality to the Standard features:

- Remotely viewing video with the following graphics resolutions:
  - Up to 1600x1200 with up to 23 bits per pixel; or
  - Up to 1920x1200 with up to 15 bits per pixel
- Remotely accessing the server using the keyboard and mouse from a remote client
- Remotely deploying an operating system
- Syslog alerting
- Redirecting serial console via SSH
- Displaying graphics for real-time and historical power usage data and temperature

XClarity Controller Enterprise Upgrade adds the following functionality to the Advanced features:

- Capping power usage
- Mapping the ISO and image files located on the local client as virtual drives for use by the server
- Mounting the remote ISO and image files via HTTPS, SFTP, CIFS, and NFS
- Collaborating across up to six users of the virtual console
- Controlling quality and bandwidth usage

The XClarity Controller provides remote server management through industry-standard interfaces:

- Intelligent Platform Management Interface (IPMI) Version 2.0
- Simple Network Management Protocol (SNMP) Version 3
- Common Information Model (CIM)
- Data Center Manageability Interface (DCMI) Version 1.5
- Redfish REpresentational State Transfer (REST) API
- Web browser with HTML5 support
- Command-line interface
- Virtual Operator Panel with XClarity Mobile App via the front USB port with XClarity Controller access

Virtual Operator Panel provides quick access to system status, firmware, network, health, and alerts information. With proper authentication, it also allows to configure systems management and network settings and to control system power (Power on, Power off, Restart). The Virtual Operator Panel can be accessed from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access (See Components and connectors).

Note: Depending on the system settings, the front USB port can be assigned to XClarity Controller for management functions, or to the system as a regular USB 2.0 port, or switched between two functions by using the system ID button.

IPMI via the Ethernet port (IPMI over LAN) is supported, however it is disabled by default. For CTO orders you can specify whether you want to the feature enabled or disabled in the factory, using the feature codes listed in the following table.

Table 40. IPMI-over-LAN settings

Part number	Feature code	Description
CTO only	B7XZ	Disable IPMI-over-LAN (default)
CTO only	B7Y0	Enable IPMI-over-LAN

The following table lists the XClarity Controller FoD upgrades.

Table 41. XClarity Controller FoD upgrades

Description	Part number	Feature code	Maximum quantity
ThinkSystem XClarity Controller Standard to Advanced Upgrade	4L47A09132	AVUT	1
ThinkSystem XClarity Controller Standard to Enterprise Upgrade	None*	AUPW	1
ThinkSystem XClarity Controller Advanced to Enterprise Upgrade	4L47A09133	None**	1

* Factory-installed only.
** Field upgrade only.

Configuration notes:

- For factory-installed upgrades, either Standard to Advanced Upgrade (feature AVUT) or Standard to Enterprise Upgrade (feature AUPW) can be selected, but not both.
- For field upgrades, the Advanced to Enterprise Upgrade (4L47A09133) requires the Standard to Advanced Upgrade to be activated on the server previously with either the factory-installed feature AVUT or field upgrade 4L47A09132.

Lenovo XClarity Provisioning Manager

Lenovo XClarity Provisioning Manager is a UEFI-embedded GUI application that combines the functions of configuring system setup settings, configuring RAID, and updating applications and firmware. It also enables you to install the supported operating systems and associated device drivers, run diagnostics, and collect service data.

Lenovo XClarity Provisioning Manager has the following features:

- Automatic hardware detection
- Collecting and viewing system inventory information
- Configuring UEFI system setup settings
- Updating the system firmware
- Configuring RAID by using the RAID Setup Wizard or Advanced mode
- Installing an operating system and device drivers automatically or manually
- Running diagnostics and collecting service data

Lenovo XClarity Essentials

Lenovo offers the following XClarity Essentials software tools that can help you set up, use, and maintain the server at no additional cost:

- Lenovo XClarity Essentials OneCLI
  OneCLI is a collection of server management tools that utilize a command line interface program to manage firmware, hardware, and operating systems. It provides functions to collect full system health information (including health status), configure system setting, and update system firmware and drivers.
- Lenovo XClarity Essentials UpdateXpress
  The UpdateXpress tool is a standalone GUI application for firmware and device driver updates that enables you to maintain your server firmware and device drivers up-to-date and help you avoid unnecessary server outages. The tool acquires and deploys individual updates and UpdateXpress System Packs (UXSPs) which are integration-tested bundles.
- Lenovo XClarity Essentials Bootable Media Creator
  The Bootable Media Creator (BOMC) tool is used to create bootable media for offline firmware update.

For more information and downloads, visit the Lenovo XClarity Essentials web page:
http://support.lenovo.com/us/en/documents/LNVO-center

Lenovo XClarity Administrator

Lenovo XClarity is a centralized systems management solution that helps administrators deliver infrastructure faster. This solution integrates easily with Lenovo x86 servers, RackSwitch switches, and DS Series storage, providing automated agent-less discovery, monitoring, firmware updates, configuration management, and bare metal deployment of operating systems and hypervisors across multiple servers.

Lenovo XClarity Administrator is an optional software component for the SR530 server which can be downloaded and used at no charge to discover and monitor the SR530 and manage firmware upgrades for them.

If software support is required for Lenovo XClarity Administrator, or Lenovo XClarity Administrator premium features (such as configuration management and operating system deployment) are required, or both, Lenovo XClarity Pro software subscription should be ordered. Lenovo XClarity Pro is licensed on a per managed system basis, that is, each managed Lenovo system requires a license.

The following table lists the geo-specific Lenovo XClarity software license options.

Table 42. Lenovo XClarity software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Pro, per Managed Endpoint w/1 Yr SW S&S	00MT201	00MT207	1
Lenovo XClarity Pro, per Managed Endpoint w/3 Yr SW S&S	00MT202	00MT208	1
Lenovo XClarity Pro, per Managed Endpoint w/5 Yr SW S&S	00MT203	00MT209	1

* NA = North America; AP = Asia Pacific
** EMEA = Europe, Middle East, Africa; LA = Latin America

Lenovo XClarity Administrator offers the following standard features that are available at no charge:

- Auto-discovery and monitoring of Lenovo x86 servers, RackSwitch switches, Flex System chassis, and DS Series storage systems
- Firmware updates and compliance enforcement
- External alerts and notifications via SNMP traps, syslog remote logging, and e-mail
- Secure connections to managed endpoints
- NIST 800-131A or FIPS 140-2 compliant cryptographic standards between the management solution and managed endpoints
- Integration into existing higher level management systems such as cloud automation and orchestration tools through REST APIs, providing extensive external visibility and control over hardware resources
- An intuitive, easy-to-use GUI
- Scripting with Windows PowerShell, providing command-line visibility and control over hardware resources

Lenovo XClarity Administrator offers the following premium features that require an optional Pro license:

- Pattern-based configuration management that allows to define configurations once and apply repeatedly without errors when deploying new servers or redeploying existing servers without disrupting the fabric
- Bare-metal deployment of operating systems and hypervisors to streamline infrastructure provisioning

For more information, refer to the Lenovo XClarity Administrator Product Guide:
http://lenovopress.com/tips1200

Lenovo XClarity Integrators

Lenovo offers at no charge (if software support is required, a Lenovo XClarity Pro software subscription license should be ordered) two software plug-in modules, Lenovo XClarity Integrators, to manage physical infrastructure from leading external virtualization management software tools from Microsoft and VMware:

- Lenovo XClarity Integrator for Microsoft System Center
- Lenovo XClarity Integrator for VMware vCenter

Lenovo XClarity Integrators offer the following additional features:

- Ability to discover, manage, and monitor Lenovo server hardware from VMware vCenter or Microsoft System Center
- Deployment of firmware updates and configuration patterns to Lenovo x86 rack servers and Flex System from the virtualization management tool
- Non-disruptive server maintenance in clustered environments that reduces workload downtime by dynamically migrating workloads from affected hosts during rolling server updates or reboots
- Greater service level uptime and assurance in clustered environments during unplanned hardware events by dynamically triggering workload migration from impacted hosts when impending hardware failures are predicted

For more information, refer to the Lenovo XClarity Integrators web page:
http://www3.lenovo.com/us/en/data-center/software/systems-management/xclarity-integrators

Lenovo XClarity Energy Manager

Lenovo XClarity Energy Manager provides a stand-alone, web-based agent-less power management console that provides real time data and enables you to observe, plan and manage power and cooling for Lenovo servers. Using built-in intelligence, it identifies server power consumption trends and ideal power settings and performs cooling analysis so that you can define and optimize power-saving policies.

Lenovo XClarity Energy Manager offers the following capabilities:

- Monitors room, row, rack, and device levels in the data center
- Reports vital server information, such as power, temperature and resource utilization
- Monitors inlet temperature to locate hot spots, reducing the risk of data or device damage
- Provides finely-grained controls to limit platform power in compliance with IT policy
- Generates alerts when a user-defined threshold is reached

Lenovo XClarity Energy Manager is an optional software component for the SR530 server that is licensed on a per managed node basis, that is, each managed server requires a license. The 1-node Energy Manager license is included in the XClarity Controller Enterprise upgrade.

To manage systems without XClarity Controller Enterprise licenses, a node license pack should be purchased. The following table lists the geo-specific Lenovo XClarity Energy Manager software license options.

Table 43. Lenovo XClarity Energy Manager software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Energy Manager, 1 Node w/ 1 Yr S&S	01DA225	01DA228	1

* NA = North America; AP = Asia Pacific.
** EMEA = Europe, Middle East, Africa; LA = Latin America.

For more information, refer to the Lenovo XClarity Energy Manager web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lxem

Lenovo Capacity Planner

Lenovo Capacity Planner is a power consumption evaluation tool that enhances data center planning by enabling IT administrators and pre-sales professionals to understand various power characteristics of racks, servers, and other devices. Capacity Planner can dynamically calculate the power consumption, current, British Thermal Unit (BTU), and volt-ampere (VA) rating at the rack level, improving the planning efficiency for large-scale deployments.

For more information, refer to the Capacity Planner web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

Security

The SR530 server offers the following security features:

- Power-on password
- Administrator's password
- Secure firmware updates
- Onboard Trusted Platform Module (TPM) version 1.2 or 2.0 (configurable UEFI system setting)
- Trusted Cryptographic Module (TCM) (optional; available in PRC only)
- Nationz Trusted Platform Module v2.0 (optional; available in PRC only)
- Lockable front bezel (optional)
- Security Key Lifecycle Manager (SKLM) encryption key management for SEDs - FoD upgrade (optional)
- Lenovo Business Vantage security software (optional; available in PRC only)

The server is NIST SP 800-147B compliant.

The following table lists the security options that are available for the SR530 server.

Table 44. Security options

Description	Part number	Feature code	Maximum quantity
Lockable front bezel			
ThinkSystem 1U Security Bezel	7Z17A02581	AUWR	1
Trusted Cryptographic Module (PRC only)			
ThinkSystem Trusted Cryptographic Module	None*	AVKE	1
Trusted Platform Module (PRC only)			
ThinkSystem Nationz Trusted Platform Module v2.0	None*	B22N	1
Security Key Lifecycle Manager - FoD (United States, Canada, Asia Pacific, and Japan)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00D9998	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00D9999	AS6C	1
Security Key Lifecycle Manager - FoD (Latin America, Europe, Middle East, and Africa)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00FP648	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00FP649	AS6C	1

* Factory-installed only; no field upgrade.

Lenovo Business Vantage is a security software tool suite (available only in PRC) designed to work with the TCM or Nationz TPM for enhanced security, to keep user data safe, and to erase confidential data completely from a drive.

Lenovo Business Vantage provides the following features:

- Encrypts files to ensure data safety by using the TCM or Nationz TPM.
- Erases confidential data from a hard disk.
- Prohibits unauthorized access to the USB port of devices.
- Encrypts files to ensure data security on a USB storage device.

For more information, refer to the Lenovo Business Vantage web page:
http://support.lenovo.com.cn/lenovo/wsi/es/es.html

Rack installation

The following table lists the rack installation options that are available for the SR530 server.

Table 45. Rack installation options

Description	Part number	Feature code	Maximum quantity
4-post rail kits			
ThinkSystem Tool-less Slide Rail	7M27A05702	AXCA	1
ThinkSystem Tool-less Slide Rail Kit with 1U CMA	7M27A05701	AXCB	1
ThinkSystem Screw-in Slide Rail	4M17A07274	AXFN	1
ThinkSystem Screw-in Slide Rail Kit with 1U CMA	4M17A07281	B0TE	1
ThinkSystem Tool-less Friction Rail	4M17A07273	AXFM	1
Cable management arm (CMA) upgrade			
ThinkSystem 1U CMA Upgrade Kit for Tool-less Slide Rail	7M27A05699	None^	1*
ThinkSystem 1U CMA Upgrade Kit for Screw-in Slide Rail	4M17A07276	AXFP	1**
Front VGA port			
ThinkSystem SR530/SR630 Front VGA Connector (for 3.5" models)	None***	AUWU	1
ThinkSystem SR530/SR570/SR630 Front VGA Connector Upgrade Kit (for 2.5" models)	7Z17A02579	AUWW	1

^ Field upgrade only.
* The CMA Upgrade Kit for Tool-less Slide Rail is supported with the Tool-less Slide Rail (7M27A05702) only.
** The CMA Upgrade Kit for Screw-in Slide Rail is supported with the Screw-in Slide Rail (4M17A07274) only.
*** Factory-installed only; no field upgrade.

The following table summarizes the rail kit features and specifications.

Table 46. Rail kit features and specifications summary

Feature	Tool-less Slide Rail		Screw-in Slide Rail		Tool-less Friction Rail
	Without CMA	With CMA	Without CMA	With CMA	
Part number	7M27A05702	7M27A05701	4M17A07274	4M17A07281	4M17A07273
CMA	7M27A05699	Included	4M17A07276	Included	No support
Rail length	730 mm (28.74 in.)	807 mm (31.8 in.)	836.8 mm (32.9 in.)	836.8 mm (32.9 in.)	728.1 mm (28.7 in.)
Rail type	Full-out slide (ball bearing)		Full-out slide (ball bearing)		Half-out slide (friction)
Tool-less installation	Yes		No		Yes
In-rack server maintenance	Yes		Yes		No
1U PDU support	Yes		Yes		Yes
0U PDU support	Limited*		Limited*		Limited**
Rack type	IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant
Mounting holes	Square or round		Square, round, or threaded		Square or round
Mounting flange thickness	2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)
Distance between front and rear mounting flanges^	609.6 mm (24 in.) – 863.6 mm (34 in.)		609.6 mm (24 in.) – 812.8 mm (32 in.)		609.6 mm (24 in.) – 863.6 mm (34 in.)

* If a 0U PDU is used, the rack cabinet must be at least 1100 mm (43.31 in.) deep if no CMA is used, or at least 1200 mm (47.24 in.) deep if a CMA is used.
** If a 0U PDU used, the rack must be at least 1000 mm (39.37 in.) deep.
^ Measured when mounted on the rack, from the front surface of the front mounting flange to the rear most point of the rail.

Operating systems

The server supports the following operating systems:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 8.1
- Red Hat Enterprise Linux 8.2
- Red Hat Enterprise Linux 8.3
- SUSE Linux Enterprise Server 12 SP4
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 12 Xen SP4
- SUSE Linux Enterprise Server 12 Xen SP5
- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Server 15 SP1
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 15 Xen
- SUSE Linux Enterprise Server 15 Xen SP1
- SUSE Linux Enterprise Server 15 Xen SP2
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2

For a complete list of supported, certified and tested operating systems, plus additional details and links to relevant web sites, see the Operating System Interoperability Guide: https://lenovopress.com/osig#servers=sr530-7x07-7x08-sp-gen-2

For configure-to-order configurations, the server can be preloaded with VMware ESXi installed on M.2 cards. Ordering information is listed in the following table.

Table 47. VMware ESXi preload

Part number	Feature code	Description
CTO only	B3VW	VMware ESXi 6.5 U2 (Factory Installed)
CTO only	B6U0	VMware ESXi 6.5 U3 (factory installed)
CTO only	B3VX	VMware ESXi 6.7 (Factory Installed)
CTO only	B4XA	VMware ESXi 6.7 U1 (Factory Installed)
CTO only	B6U1	VMware ESXi 6.7 U2 (factory installed)
CTO only	B88T	VMware ESXi 6.7 U3 (factory installed)
CTO only	BBZG	VMware ESXi 7.0 (Factory Installed)
CTO only	BE5E	VMware ESXi 7.0 U1 (Factory Installed)

Physical specifications

The SR530 has the following overall physical dimensions, excluding components that extend outside the standard chassis, such as EIA flanges, front security bezel (if any), and power supply handles:

- Width: 435 mm (17.1 inches)
- Height: 43 mm (1.7 inches)

- Depth: 750 mm (29.5 inches)

The following table lists the detailed dimensions. See the figure below for the definition of each dimension.

Table 48. Detailed dimensions

Dimension	Description
482 mm	X_a = Width, to the outsides of the front EIA flanges
435 mm	X_b = Width, to the rack rail mating surfaces
435 mm	X_c = Width, to the outer most chassis body feature
43 mm	Y_a = Height, from the bottom of chassis to the top of the chassis
715 mm	Z_a = Depth, from the rack flange mating surface to the rearmost I/O port surface
716 mm	Z_b = Depth, from the rack flange mating surface to the rearmost feature of the chassis body
744 mm	Z_c = Depth, from the rack flange mating surface to the rearmost feature such as power supply handle
35 mm	Z_d = Depth, from the forwardmost feature on front of EIA flange to the rack flange mating surface
47 mm	Z_e = Depth, from the front of security bezel (if applicable) or forwardmost feature to the rack flange mating surface

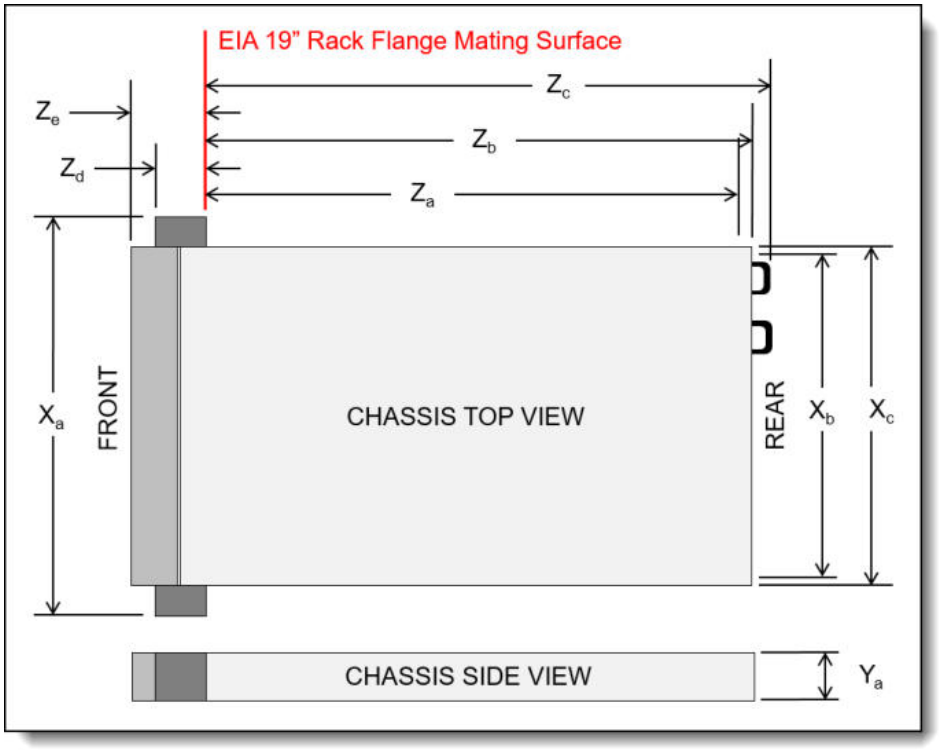


Figure 8. Server dimensions

The shipping dimensions (cardboard packaging) of the SR530 are as follows:

- Width: 587 mm (23.1 inches)
- Height: 225 mm (8.9 inches)
- Depth: 998 mm (39.3 inches)

The SR530 server has the following weight:

- Minimum configuration: 10.2 kg (22.5 lb)
- Maximum configuration: 16.0 kg (35.3 lb)

Operating environment

The SR530 server complies with ASHRAE class A2 specifications. The server performance might be impacted when the operating temperature is outside the ASHRAE A2 specifications. Depending on the hardware configuration, some server models comply with ASHRAE class A3 and class A4 specifications. To comply with ASHRAE class A3 and class A4 specifications, the server models must meet the following hardware configuration requirements at the same time:

- Two power supplies must be installed
- No system fan failure

The SR530 server is supported in the following environment:

- Air temperature:
  - Operating:
    - ASHRAE Class A4: 5 °C - 45 °C (41 °F - 113 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 125-m (410-ft) increase in altitude
    - ASHRAE Class A3: 5 °C - 40 °C (41 °F - 104 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 175-m (574-ft) increase in altitude
    - ASHRAE Class A2: 10 °C - 35 °C (50 °F - 95 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 300-m (984-ft) increase in altitude
  - Non-operating: 5 °C - 45 °C (41 °F - 113 °F)
  - Storage: -40 °C - +60 °C (-40 °F - 140 °F)
- Maximum altitude: 3,050 m (10,000 ft)
- Humidity:
  - Operating:
    - ASHRAE Class A4: 8% - 90% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A3: 8% - 85% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A2: 8% - 80% (non-condensing); maximum dew point: 21 °C (70 °F)
  - Storage: 8% - 90% (non-condensing)
- Electrical:
  - 100 - 127 (nominal) V AC; 50 Hz / 60 Hz
  - 200 - 240 (nominal) V AC; 50 Hz / 60 Hz
  - 180 - 300 V DC (HVDC; supported in PRC only)
- Acoustics:
  - Minimum configuration:
    - Operating: 5.0 bels
    - Idle: 4.5 bels
  - Maximum configuration:
    - Operating: 5.5 bels
    - Idle: 5.2 bels
- Vibration:
  - Operating: 0.21 G rms at 5 Hz to 500 Hz for 15 minutes across 3 axes
  - Non-operating: 1.04 G rms at 2 Hz to 200 Hz for 15 minutes across 6 surfaces
- Shock:
  - Operating: 15 G for 3 milliseconds in each direction (positive and negative X, Y, and Z axes)
  - Non-operating:
    - 12 kg - 22 kg: 50 G for 152 in./sec velocity change across 6 surfaces
    - 23 kg - 31 kg: 35 G for 152 in./sec velocity change across 6 surfaces

The following table lists the maximum system power load, rated inlet current, and system heat output based on the power supply and source voltage.

Table 49. Rated system power, inlet current, and system heat output

Power supply	Source voltage	Maximum power load per system (two power supplies)	Rated current per inlet	System heat output
550 W Platinum	100 - 127 V AC	722 W	6.2 A	2463 BTU/hour
	200 - 240 V AC	704 W	3 A	2402 BTU/hour
	180 - 300 V DC	702 W	2.5 A	2395 BTU/hour
750 W Platinum	100 - 127 V AC	984 W	8.4 A	3357 BTU/hour
	200 - 240 V AC	958 W	4.1 A	3269 BTU/hour
	180 - 300 V DC	958 W	3.5 A	3269 BTU/hour
750 W Titanium	200 - 240 V AC	949 W	4.1 A	3238 BTU/hour
	180 - 300 V DC	948 W	3.5 A	3235 BTU/hour

Warranty and support

The SR530 server has a one-year (7X07) or three-year (Machine Type 7X08) warranty.

The standard warranty terms are customer-replaceable unit (CRU) and onsite (for field-replaceable units FRUs only) with standard call center support during normal business hours and 9x5 Next Business Day Parts Delivered.

Lenovo's additional support services provide a sophisticated, unified support structure for your data center, with an experience consistently ranked number one in customer satisfaction worldwide. Available offerings include:

- **Premier Support**

  Premier Support provides a Lenovo-owned customer experience and delivers direct access to technicians skilled in hardware, software, and advanced troubleshooting, in addition to the following:

  - Direct technician-to-technician access through a dedicated phone line
  - 24x7x365 remote support
  - Single point of contact service
  - End to end case management
  - Third-party collaborative software support
  - Online case tools and live chat support
  - On-demand remote system analysis
- **Warranty Upgrade (Preconfigured Support)**

  Services are available to meet the on-site response time targets that match the criticality of your systems.

  - 3, 4, or 5 years of service coverage
  - 1-year or 2-year post-warranty extensions
  - **Foundation Service**: 9x5 service coverage with next business day onsite response. YourDrive YourData is an optional extra (see below).
  - **Essential Service:** 24x7 service coverage with 4-hour onsite response or 24-hour committed repair (available only in select countries). Bundled with YourDrive YourData.
  - **Advanced Service:** 24x7 service coverage with 2-hour onsite response or 6-hour committed repair (available only in select countries). Bundled with YourDrive YourData.

- **Managed Services**

  Lenovo Managed Services provides continuous 24x7 remote monitoring (plus 24x7 call center availability) and proactive management of your data center using state-of-the-art tools, systems, and practices by a team of highly skilled and experienced Lenovo services professionals.

  Quarterly reviews check error logs, verify firmware & OS device driver levels, and software as needed. We'll also maintain records of latest patches, critical updates, and firmware levels, to ensure you systems are providing business value through optimized performance.

- **Technical Account Management (TAM)**

  A Lenovo Technical Account Manager helps you optimize the operation of your data center based on a deep understanding of your business. You gain direct access to your Lenovo TAM, who serves as your single point of contact to expedite service requests, provide status updates, and furnish reports to track incidents over time. In addition, your TAM will help proactively make service recommendations and manage your service relationship with Lenovo to make certain your needs are met.

- **Enterprise Server Software Support**

  Enterprise Software Support is an additional support service providing customers with software support on Microsoft, Red Hat, SUSE, and VMware applications and systems. Around the clock availability for critical problems plus unlimited calls and incidents helps customers address challenges fast, without incremental costs. Support staff can answer troubleshooting and diagnostic questions, address product comparability and interoperability issues, isolate causes of problems, report defects to software vendors, and more.

- **YourDrive YourData**

  Lenovo's YourDrive YourData is a multi-drive retention offering that ensures your data is always under your control, regardless of the number of drives that are installed in your Lenovo server. In the unlikely event of a drive failure, you retain possession of your drive while Lenovo replaces the failed drive part. Your data stays safely on your premises, in your hands. The YourDrive YourData service can be purchased in convenient bundles and is optional with Foundation Service. It is bundled with Essential Service and Advanced Service.

- **Health Check**

  Having a trusted partner who can perform regular and detailed health checks is central to maintaining efficiency and ensuring that your systems and business are always running at their best. Health Check supports Lenovo-branded server, storage, and networking devices, as well as select Lenovo-supported products from other vendors that are sold by Lenovo or a Lenovo-Authorized Reseller.

Examples of region-specific warranty terms are second or longer business day parts delivery or parts-only base warranty.

If warranty terms and conditions include onsite labor for repair or replacement of parts, Lenovo will dispatch a service technician to the customer site to perform the replacement. Onsite labor under base warranty is limited to labor for replacement of parts that have been determined to be field-replaceable units (FRUs). Parts that are determined to be customer-replaceable units (CRUs) do not include onsite labor under base warranty.

If warranty terms include parts-only base warranty, Lenovo is responsible for delivering only replacement parts that are under base warranty (including FRUs) that will be sent to a requested location for self-service. Parts-only service does not include a service technician being dispatched onsite. Parts must be changed at customer's own cost and labor and defective parts must be returned following the instructions supplied with the spare parts.

Lenovo Service offerings are region-specific. Not all preconfigured support and upgrade options are available in every region. For information about Lenovo service upgrade offerings that are available in your region, refer to the following resources:

- Service part numbers in Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com/#/services
- Lenovo Services Availability Locator
  http://lenovolocator.com/

For service definitions, region-specific details, and service limitations, please refer to the following documents:

- Lenovo Statement of Limited Warranty for Data Center Group (DCG) Servers and System Storage
  http://pcsupport.lenovo.com/us/en/solutions/ht503310
- Lenovo Data Center Services Agreement
  http://support.lenovo.com/us/en/solutions/ht116628

Services

Lenovo Services is a dedicated partner to your success. Our goal is to reduce your capital outlays, mitigate your IT risks, and accelerate your time to productivity.

Note: Some service options may not be available in all countries. For more information, go to https://www.lenovo.com/systems/services. For information about Lenovo service upgrade offerings that are available in your region, contact your local Lenovo sales representative or business partner.

Here's a more in-depth look at what we can do for you:

- **Asset Recovery Services**

  Asset Recovery Services (ARS) helps customers recover the maximum value from their end-of-life equipment in a cost-effective and secure way. On top of simplifying the transition from old to new equipment, ARS mitigates environmental and data security risks associated with data center equipment disposal. Lenovo ARS is a cash-back solution for equipment based on its remaining market value, yielding maximum value from aging assets and lowering total cost of ownership for your customers. For more information, see the ARS page, https://lenovopress.com/lp1266-reduce-e-waste-and-grow-your-bottom-line-with-lenovo-ars.

- **Assessment Services**

  An Assessment helps solve your IT challenges through an onsite, multi-day session with a Lenovo technology expert. We perform a tools-based assessment which provides a comprehensive and thorough review of a company's environment and technology systems. In addition to the technology based functional requirements, the consultant also discusses and records the non-functional business requirements, challenges, and constraints. Assessments help organizations like yours, no matter how large or small, get a better return on your IT investment and overcome challenges in the ever-changing technology landscape.

- **Design Services**

  Professional Services consultants perform infrastructure design and implementation planning to support your strategy. The high-level architectures provided by the assessment service are turned into low level designs and wiring diagrams, which are reviewed and approved prior to implementation. The implementation plan will demonstrate an outcome-based proposal to provide business capabilities through infrastructure with a risk-mitigated project plan.

- **Basic Hardware Installation**

  Lenovo experts can seamlessly manage the physical installation of your server, storage, or networking hardware. Working at a time convenient for you (business hours or off shift), the technician will unpack and inspect the systems on your site, install options, mount in a rack cabinet, connect to power and network, check and update firmware to the latest levels, verify operation, and dispose of the packaging, allowing your team to focus on other priorities.

- **Deployment Services**

  When investing in new IT infrastructures, you need to ensure your business will see quick time to value with little to no disruption. Lenovo deployments are designed by development and engineering teams who know our Products & Solutions better than anyone else, and our technicians own the process from delivery to completion. Lenovo will conduct remote preparation and planning, configure & integrate systems, validate systems, verify and update appliance firmware, train on administrative tasks, and provide post-deployment documentation. Customer's IT teams leverage our skills to enable IT staff to transform with higher level roles and tasks.

- **Integration, Migration, and Expansion Services**

  Move existing physical & virtual workloads easily, or determine technical requirements to support increased workloads while maximizing performance. Includes tuning, validation, and documenting ongoing run processes. Leverage migration assessment planning documents to perform necessary migrations.

Regulatory compliance

The ThinkSystem SR530 server conforms to the following regulations:

- United States: FCC Part 15, Class A; UL 60950-1
- Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1
- Mexico: NOM-19
- Argentina: IEC60950-1
- European Union: CE Mark (EN55022 Class A, IEC/EN60950-1, EN55024, EN61000-3-2, EN61000-3-3)
- Germany: TUV-GS (IEC/EN 60950-1, EK1-ITB2000)
- Russia, Kazakhstan, Belarus: EAC (TR CU 004/2011, TR CU 020/2011)
- China: CCC GB4943.1, GB9254 Class A, GB17625.1
- India: BIS
- Japan: VCCI, Class A
- Taiwan: BSMI CNS13438, Class A; CNS14336-1
- Korea: KN22, Class A; KN24
- Australia/New Zealand: AS/NZS CISPR 22 Class A
- Reduction of Hazardous Substances (ROHS)
- Energy Star 3.0 (excluding configurations with Bronze 3204, Gold 5222, or Platinum 8256 processors)

Note: For more information on the Energy Star 3.0 certification, refer to the *Energy Star 3.0 Certifications for ThinkSystem Servers* publication:
http://lenovopress.com/lp1230

External drive enclosures

The server supports attachment to external drive enclosures using a RAID controller with external ports or a SAS host bus adapter. Adapters supported by the server are listed in the SAS adapters for external storage section.

Note: Information provided in this section is for ordering reference purposes only. For the operating system and adapter support details, refer to the interoperability matrix for a particular storage enclosure that can be found on the Lenovo Data Center Support web site:
http://datacentersupport.lenovo.com

Table 50. External drive enclosures

Description	Part number		
	Worldwide	Japan	PRC
Lenovo Storage D1212 LFF Disk Expansion with Dual SAS IO Modules	4587A11	4587A1J	4587A1C
Lenovo Storage D1224 SFF Disk Expansion with Dual SAS IO Modules	4587A31	4587A3J	4587A3C
Lenovo Storage D3284 4TB x 84 HD Expansion Enclosure	641311F		
Lenovo Storage D3284 6TB x 84 HD Expansion Enclosure	641312F		
Lenovo Storage D3284 8TB x 84 HD Expansion Enclosure	641313F		
Lenovo Storage D3284 10TB x 84 HD Expansion Enclosure	641314F		

For details about supported drives, adapters, and cables, see the following Lenovo Press Product Guides:

- Lenovo Storage D1212 and D1224
  http://lenovopress.com/lp0512
- Lenovo Storage D3284
  http://lenovopress.com/lp0513

External storage systems

Lenovo offers the ThinkSystem DE Series and ThinkSystem DM Series external storage systems for high-performance storage. See the DE Series and DM Series product guides for specific controller models, expansion enclosures and configuration options:

- ThinkSystem DE Series Storage
  https://lenovopress.com/storage/thinksystem/de-series#rt=product-guide
- ThinkSystem DM Series Storage
  https://lenovopress.com/storage/thinksystem/dm-series#rt=product-guide

External backup units

The following table lists the external backup options that are offered by Lenovo.

Table 51. External backup options

Part number	Description
External RDX USB drives	
4T27A10725	ThinkSystem RDX External USB 3.0 Dock
External SAS tape backup drives	
6160S6E	IBM TS2260 Tape Drive Model H6S
6160S7E	IBM TS2270 Tape Drive Model H7S
6160S8E	IBM TS2280 Tape Drive Model H8S
External SAS tape backup autoloaders	
6171S5R	IBM TS2900 Tape Autoloader w/LTO5 HH SAS
6171S6R	IBM TS2900 Tape Autoloader w/LTO6 HH SAS
6171S7R	IBM TS2900 Tape Autoloader w/LTO7 HH SAS
External tape backup libraries	
6741A1F	IBM TS4300 3U Tape Library-Base Unit
6741A3F	IBM TS4300 3U Tape Library-Expansion Unit
Full High 8 Gb Fibre Channel for TS4300	
01KP954	LTO 8 FH Fibre Channel Drive
01KP938	LTO 7 FH Fibre Channel Drive
01KP935	LTO 6 FH Fibre Channel Drive
Half High 8 Gb Fibre Channel for TS4300	
01KP952	LTO 8 HH Fibre Channel Drive
01KP936	LTO 7 HH Fibre Channel Drive
01KP933	LTO 6 HH Fibre Channel Drive
Half High 6 Gb SAS for TS4300	
01KP953	LTO 8 HH SAS Drive
01KP937	LTO 7 HH SAS Drive
01KP934	LTO 6 HH SAS Drive

For more information, see the list of Product Guides in the Backup units category:
https://lenovopress.com/servers/options/backup

Fibre Channel SAN switches

Lenovo offers the ThinkSystem DB Series of Fibre Channel SAN switches and directors for high-performance storage expansion. See the DB Series product guides for models and configuration options:

- ThinkSystem DB Series SAN Switches and Directors: https://lenovopress.com/storage/switches/rack#rt=product-guide

Rack cabinets

The following table lists the supported rack cabinets.

Table 52. Rack cabinets

Part number	Description
7D2B0001WW / 7D2N0001WW	12U 1200mm Deep Micro Datacenter Rack
7D2C0001WW / 7D2P0001WW	18U 1200mm Deep Micro Datacenter Rack
93072RX	25U Standard Rack
93072PX	25U Static S2 Standard Rack
93634PX	42U 1100mm Dynamic Rack
93634EX	42U 1100mm Dynamic Expansion Rack
93604PX	42U 1200mm Deep Dynamic Rack
93614PX	42U 1200mm Deep Static Rack
93084EX	42U Enterprise Expansion Rack
93084PX	42U Enterprise Rack
93074RX	42U Standard Rack

For specifications about these racks, see the Lenovo Rack Cabinet Reference, available from: https://lenovopress.com/lp1287-lenovo-rack-cabinet-reference

For more information, see the list of Product Guides in the Rack cabinets category: https://lenovopress.com/servers/options/racks

KVM switches and consoles

The following table lists the supported KVM consoles, keyboards, and KVM switches.

Table 53. Console keyboards

Part number	Description
Console keyboards	
7ZB7A05469	ThinkSystem Keyboard w/ Int. Pointing Device USB - Arabic 253 RoHS v2
7ZB7A05468	ThinkSystem Keyboard w/ Int. Pointing Device USB - Belg/UK 120 RoHS v2
7ZB7A05206	ThinkSystem Keyboard w/ Int. Pointing Device USB - Czech 489 RoHS v2
7ZB7A05207	ThinkSystem Keyboard w/ Int. Pointing Device USB - Danish 159 RoHS v2
7ZB7A05208	ThinkSystem Keyboard w/ Int. Pointing Device USB - Dutch 143 RoHS v2
7ZB7A05210	ThinkSystem Keyboard w/ Int. Pointing Device USB - Fr/Canada 445 RoHS v2
7ZB7A05209	ThinkSystem Keyboard w/ Int. Pointing Device USB - French 189 RoHS v2
7ZB7A05211	ThinkSystem Keyboard w/ Int. Pointing Device USB - German 129 RoHS v2
7ZB7A05212	ThinkSystem Keyboard w/ Int. Pointing Device USB - Greek 219 RoHS v2
7ZB7A05213	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hebrew 212 RoHS v2
7ZB7A05214	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hungarian 208 RoHS v2

Part number	Description
7ZB7A05215	ThinkSystem Keyboard w/ Int. Pointing Device USB - Italian 141 RoHS v2
7ZB7A05216	ThinkSystem Keyboard w/ Int. Pointing Device USB - Japanese 194 RoHS v2
7ZB7A05217	ThinkSystem Keyboard w/ Int. Pointing Device USB - Korean 413 RoHS v2
7ZB7A05218	ThinkSystem Keyboard w/ Int. Pointing Device USB - LA Span 171 RoHS v2
7ZB7A05219	ThinkSystem Keyboard w/ Int. Pointing Device USB - Norwegian 155 RoHS v2
7ZB7A05220	ThinkSystem Keyboard w/ Int. Pointing Device USB - Polish 214 RoHS v2
7ZB7A05221	ThinkSystem Keyboard w/ Int. Pointing Device USB - Portuguese 163 RoHS v2
7ZB7A05222	ThinkSystem Keyboard w/ Int. Pointing Device USB - Russian 441 RoHS v2
7ZB7A05223	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovak 245 RoHS v2
7ZB7A05231	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovenian 234 RoHS v2
7ZB7A05224	ThinkSystem Keyboard w/ Int. Pointing Device USB - Spanish 172 RoHS v2
7ZB7A05225	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swed/Finn 153 RoHS v2
7ZB7A05226	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swiss F/G 150 RoHS v2
7ZB7A05227	ThinkSystem Keyboard w/ Int. Pointing Device USB - Thai 191 RoHS v2
7ZB7A05467	ThinkSystem Keyboard w/ Int. Pointing Device USB - Trad Chinese/US 467 RoHS v2
7ZB7A05228	ThinkSystem Keyboard w/ Int. Pointing Device USB - Turkish 179 RoHS v2
7ZB7A05229	ThinkSystem Keyboard w/ Int. Pointing Device USB - UK Eng 166 RoHS v2
7ZB7A05470	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Eng 103P RoHS v2
7ZB7A05230	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Euro 103P RoHS v2
ThinkSystem Digital and Analog KVM Console switches and cables	
1754D1T	ThinkSystem Digital 2x1x16 KVM Switch (DVI video output port)
1754A1T	ThinkSystem Analog 1x8 KVM Switch (DVI video output port)
4X97A11108	ThinkSystem VGA to DVI Conversion Cable
4X97A11109	ThinkSystem Single-USB Conversion Cable for Digital KVM
4X97A11107	ThinkSystem Dual-USB Conversion Cable for Digital KVM
4X97A11106	ThinkSystem USB Conversion Cable for Analog KVM
GCM and LCM Console switches and cables	
1754D2X	Global 4x2x32 Console Manager (GCM32)
1754D1X	Global 2x2x16 Console Manager (GCM16)
1754A2X	Local 2x16 Console Manager (LCM16)
1754A1X	Local 1x8 Console Manager (LCM8)
43V6147	Single Cable USB Conversion Option (UCO)
39M2895	USB Conversion Option (4 Pack UCO)
46M5383	Virtual Media Conversion Option Gen2 (VCO2)
46M5382	Serial Conversion Option (SCO)

For more information, see the list of Product Guides in the KVM Switches and Consoles category:
http://lenovopress.com/servers/options/kvm

Power distribution units

The following table lists the power distribution units (PDUs) that are offered by Lenovo.

Table 54. Power distribution units

Part number	Description
0U Basic PDUs	
00YJ776	0U 36 C13/6 C19 24A/200-240V 1 Phase PDU with NEMA L6-30P line cord
00YJ777	0U 36 C13/6 C19 32A/200-240V 1 Phase PDU with IEC60309 332P6 line cord
00YJ778	0U 21 C13/12 C19 32A/200-240V/346-415V 3 Phase PDU with IEC60309 532P6 line cord
00YJ779	0U 21 C13/12 C19 48A/200-240V 3 Phase PDU with IEC60309 460P9 line cord
Switched and Monitored PDUs	
00YJ780	0U 20 C13/4 C19 Switched and Monitored 32A/200-240V/1Ph PDU w/ IEC60309 332P6 line cord
00YJ781	0U 20 C13/4 C19 Switched and Monitored 24A/200-240V/1Ph PDU w/ NEMA L6-30P line cord
00YJ782	0U 18 C13/6 C19 Switched / Monitored 32A/200-240V/346-415V/3Ph PDU w/ IEC60309 532P6 cord
00YJ783	0U 12 C13/12 C19 Switched and Monitored 48A/200-240V/3Ph PDU w/ IEC60309 460P9 line cord
46M4003	1U 9 C19/3 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
46M4004	1U 12 C13 Switched and Monitored DPI PDU (without line cord)
46M4005	1U 12 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
Ultra Density Enterprise PDUs (9x IEC 320 C13 + 3x IEC 320 C19 outlets)	
71762NX	Ultra Density Enterprise C19/C13 PDU Module (without line cord)
71763NU	Ultra Density Enterprise C19/C13 PDU 60A/208V/3ph with IEC 309 3P+Gnd line cord
C13 Enterprise PDUs (12x IEC 320 C13 outlets)	
39M2816	DPI C13 Enterprise PDU+ (without line cord)
39Y8941	DPI Single Phase C13 Enterprise PDU (without line cord)
C19 Enterprise PDUs (6x IEC 320 C19 outlets)	
39Y8948	DPI Single Phase C19 Enterprise PDU (without line cord)
39Y8923	DPI 60A 3 Phase C19 Enterprise PDU with IEC 309 3P+G (208 V) fixed line cord
Front-end PDUs (3x IEC 320 C19 outlets)	
39Y8938	DPI 30amp/125V Front-end PDU with NEMA L5-30P line cord
39Y8939	DPI 30amp/250V Front-end PDU with NEMA L6-30P line cord
39Y8934	DPI 32amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8940	DPI 60amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8935	DPI 63amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
NEMA PDUs (6x NEMA 5-15R outlets)	
39Y8905	DPI 100-127V PDU with Fixed NEMA L5-15P line cord
Line cords for PDUs that ship without a line cord	
40K9611	DPI 32a Line Cord (IEC 309 3P+N+G)
40K9612	DPI 32a Line Cord (IEC 309 P+N+G)
40K9613	DPI 63a Cord (IEC 309 P+N+G)
40K9614	DPI 30a Line Cord (NEMA L6-30P)
40K9615	DPI 60a Cord (IEC 309 2P+G)
40K9617	DPI Australian/NZ 3112 Line Cord
40K9618	DPI Korean 8305 Line Cord

For more information, see the Lenovo Press documents in the PDU category:
https://lenovopress.com/servers/options/pdu

Uninterruptible power supply units

The following table lists the uninterruptible power supply (UPS) units that are offered by Lenovo.

Table 55. Uninterruptible power supply units

Part number	Description
55941AX	RT1.5kVA 2U Rack or Tower UPS (100-125VAC)
55941KX	RT1.5kVA 2U Rack or Tower UPS (200-240VAC)
55942AX	RT2.2kVA 2U Rack or Tower UPS (100-125VAC)
55942KX	RT2.2kVA 2U Rack or Tower UPS (200-240VAC)
55943AX	RT3kVA 2U Rack or Tower UPS (100-125VAC)
55943KX	RT3kVA 2U Rack or Tower UPS (200-240VAC)
55945KX	RT5kVA 3U Rack or Tower UPS (200-240VAC)
55946KX	RT6kVA 3U Rack or Tower UPS (200-240VAC)
55948KX	RT8kVA 6U Rack or Tower UPS (200-240VAC)
55949KX	RT11kVA 6U Rack or Tower UPS (200-240VAC)
55948PX	RT8kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55949PX	RT11kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55943KT†	ThinkSystem RT3kVA 2U Standard UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55943LT†	ThinkSystem RT3kVA 2U Long Backup UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55946KT†	ThinkSystem RT6kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)
5594XKT†	ThinkSystem RT10kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)

† Only available in China and countries in the Asia Pacific region.

For more information, see the list of Product Guides in the UPS category:
https://lenovopress.com/servers/options/ups

Lenovo Financial Services

Lenovo Financial Services reinforces Lenovo's commitment to deliver pioneering products and services that are recognized for their quality, excellence, and trustworthiness. Lenovo Financial Services offers financing solutions and services that complement your technology solution anywhere in the world.

We are dedicated to delivering a positive finance experience for customers like you who want to maximize your purchase power by obtaining the technology you need today, protect against technology obsolescence, and preserve your capital for other uses.

We work with businesses, non-profit organizations, governments and educational institutions to finance their entire technology solution. We focus on making it easy to do business with us. Our highly experienced team of finance professionals operates in a work culture that emphasizes the importance of providing outstanding customer service. Our systems, processes and flexible policies support our goal of providing customers with a positive experience.

We finance your entire solution. Unlike others, we allow you to bundle everything you need from hardware and software to service contracts, installation costs, training fees, and sales tax. If you decide weeks or months later to add to your solution, we can consolidate everything into a single invoice.

Our Premier Client services provide large accounts with special handling services to ensure these complex transactions are serviced properly. As a premier client, you have a dedicated finance specialist who manages your account through its life, from first invoice through asset return or purchase. This specialist develops an in-depth understanding of your invoice and payment requirements. For you, this dedication provides a high-quality, easy, and positive financing experience.

For your region specific offers please ask your Lenovo sales representative or your technology provider about the use of Lenovo Financial Services. For more information, see the following Lenovo website:

https://www.lenovo.com/us/en/landingpage/lenovo-financial-services/

Related publications and links

For more information, see these resources:

- ThinkSystem SR530 product page
  https://www.lenovo.com/us/en/data-center/servers/racks/ThinkSystem-SR530/p/77XX7SRSR53
- Datasheet for the ThinkSystem SR530:
  https://lenovopress.com/ds0002-lenovo-thinksystem-sr530
- 3D Interactive Tour of the ThinkSystem SR530:
  https://lenovopress.com/lp0670-3d-tour-thinksystem-sr530
- Walkthrough Video for the ThinkSystem SR530:
  https://lenovopress.com/lp0744-thinksystem-sr530-server-video-walkthrough
- User Manuals for the ThinkSystem SR530:
  https://thinksystem.lenovofiles.com/help/topic/7X07/introduction.html?cp=4_2
  - Quick Start Guide
  - Setup Guide
  - Rack Installation Guides
  - Maintenance Manual
  - Messages and Codes Reference
  - UEFI Manual
- Lenovo Data Center Support Downloads - ThinkSystem SR530:
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x07/downloads
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x08/downloads
- Lenovo Hardware Installation & Removal Videos on the ThinkSystem SR530:
  - YouTube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
  - Youku: https://list.youku.com/albumlist/show/id_50437162
- Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com

Related product families

Product families related to this document are the following:

- 2-Socket Rack Servers
- ThinkSystem SR530 Server

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2021. All rights reserved.

This document, LP1045, was created or updated on March 2, 2021.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  http://lenovopress.com/LP1045
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at http://lenovopress.com/LP1045.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
Bootable Media Creator
Flex System
Lenovo Services
RackSwitch
System x®
ThinkSystem
TopSeller
TruDDR4
UpdateXpress System Packs
XClarity®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Hyper-V®, Microsoft®, PowerShell, Windows PowerShell®, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Lenovo XClarity Administrator User's Guide



Version 3.2.0

Fourth Edition (March 2021)

© Copyright Lenovo 2015, 2021.
LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Tables v

Summary of changes vii

Chapter 1. Lenovo XClarity Administrator Overview 1

Logging in to Lenovo XClarity Administrator 5
User interface tips and techniques 9
Using the Lenovo XClarity Mobile app 10

Chapter 2. Administering Lenovo XClarity Administrator 17

Managing authentication and authorization 17
Managing the authentication server 17
Managing user accounts 32
Managing stored credentials 38
Managing roles and role groups. 39
Managing access to devices 56
Implementing a secure environment 59
Changing the user-account security settings 60
Configuring cryptography settings. 63
Working with security certificates 64
Enabling encapsulation 74
Implementing NIST SP 800-131A compliance. 75
Using VMware Tools 76
Configuring network access 76
Setting the date and time 83
Setting inventory preferences 85
Setting threshold preferences for generating alerts and events. 86
Setting up automatic problem notification to Lenovo Support (Call Home) 86
Setting up automatic problem notification to a preferred service provider 91
Backing up and restoring system data and settings 93
Backing up Lenovo XClarity Administrator. . . 93
Restoring Lenovo XClarity Administrator . . . 95
Migrating data and settings to another Lenovo XClarity Administrator instance 96
Managing disk space 99
Managing remote shares 100
Changing the language of the user interface . . . 101
Shutting down Lenovo XClarity Administrator . . . 101
Restarting Lenovo XClarity Administrator 102

Chapter 3. Monitoring devices and activities 105

Viewing a summary of your environment 105
Viewing a summary of your hardware status 106
Viewing a summary of your provisioning status 107
Viewing a summary of Lenovo XClarity Administrator activity 109
Monitoring system resources 109
Monitoring trends in provisioning status 111
Placing devices in maintenance mode 112
Working with alerts 113
Viewing active alerts 113
Excluding alerts 117
Resolving an alert 118
Acknowledging alerts. 119
Working with events 119
Monitoring events in the event log 119
Monitoring events in the audit log 121
Resolving an event. 123
Excluding events 123
Forwarding events 124
Working with jobs 154
Monitoring jobs 154
Scheduling jobs 157
Adding a resolution and comments to a job 160
Viewing relationships between jobs and events . . 160

Chapter 4. Management considerations 163

Comparison between Flex System Manager and Lenovo XClarity Administrator 163
Migrating from Flex System Manager 165
Using another management software in tandem with Lenovo XClarity Administrator 166

Chapter 5. Managing resource groups 169

Viewing the status of devices in a resource group. 169
Viewing the members of a resource group 171
Creating a dynamic resource group 174
Creating a static resource group 176
Removing a resource group 177
Modifying resource-group properties 178

© Copyright Lenovo 2015, 2021

Chapter 6. Managing racks 179
Viewing the status of devices in a rack 183
Removing a rack 185

Chapter 7. Managing chassis 187
Viewing the status of a managed chassis 195
Viewing the details of a managed chassis. 196
Backing up and restoring CMM-configuration data 200
Launching the CMM web interface for a chassis 200
Modifying the system properties for a chassis . . . 201
Modifying the management-IP settings for a chassis 201
Configuring CMM failover 202
Restarting a CMM 203
Virtually reseating a CMM 204
Resolving expired or invalid stored credentials for a chassis 205
Recovering management with a CMM after a management server failure 206
Unmanaging a chassis 207
Recovering a chassis that was not unmanaged correctly 208

Chapter 8. Managing servers 211
Viewing the status of a managed server 221
Viewing the details of a managed server 224
Backing up and restoring server-configuration data 227
Using remote control. 228
Using remote control to manage ThinkSystem or ThinkAgile servers 228
Using remote control to manage ThinkServer and NeXtScale sd350 M5 servers 229
Using remote control to manage Converged, Flex System, NeXtScale, and System x servers 230
Managing access to operating-systems on managed servers 240
Viewing Features on Demand keys 242
Managing energy and temperature 243
Powering on and off a server. 244
Virtually reseating a server in a Flex System chassis 245
Launching the management controller interface for a server 245
Modifying the system properties for a server . . . 247
Resolving expired or invalid stored credentials for a server 247
Recovering a failed server after deploying a server pattern 248
Recovering boot settings after server pattern deployment 249
Recovering rack or tower server management after a management server failure 250
Recovering rack or tower server management after a management server failure by force management 250
Recovering a System x or NeXtScale M4 server that was not unmanaged correctly by using the management controller 250
Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by resetting the management controller 251
Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by using cimcli. 252
Recovering ThinkServer server management after a management server failure by using the management controller interface 253
Unmanaging a rack or tower server 254
Recovering a rack or tower server that was not unmanaged correctly 255

Chapter 9. Managing storage devices 261
Storage management considerations 265
Viewing the status of storage devices 266
Viewing the details of a storage device 268
Backing up and restoring storage-configuration data 271
Powering on and off a storage device 271
Virtually reseating storage controllers in a Flex System storage device 272
Launching the management controller interface for a storage device 272
Modifying the system properties for a storage device 273
Recovering management of a rack storage device after a management server failure. 274
Recovering management of a Lenovo ThinkSystem DE Series storage device after a management server failure 274
Unmanaging a Lenovo Storage or Nimble storage system 275
Recovering a rack storage device that was not unmanaged correctly 275

Chapter 10. Managing switches . . .277
Switch management considerations. 282
Viewing the status of switches 284
Viewing the details of a switch 286
Powering on and off a switch 289
Enabling and disabling switch ports 289
Backing up and restoring switch-configuration data 290

Backing up switch-configuration data 291
Restoring switch-configuration data 292
Exporting and importing switch-configuration files 294
Launching the management controller interface for a switch 295
Launching a remote SSH session for a switch . . . 296
Modifying the system properties for a switch . . . 297
Resolving expired or invalid stored credentials for a switch 298
Recovering management with a RackSwitch switch after a management server failure 298
Unmanaging a RackSwitch switch 299
Recovering a RackSwitch switch that was not unmanaged correctly 300

Chapter 11. Configuring servers using configuration patterns. 301

Configuration considerations 303
Defining address pools 304
Creating an IP address pool 306
Creating an Ethernet address pool. 307
Creating a Fibre Channel address pool 308
Working with server patterns. 314
Creating a server pattern 316
Deploying a server pattern to a server 339
Modifying a server pattern 340
Exporting and importing server and category patterns 341
Working with server profiles 342
Activating a server profile 343
Deactivating a server profile 345
Deleting a server profile 346
Working with placeholder chassis. 346
Creating a placeholder chassis 347
Deploying a server pattern to a placeholder chassis 348
Deploying a placeholder chassis 349
Resetting storage adapters to default values . . . 350
Configuring memory 352

Chapter 12. Configuring switches using configuration templates. 353

Setting default server-configuration preferences 354
Creating a switch-configuration template 355
Defining VLAN port-membership settings . . . 357
Defining VLAN properties 358
Removing VLAN settings 359
Deleting VLANs 359
Defining port-channel basic settings 360
Defining port-channel advanced settings . . . 361
Deleting port channels 361
Defining general switch settings. 362
Defining global L2 interface settings 362
Defining peer VLAG settings 363
Defining VLAG instance settings 364
Defining VLAG advanced settings 364
Deleting a VLAG instance 365
Defining a spine-leaf topology 365
Deploying switch-configuration templates to a target switch 366
Viewing switch-configuration deployment history 366

Chapter 13. Updating firmware and Windows device drivers 369

Updating firmware on managed devices 369
Firmware-update considerations 376
Managing the firmware-updates repository . . 382
Creating firmware-compliance policies 396
Assigning firmware-compliance policies . . . 399
Identifying devices that are not compliant . . . 401
Configuring global firmware-update settings 401
Applying and activating firmware updates . . . 402
Updating Windows device drivers on managed servers 419
OS device-driver update considerations . . . 421
Managing the OS device-drivers repository 422
Configuring Windows Server for OS device-driver updates 427
Configuring global Windows device-driver update settings 429
Applying Windows device drivers 430

Chapter 14. Installing operating systems on bare-metal servers 435

Operating-system deployment considerations . . . 438
Supported operating systems 442
Operating-system image profiles 446
Port availability for deployed operating systems 450
Configuring a remote file server 452
Importing operating-system images 454
Customizing OS-image profiles. 456
Importing a customized OS image profile . . . 463
Importing boot files 465
Importing device drivers. 469
Importing custom configuration settings . . . 473
Importing custom unattend files. 489
Associating an unattend file with a configuration settings file 494

© Copyright Lenovo 2015, 2021

Importing custom installation scripts 495
Importing custom software 500
Creating a custom OS-image profile 502
Configuring global OS-deployment settings 504
Configuring network settings for managed servers 506
Choosing the storage location for managed servers 508
Deploying an operating-system image 511
Integrating with Windows Active Directory 514
OS-deployment scenarios. 518
Deploying RHEL with custom device drivers 518
Deploying RHEL and a Hello World PHP application using a custom unattend file . . . 520
Deploying RHEL and a Hello World PHP application using custom software and a post-installation script 524
Deploying SLES 12 SP3 with custom packages and time zone 527
Deploying SLES 12 SP3 with custom software 533
Deploying SLES 12 SP3 with a configurable locale and NTP servers 535
Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address 540
Deploying VMware ESXi v6.7 with Lenovo Customization with a configurable locale and second-user credentials. 543
Deploying Windows 2016 with custom features 547
Deploying Windows 2016 with custom software 550
Deploying Windows 2016 for Japanese. 554

Chapter 15. End-to-end scenarios for setting up new devices 561

Deploying ESXi to a local hard drive 561
Deploying a predefined virtualization pattern 561
Deploying VMware ESXi to a Flex System x240 Compute Node 563
Deploying ESXi to SAN storage. 568
Deploying a server pattern to support SAN boot 568
Deploying VMware ESXi to SAN storage . . . 571
Notices . . . . . dlxxvii
Trademarks . . . . . dlxxviii

Tables

1. Account Security settings. 61
2. Role of each network interface based on network topology 78
3. Functional comparison between Flex System Manager and XClarity Administrator. 164
4. Lenovo MAC address pool 308
5. Brocade WWN address pool 310
6. Emulex WWN address pool 311
7. Lenovo WWN address pool 312
8. QLogic WWN address pool 313
9. Port availability for RHEL Virtualization profiles 451
10. Port availability for RHEL Basic and Minimal profiles 451
11. Port availability for Windows profiles 452

© Copyright Lenovo 2015, 2021

Summary of changes

Follow-on releases of Lenovo XClarity Administrator management software support new hardware, software enhancements, and fixes.

Refer to the change history file (*.chg) that is provided in the update package for information about fixes.

This version supports the following enhancements to the management software.

For information about changes in earlier releases, See What's new in the XClarity Administrator online documentation.

Function	Description
Administration	You use an external CyberArk identity-management system as an external password vault to store XClarity Administrator and Lenovo XClarity Controller credentials (see Setting up a CyberArk identity-management system). Single sign-on to the management controller interface is supported for ThinkSystem SR645 and SR665 servers (requires XCC 21A or later firmware).
Device management	Thermal design power (TDP), which is the maximum power that is running at the highest p-state, is available in the processor inventory (see Viewing the details of a managed server).
Operating system deployment	You can deploy Ubunto operating-system images using the predefined Virtualization profile (see Operating-system image profiles).
Firmware updates	You can update firmware on ThinkSystem DM storage devices (see Updating firmware on managed devices). You can create update compliance policies that set compliance rules at the firmware-component level (see Creating firmware-compliance policies). You can apply firmware updates for Lenovo XClarity Provisioning Manager (LXPM), LXPM windows drivers, or LXPM Linux drivers to ThinkSystem SR635 and SR655 servers (see Applying bundled firmware updates using compliance policies).
Windows device-driver updates	You can use a domain account when updating OS device-drivers updates (see).

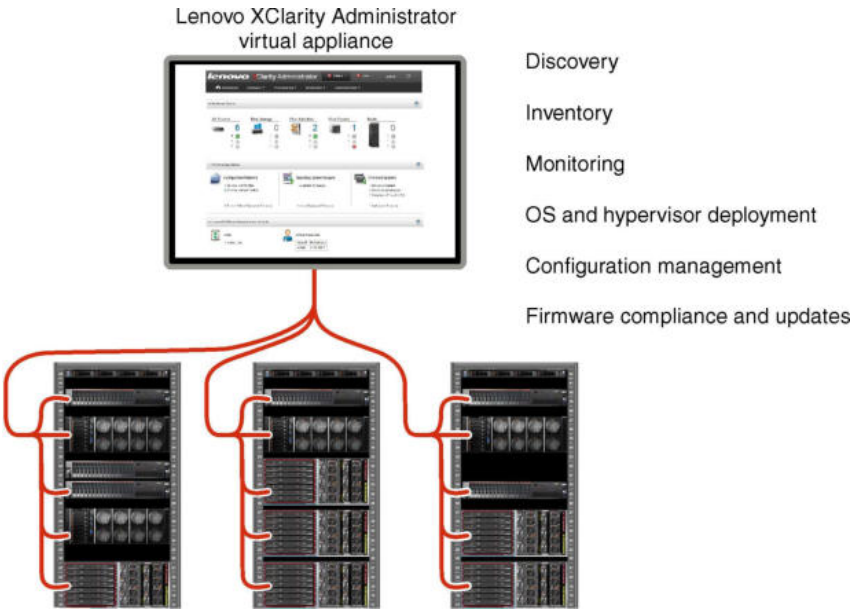
© Copyright Lenovo 2015, 2021

Chapter 1. Lenovo XClarity Administrator Overview

Lenovo XClarity Administrator is a centralized, resource-management solution that simplifies infrastructure management, speeds responses, and enhances the availability of Lenovo® server systems and solutions. It runs as a virtual appliance that automates discovery, inventory, tracking, monitoring, and provisioning for server, network, and storage hardware in a secure environment.

Learn more:

- XClarity Administrator: Managing hardware like software
- XClarity Administrator: Overview



XClarity Administrator provides a central interface to perform the following functions for all managed devices.

Hardware management

XClarity Administrator provides agent-free hardware management. It can automatically discover manageable devices, including server, network, and storage hardware. Inventory data is collected for managed devices for an at-a-glance view of the managed hardware inventory and status.

There are various management tasks for each supported device, including viewing status and properties, and configuring system and network settings, launching the management interfaces, powering on and off, and remote control. For more information about managing devices, see Managing chassis, Managing servers, and Managing switches.

Tip: Server, network, and storage hardware that can be managed by XClarity Administrator is referred to as *devices*. Hardware that is under XClarity Administrator management is referred to as *managed devices*.

You can use the rack view in XClarity Administrator to group your managed devices to reflect the physical rack setup in your datacenter. For more information about racks, see Managing racks.

Learn more:

- XClarity Administrator: Discovery

© Copyright Lenovo 2015, 2021

- XClarity Administrator: Inventory
- XClarity Administrator: Remote control

Hardware monitoring

XClarity Administrator provides a centralized view of all events and alerts that are generated from the managed devices. An event or alert is passed to the XClarity Administrator and is displayed in the events or alerts log. A summary of all events and alerts is visible from the Dashboard and the Status bar. Events and alerts for a specific device are available from the Alerts and Events detail page for that device.

For more information about monitoring hardware, see Working with events and Working with alerts.

Learn more: XClarity Administrator: Monitoring

Configuration management

You can quickly provision and pre-provision all of your servers using a consistent configuration. Configuration settings (such as local storage, I/O adapters, boot settings, firmware, ports, and management controller and UEFI settings) are saved as a server pattern that can be applied to one or more managed servers. When the server patterns are updated, the changes are automatically deployed to the applied servers.

Server patterns also integrate support for virtualizing I/O addresses, so you can virtualize Flex System fabric connections or repurpose servers without disruption to the fabric.

For more information about configuring servers, see Configuring servers using configuration patterns.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Configuration patterns

Firmware compliance and updates

Firmware management is simplified by assigning firmware-compliance policies to managed devices. When you create and assign a compliance policy to managed devices, XClarity Administrator monitors changes to the inventory for those devices and flags any devices that are out of compliance.

When a device is out of compliance, you can use XClarity Administrator to apply and activate firmware updates for all devices in that device from a repository of firmware updates that you manage.

Note: Refreshing the repository and downloading firmware updates requires an Internet connection. If XClarity Administrator has no Internet connection, you can manually import firmware updates to the repository.

For more information about updating firmware, see Updating firmware on managed devices.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Firmware updates
- XClarity Administrator: Provisioning firmware security updates

Operating-system deployment

You can use XClarity Administrator to manage a repository of operating-system images and to deploy operating-system images to up to 28 servers managed servers concurrently.

For more information about deploying operating systems, see Installing operating systems on bare-metal servers.

Learn more:

-  XClarity Administrator: Bare metal to cluster
-  XClarity Administrator: Operating-system deployment

User management

XClarity Administrator provides a centralized authentication server to create and manage user accounts and to manage and authenticate user credentials. The authentication server is created automatically when you start the management server for the first time. The user accounts that you create for XClarity Administrator can also be used to log in to managed chassis and servers in managed-authentication mode. For more information about users, see Managing user accounts.

XClarity Administrator supports three types of authentication servers:

- **Local authentication server**. By default, XClarity Administrator is configured to use the local authentication server that resides on the management node.
- **External LDAP server**. Currently, only Microsoft Active Directory is supported. This server must reside on an outboard Microsoft Windows server that is connected to the management network. When an external LDAP server is used, the local authentication server is disabled.
- **External SAML 2.0 identity provider**. Currently, only Microsoft Active Directory Federation Services (AD FS) is supported. In addition to entering a user name and password, multi-factor authentication can be set up to enable additional security by requiring a PIN code, reading smart card, and client certificate.

For more information about authentication types, see Managing the authentication server.

When you create a user account, you assign a predefined or customized role group to the user account to control the level of access for that user. For more information about role groups, see Creating a custom role group.

XClarity Administrator includes an audit log that provides a historical record of user actions, such as logging on, creating new users, or changing user passwords. For more information about the audit log, see Working with events.

Device authentication

XClarity Administrator uses the following methods for authenticating with managed chassis and servers.

- **Managed authentication**. When managed authentication is enabled, the user accounts that you create in XClarity Administrator are used to authenticate managed chassis and servers.

  For more information about users, see Managing user accounts .
- **Local authentication**. When managed authentication is disabled, the stored credentials that are defined in XClarity Administrator are used to authenticate managed servers. The stored credentials must correspond to an active user account on the device or in Active Directory.

  For more information about stored credentials, see Managing stored credentials.

Security

If your environment must comply with NIST SP 800-131A standards, XClarity Administrator can help you achieve a fully compliant environment.

XClarity Administrator supports self-signed SSL certificates (which are issued by an internal certificate authority) and external SSL certificates (which are issued by a private or commercial CA).

Firewalls on chassis and servers can be configured to accept incoming requests from only XClarity Administrator.

For more information about security, see Implementing a secure environment.

Service and support

XClarity Administrator can be set up to collect and send diagnostic files automatically to your preferred service provider when certain serviceable events occur in XClarity Administrator and the managed devices. You can choose to send diagnostic files to Lenovo Support using Call Home or to another service provider using SFTP. You can also manually collect diagnostic files, open a problem record, and send diagnostic files to the Lenovo Support Center.

Learn more: XClarity Administrator: Service and support

Task automation using scripts

XClarity Administrator can be integrated into external, higher-level management and automation platforms through open REST application programming interfaces (APIs). Using the REST APIs, XClarity Administrator can easily integrate with your existing management infrastructure.

The PowerShell toolkit provides a library of cmdlets to automate provisioning and resource management from a Microsoft PowerShell session. The Python toolkit provides a Python-based library of commands and APIs to automate provisioning and resource management from an OpenStack environment, such as Ansible or Puppet. Both of these toolkits provide an interface to XClarity Administrator REST APIs to automate functions such as:

- Logging in to XClarity Administrator
- Managing and unmanaging chassis, servers, storage devices, and top-of-rack switches (devices)
- Collecting and viewing inventory data for devices and components
- Deploying an operating-system image to one or more servers
- Configuring servers through the use of Configuration Patterns
- Applying firmware updates to devices

Integration with other managed software

XClarity Administrator modules integrate XClarity Administrator with third-party management software to provide discovery, monitoring, configuration, and management functions to reduce the cost and complexity of routine system administration for supported devices.

For more information about XClarity Administrator, see the following documents:

- Lenovo XClarity Integrator for Microsoft System Center
- Lenovo XClarity Integrator for VMware vCenter
- Lenovo XClarity Integrator for Nutanix Prism

For additional considerations, see Using management software other than the XClarity Administrator in the XClarity Administrator online documentation.

Learn more:

- Lenovo XClarity Integrator for Microsoft System Center overview
- Lenovo XClarity Integrator for Nutanix
- Lenovo XClarity Integrator for VMware vCenter

Documentation

The XClarity Administrator documentation is updated regularly online in English See the XClarity Administrator online documentation for the most current information and procedures.

The online documentation is available in the following languages:

- German (de)
- English (en)
- Spanish (es)
- French (fr)

- Italian (it)
- Japanese (ja)
- Korean (ko)
- Brazilian Portuguese (pt_BR)
- Russian (ru)
- Thai (th)
- Simplified Chinese (zh_CN)
- Traditional Chinese (zh_TW)

You can change the language of the online documentation in the following ways:

- Change the language setting in your web browser
- Append `?lang=<language_code>` to the end of URL, for example, to display the online documentation in Simplified Chinese:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**?lang=zh_CN**

Logging in to Lenovo XClarity Administrator

Log in to the Lenovo XClarity Administrator web interface using a supported web browser.

Before you begin

Ensure that you are using one of the following supported web browsers:
- Chrome™ 48.0 or later (55.0 or above for Remote Console)
- Firefox® ESR 38.6.0 or later
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 or later (IOS7 or later and OS X)

Note: Launching the management-controller interfaces from XClarity Administrator using the Safari web browser is not supported.

Ensure that you log in to the XClarity Administrator web interface from a system that has network connectivity to XClarity Administrator management node.

Procedure

Complete the following steps to log in to the XClarity Administrator web interface.

Step 1. Point your browser to the IP address of XClarity Administrator.

Note: If you have Eth0 and Eth1 networks on separate subnets, and if DHCP is used on both subnets, use the *Eth1* IP address when accessing the web interface for initial setup. When XClarity Administrator starts for the first time, both Eth0 and Eth1 get a DHCP-assigned IP address, and the XClarity Administrator default gateway is set to the DHCP-assigned gateway for *Eth1*.

Tip: Access to the web interface is through a secure connection. Ensure that you use **https**.

Using static a IPv4 address

If you specified an IPv4 address in eth0_config, use that IPv4 address to access XClarity Administrator using the following URL:
`https://<IPv4_address>/ui/login.html`

For example:
`https://192.0.2.10/ui/login.html`

Using a DHCP server in the same broadcast domain as XClarity Administrator

If a DHCP server is set up in the same broadcast domain as XClarity Administrator, use the IPv4 address that is displayed in the XClarity Administrator virtual-machine console to access XClarity Administrator using the following URL:
`https://<IPv4_address>/ui/login.html`

For example:
`https://192.0.2.10/ui/login.html`

Using a DHCP server in a different broadcast domain as XClarity Administrator

If a DHCP server *is not* set up in the same broadcast domain, use the IPv6 Link-Local Address (LLA) that is displayed for eEth0 (the management network) in the XClarity Administrator virtual-machine console to access XClarity Administrator, for example:

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0     Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56
         inet addr: 192.0.2.10  Bcast 192.0.2.55  Mask 255.255.255.0
         inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link

eth1     Link encap:Ethernet  HWaddr 2001:db8:64:23:45:67
         inet addr: 192.0.2.20  Bcast 192.0.2.130 Mask 255.255.255.0
         inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

Tip: The IPv6 link local address (LLA) is derived from the MAC address of the interface.

Attention: If you are configuring XClarity Administrator remotely, you must have connectivity to the same layer 2 network. It must be accessed from a non-routed address until the initial setup is complete. Therefore, consider accessing XClarity Administrator from another VM that has connectivity to XClarity Administrator. For example, you can access XClarity Administrator from another VM on the host where XClarity Administrator is installed.

- **Firefox:**

  To access the XClarity Administrator web interface from a Firefox browser, log in using the following URL. Note that brackets are required when entering IPv6 addresses.

  `https://[<IPv6_LLA>/ui/login.html]`

  For example, based on the previous example shown for Eth0, enter the following URL in your web browser:

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

- **Internet Explorer:**

  To access the XClarity Administrator web interface from an Internet Explorer browser, log in using the following URL. Note that brackets are required when entering IPv6 addresses.

  `https://[<IPv6_LLA>%25<zone_index>]/ui/login.html`

  where <*zone_index*> is the identifier for the Ethernet adapter that is connected to the management network from the computer on which you launched the web browser. If you are using a browser on Windows, use the **ipconfig** command to find the zone index, which is displayed after the percent sign (%) in the **Link-Local IPv6 Address** field for the adapter. In the following example, the zone index is “30.”

```
PS C:> ipconfig
Windows IP Configuration

Ethernet adapter vEthernet (teamVirtualSwitch):

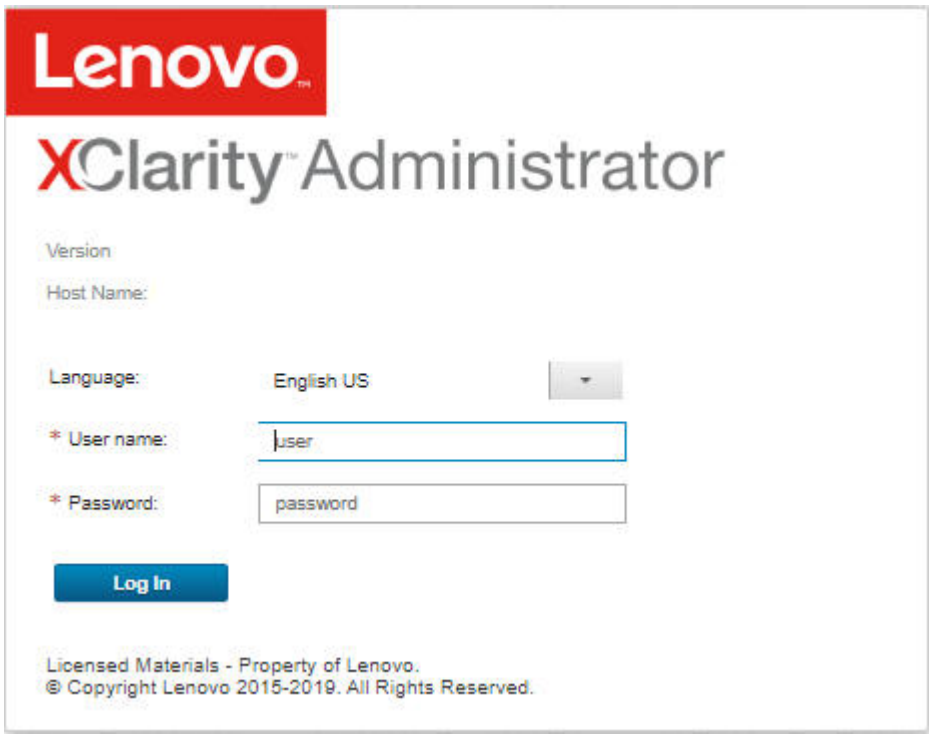
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : 2001:db8:56ff:fe80:bea3%30
   Autoconfiguration IPv4 Address. . : 192.0.2.30
   Default Gateway . . . . . :
```

If you are using a browser on Linux, use the **ifconfig** command to find the zone index. You can also use the name of the adapter (typically Eth0) as the zone index.

For example, based on the examples shown for Eth0 and the zone index, enter the following URL in your web browser:

```
https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html
```

The XClarity Administrator initial login page is displayed:



Step 2. Select the desired language from the **Language** drop-down list.

Note: The configuration settings and values that are provided by the managed devices might be available only in English.

Step 3. Enter a valid user ID and password, and click **Log In**.

The first time you log in with a user account, you are required to change the password. Passwords must meet the following criteria:

- Must contain eight or more characters with at least one number (0 - 9) and one alphabetical character (a - z, A - Z)
- Cannot contain spaces
- Cannot repeat or reverse the user name
- Cannot use more than three of the same characters consecutively
- Must contains at least *two* of the following combinations:

- One uppercase alphabetical character
- One lowercase alphabetical character
- One of the following special characters: ; @ _ ! ' $ & +

What to do next

The XClarity Administrator dashboard page is displayed:



Note: If the host operating system is shut down unexpectedly, you might receive an authentication error when you attempt to log in to XClarity Administrator. To resolve this problem, restore XClarity Administrator from the last backup to access the management server (see Backing up Lenovo XClarity Administrator).

You can perform the following actions from the user-actions menu (

) on the XClarity Administrator title bar.

- Find information about how to use XClarity Administrator in the embedded help system by clicking **Help**.

  The XClarity Administrator documentation is updated regularly online in English See the XClarity Administrator online documentation for the most current information and procedures.
- View the XClarity Administrator license by clicking **License**.
- View information about the XClarity Administrator release by clicking **About**.
- Change the language of the user interface by clicking **Change language**.
- Log out of the current session by clicking **Log out**.
- Submit ideas or provide feedback about XClarity Administrator by clicking **Submit ideas** or **Submit feedback**.
- Ask questions and find answers on the Lenovo XClarity Community forum website by clicking **Visit forum**.

User interface tips and techniques

Consider these tips and techniques when using the Lenovo XClarity Administrator user interface

Viewing more or less data per page

You can change the number of rows that are displayed per page using the links on the bottom right of the table. You can display **10**, **25**, **50**, or **All** rows

Finding data in large lists

Most fields can accept up to 128 characters.

There are several ways to display a subset of a large list based on specific criteria.

- You can sort the table rows by clicking the column header.

  Changing the sort order of a table column is persistent across the user sessions.
- You can use the **Filter By** icons and **Show** drop-down list that is available on some pages to display a subset of data based on the selected criteria.
- You can further refine the subset by entering text (such as a name or IP address) in the **Filters** field to find data that is found in any available column.

  You can choose from the past 10 searches by selecting the searches from the drop-down menu on the **Filters** field. The last active search on a page is persistent across user sessions.

Viewing column data

If the column size prevents all information from displaying in the table cell (indicated by an ellipsis), you can view the complete information in a popup by hovering over text in the cell.

Configure table columns

You can configure tables to show information that is important to you.

- You can choose which columns to show or hide by clicking **All Actions → Toggle Columns**.
- You can reorder columns by dragging the column headers to the preferred location.

Changing the language of the user interface

You have an option to set the language of the user interface when you first log in.

After you are logged in, you can change the language of the user interface by clicking the user-actions menu(

), and then clicking **Change language**. Select the language that you want to display.

Note: The help system displays in the same language that is set for the user interface

Getting help

XClarity Orchestrator offers several ways to get help with the user interface.

- Some pages provide additional details about a specific field or status using **Help** icons ( ). Hover the cursor over the icon to display a pop-up with helpful information.
- To get help about how to perform specific actions from the user interface, click the user-actions menu (

) and then click **Help**.

Using the Lenovo XClarity Mobile app

Lenovo XClarity Administrator offers a mobile app for Android and iOS devices. You can use the Lenovo XClarity Mobile app to securely monitor physical systems, get real-time status alerts and notifications, and take action on common system level tasks. The app can also connect directly via an enabled USB port to a ThinkSystem server and provide virtual LCD capability.

Learn more:  Lenovo XClarity Mobile app overview

Using the XClarity Mobile app, you can perform the following activities:

- Configure network settings and properties
- View the status summary of each connected XClarity Administrator.
- View the status summary of all managed devices.
- Display graphical views (maps) for chassis, rack servers, and storage devices.
- View resource groups that are defined on the XClarity Administrator.
- View rack-switch port information and change configured port status.
- Monitor the inventory and detailed status of each managed device.
- Monitor audit events, hardware and management events, alerts, and jobs.
- Turn on or off the location LED on a managed device.
- Power on, power off, restart, or reseat a managed device.
- Trigger the collection of diagnostic data.
- View device warranty information and status
- Set up automatic problem notification through Call Home.
- View the summary of open service tickets and delete service tickets
- Push event notifications to your mobile device (see Forwarding events to mobile devices).
- View the summary of active users and system resource usage
- Send feedback about this mobile app to Lenovo Support.
- Connect your mobile device directly to a ThinkSystem server to manage the server using the XClarity Mobile app (for devices that support USB tethering).
- Download Lenovo XClarity Controller service data when the mobile device is connected to a ThinkSystem server.

You can also connect your mobile device directly to ThinkSystem servers and then launch the XClarity Mobile app and log in to the server's baseboard management controller using the same web and CLI credentials. A menu of additional information and actions is available, including:

- Service
  - Share summary information using email or other means that is provided by the mobile device
  - Clear the event and audit log
  - Download the event and audit log to the mobile-device local storage or transmitting the log by any means that is provided by the mobile device
  - Download the BMC FFDC service file to the mobile-device local storage or transmitting the file by any means that is provided by the mobile device
  - View historical graph data for power, thermal and system usage
  - Enable "One-Touch" service mode, which provides an immediate summary of active alerts and critical device information
- Configuration and Initial Setup
  - Manage a new device using the selected XClarity Administrator
  - Configure server properties, such as location and contact information for initial setup
  - View and changing the IPv4 and IPv6 BMC network interface settings
  - Specify boot order and one-time boot settings
  - Change the front panel USB port assignment
  - View the number of server reboots and total power on hours
- Power Actions

- Power the server on or off, restarting the server, or triggering NMI
- Reset the BMC

Tip: After the app is open, you must refresh the app to see the updated status, inventory, events, and jobs.

Prerequisites

- iOS tablets are supported at iPhone screen-resolution only. Android tablets are not currently supported.
- The following mobile operating systems are supported:
  - Android 7 – 10
  - iOS 10 and later

    Notes:

    - Android 5 is supported only for XClarity Mobile 2.3.0 and earlier.
    - iOS 8 is supported only for XClarity Mobile v1.3.0 and earlier.
    - iOS 9 is supported only for XClarity Mobile v1.3.1 and earlier.
    - Facial recognition that is used on iPhone X/XR/XS devices is not supported.
- XClarity Mobile can connect to XClarity Administrator 1.2.1 or later.
- Ensure that a network connection is available from your mobile device to the XClarity Administrator instances. This might require the use of a VPN solution. See your network administrator for assistance.
- Import the CA certificate for each XClarity Administrator instance.

  Important: All connections to XClarity Administrator use HTTPS. However, there must be a valid certificate chain before the connection is considered trusted and data can be passed to the mobile device. To create a trusted certificate chain, you must import the XClarity Administrator self-signed certificate authority (CA) into the mobile device.

  To import the self-signed CA certificate for *each XClarity Administrator instance* into the mobile device, complete the following steps.

  1. Download the CA certificate to a local system:
     a. Connect to the XClarity Administrator instance using a web browser on your local system.
     b. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.
     c. Click **Certificate Authority** under the Certificate Management section. The Certificate Authority page is displayed.
     d. Click **Download Certificate Authority Root Certificate**.

        Attention: Normally, it is not necessary to click **Regenerate Certificate Authority Root Certificate** to complete this process. Doing so might disrupt communication with managed devices unless the correct procedure is followed. For more information, see Working with security certificates.
     e. Click **Save as der** or **Save as pem** to save the CA certificate as a DER or PEM file on your local system. PEM format works in most cases.
  2. Transfer the CA certificate file to your mobile device, for example, by using an accessible storage repository (such as Dropbox™), email, or file transfer through a connected cable.
  3. Import the trusted CA certificate:
     - (Android) Typically this is done by selecting **Settings → Security → Install** from phone storage, and then selecting the certificate file that you downloaded.

Important: If your successfully installed CA certificate is not signed by a third party, the `Network may be monitored by an unknown third-party` message is displayed on Android devices. Because the CA certificate is generated in your trusted environment, this message can be safely ignored. Ensure that the message is for the XClarity Administrator CA certificate before ignoring the message.

– (iOS) Open the email on your mobile device, and click the document link in the email to import the trusted CA certificate.

Attention: For iOS 10.3 and later, imported certificates are not trusted by default. To trust the certificates, select **Settings → General → About → Certificate Trust Settings**, and then enable the certificate trust.

Installing and setting up

1. Download the XClarity Mobile app from iTunes App Store (iOS) or Google Play Store (Android).

   Note: Users in China can also download the Android version from Lenovo app store (乐商城), Baidu app store website (百度手机助手) or Tencent app store website (应用宝). After logging in to the website, search for "XClarity."

2. To install the app, follow instructions on the mobile device.

   Important: A mobile OS-level security code to unlock screen access is required to use the XClarity Mobile app. If one is not already set up, you are instructed to set one up during installation.

3. Click **Settings** to add or edit connections to multiple XClarity Administrator instances using the automatic discovery or by providing an IP address and user credentials, set a PIN code for the app, change the event and audit log settings, and select your preferred language.

Important: For Android devices, XClarity Mobile app v2.1.0 and earlier is not automatically updated to v2.2.0. You must manually uninstall the current XClarity Mobile app before installing v2.2.0 (see "Resolving issues" for more information).

Updating to XClarity Mobile app v3.0

XClarity Mobile app v3.0 has upgrades to the most modern technologies with emphasis on performance and security. This includes changes to the local storage model, which requires you to reconfigure some settings when updating to the latest app:

- Connections to XClarity Administrator instances (IP addresses or hostnames, user name, and password)
- Security settings, including your four-digit passcode and fingerprint authentication, . if applicable
- Language setting (English is the default)

Connecting directly to ThinkSystem servers

Lenovo Think System servers include a front panel USB port that you can use to connect to your mobile device to provide similar capabilities that were available on the LCD system-information display panel on other Lenovo servers.

To manage a ThinkSystem server by directly connecting to server, complete these steps.

1. Switch the server front panel USB from host to BMC by performing one of the following steps.
   a. From the management controller CLI, run the **usbfp** command
   b. From the management controller web interface, click **BMC Configuration → Network → Front Panel USB Port Management**.
   c. Hold the blue ID location LED on the front panel for at least 3 seconds until the light blinks every couple of seconds.
2. Connect your phone USB cable to the front panel USB port on the ThinkSystem server.

3. On your mobile device, enable USB tethering.
   a. For iOS, click **Settings → Cellular → Personal Hotspot**.
   b. For Android, click **Settings → Mobile hotspot and tethering → USB tethering**.
4. On your mobile device, launch the XClarity Mobile app.
5. If automatic discovery is disabled, click **Discovery** on the USB Discovery page to connect to the server's management controller and collect information, including inventory, health, firmware, network configuration, and a list of the latest active events.

Tip:

- Ensure that you use a high-quality USB cable that supports data and power. Be aware that some cables that are supplied with mobile devices are only for charging purposes.

  Note: To connect to ThinkSystem SD530, you must also use a high-quality micro USB to USB cable or adapter.
- The USB-attached server must be powered on to report the full set of voltage, temperature, and usage statistics in the summary status cards.
- If the USB-attached server does not have an external "blue identification" LED/button on the front panel, you must use the management controller web interface or CLI to change the front panel USB port management selection, if needed.
- Changes made to the management-controller network interface from the XClarity Mobile app take effect immediately without requiring management controller to be restarted. For example, if the IPv4 interface is changed from a static address to DHCP, the interface immediately obtains a DHCP assigned address.
- On the Newsfeed tab, the "Latest active events" card initially displays up to three active events that are listed on the management controller's Active Events tab. On the mobile app, if you tap that card, all of the active events are displayed. Note that this is a list of active and resolved events, not a full list of all events.
- When using the XClarity Mobile app v1.3.2 to connect to XClarity Administrator v1.3.0 and later, some data that is received from the XClarity Administrator (such as event logs) might not be fully translated in supported languages.

Using demonstration mode

You can enable **Demonstration Mode** on the Settings page to populate the XClarity Mobile app with demo data for two XClarity Administrator instances, including racks and chassis. In this mode, you can view the status summary of the XClarity Administrator instances, view detailed status and inventory of devices, and monitor events and alerts. However, management actions, such as powering on and off, are not supported.

Notes:

- You can enable demonstration mode only when there are no connections to actual XClarity Administrator instances.
- You cannot add connections to actual XClarity Administrator instances while demonstration mode is enabled.

Searching

You can use the **Search** field to display managed devices with a specific name or status (Critical, Warning, or Normal). For example, if you search for "crit," only managed devices in the Critical status and with names that include "crit" are displayed.

Resolving issues

Installation issues:

- Typically, when a new version of the Android mobile app is posted to the app store, the app automatically updated on your mobile device. However, due to enhanced security measures, the newly released mobile app v2.2.0 is no longer updated automatically. This is a one-time "transition" issue and only affects the upgrade to v2.2.0. Subsequent updates will operate as expected.

  The Android mobile app is "signed" with a secure key to enhance security. The secure key size was increased in the new release. Because the signed app does not match the earlier apps signature, the Android installation security process prevents the automatic update.

  To update the mobile app, uninstall the current version of the mobile app, download the latest version of the Android app from the app store, and reinstall the app. On most Android devices, the app can be uninstalled using the **Settings → Applications → Application Manager** menu item.

Connectivity issues:

- The USB tethering function in iOS 14, 14.0.1, and 14.0.2 is not working correctly, and therefore, the Lenovo XClarity Mobile app tethering function is not available for these iOS versions. This affects only the USB-attached handheld management in the datacenter. Remote management using mobile devices that support cellular and Wi-Fi communications are not affected and can be used to connect and collect data from XClarity Administrator and to perform management actions on managed devices.

  If the USB-attached handheld management function is needed, do not upgrade to iOS 14.

  This notification will be updated when Apple resolves the issue with iOS 14.
- XClarity Mobile requires an available network connection from your mobile device to the XClarity Administrator instances. This might require the use of a VPN solution. See your network administrator for assistance.
- Connections from your mobile device to each XClarity Administrator instance require a trusted certificate chain. See the online documentation for instructions to download and install the trusted CA certificates on your mobile device.

  If your successfully installed CA certificate is not signed by a third party, the `Network may be monitored by an unknown third-party` message is displayed. Because the CA certificate is generated in your trusted environment, this message can be safely ignored. Ensure that the message is for the XClarity Administrator CA certificate before ignoring the message.
- When switching your mobile device from a virtual private network (VPN) to a local network or vice versa, you might see the message `The secure gateway has rejected the connection attempt. A new connection attempt to the same or other secure gateway is needed, which requires reauthentication.` Log on to Lenovo XClarity Mobile to continue using the app.

Security issues:

- If you forget your PIN code, uninstall and reinstall the XClarity Mobile app. Then, re-establish all connections.
- If you clear credentials on an Android device, the encryption key is erased. You must re-establish all connections.

Event issues:

- By default, the event log shows hardware and management events that were received in the last 24 hours, and the audit log shows audit events that were received in the last 2 hours. If no events were received during the selected time periods, then the event log and audit log are not shown on the Monitoring page in XClarity Mobile.
- If you set up event forwarding in XClarity Administrator to send events to an email account, links in the email might not work on Android devices. Ensure that your version of Android and your email app support hyperlinks. If hyperlinks are unsupported, use another email app.

Help system issues:

- On some devices, the help system does not scale correctly to the size of the screen. Use the help-system controls to maximize and then minimize the page.

Chapter 2. Administering Lenovo XClarity Administrator

Several administration tasks, such as adding users or viewing jobs, are available from Lenovo XClarity Administrator.

Managing authentication and authorization

Lenovo XClarity Administrator provides security mechanisms to verify a user's credentials and control access to resources and tasks.

Managing the authentication server

By default, Lenovo XClarity Administrator uses a local Lightweight Directory Access Protocol (LDAP) server to authenticate user credentials.

About this task

Supported authentication servers

The *authentication server* is a user registry that is used to authenticate user credentials. Lenovo XClarity Administrator supports three types of authentication servers:

- **Local authentication server**. By default, XClarity Administrator is configured to use the embedded Lightweight Directory Access Protocol (LDAP) server that resides in the management server.
- **External LDAP server**. Currently, only Microsoft Active Directory and OpenLDAP are supported. This server must reside on an outboard Microsoft Windows server that is connected to the management network. When an external LDAP server is used, the local authentication server is disabled.

  Attention: To configure the Active Directory binding method to use login credentials, the baseboard management controller for each managed server must be running firmware from September 2016 or later.
- **External identity-management system**. Currently only CyberArk is supported.

  If user accounts for a ThinkSystem or ThinkAgile server are onboarded onto CyberArk, when the server Is initially setup for management using managed authentication, XClarity Administrator retrieves the credentials to authenticate to the server from CyberArk. Before credentials can be retrieved from CyberArk, the CyberArk paths must be defined in XClarity Administrator and mutual trust must be established between CyberArk and XClarity Administrator using TLS mutual authentication through client certificates.
- **External SAML identity provider**. Currently, only Microsoft Active Directory Federation Services (AD FS) is supported. In addition to entering a user name and password, multi-factor authentication can be set up to enable additional security by requiring a PIN code, reading smart card, and client certificate. When an SAML identity provider is used, the local authentication server is not disabled. Local user accounts are required to log in directly to a managed chassis or server (unless Encapsulation is enabled on that device), for PowerShell and REST API authentication, and for recovery if external authentication is not available.

  You can choose to use both an external LDAP server and an external identity provider. If both are enabled, the external LDAP server is used to log in directly to the manage devices, and the identity provider is used to log in to the management server.

Device authentication

© Copyright Lenovo 2015, 2021

By default, devices are managed using XClarity Administrator managed authentication to log in to the devices. When managing rack servers and Lenovo chassis, you can choose to use local authentication or managed authentication to log in to the devices.

- When *local authentication* is used for rack servers, Lenovo chassis, and Lenovo rack switches, XClarity Administrator uses a stored credential to authenticate to the device. The *stored credential* can be an active user account on the device or a user account in an Active Directory server.

  You must create a stored credential in XClarity Administrator that matches an active user account on the device or a user account in an Active Directory server before managing the device using local authentication (see Managing stored credentials in the XClarity Administrator online documentation).

  Notes:

  – RackSwitch devices support only stored credentials for authentication. XClarity Administrator user credentials are not supported.

- Using *managed authentication* allows you to manage and monitor multiple devices using credentials in the XClarity Administrator authentication server instead of local credentials. When managed authentication is used for a device (other than ThinkServer servers, System x M4 servers, and switches), XClarity Administrator configures the device and its installed components to use the XClarity Administrator authentication server for centralized management.

  – When managed authentication is enabled, you can manage devices using either manually-entered or stored credentials (see Managing user accounts and in the XClarity Administrator online documentation).

    The stored credential is used only until XClarity Administrator configures the LDAP settings on the device. After that, any change to the stored credential has no impact the management or monitoring of that device.

    Note: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.

  – If a local or external LDAP server is used as the XClarity Administrator authentication server, user accounts that are defined in the authentication server are used to log in to XClarity Administrator, CMMs and baseboard management controllers in the XClarity Administrator domain. Local CMM and management controller user accounts are disabled.

  – If an SAML 2.0 identity provider is used as the XClarity Administrator authentication server, SAML accounts are not accessible to managed devices. However, when using an SAML identity provider and an LDAP server together, if the identity provider uses accounts that exist in the LDAP server, LDAP user accounts can be used to log into the managed devices while the more advanced authentication methods that are provided by SAML 2.0 (such as multifactor authentication and single sign-on) can be used to log into XClarity Administrator.

  – When managed authentication is enabled for ThinkSystem SR635 and SR655 servers:

    – Baseboard management-controller firmware supports up to five LDAP user roles. XClarity Administrator adds these LDAP user roles to the servers during management: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin**, and **lxc-os-admin**.

      Users must be assigned to at least one of the specified LDAP user roles to communicate with ThinkSystem SR635 and SR655 servers.

    – Management-controller firmware does not support LDAP users with the same username as local user of the sever.

  – For ThinkServer and System x M4 servers, the XClarity Administrator authentication server is not used. Instead, an IPMI account is created on the device with the prefix “LXCA_” followed by a random string. (The existing local IPMI user accounts are not disabled.) When you unmanage a ThinkServer server, the “LXCA_” user account is disabled, and the prefix “LXCA_” is replaced with the prefix “DISABLED_”. To determine whether a ThinkServer server is managed by another instance, XClarity Administrator checks

for IPMI accounts with the prefix “LXCA_”. If you choose to force management of a managed ThinkServer server, all the IPMI accounts on the device with the “LXCA_” prefix are disabled and renamed. Consider manually clearing IPMI accounts that are no longer used.

In XClarity Administrator v2.4 and later, if you use manually-entered credentials, XClarity Administrator automatically creates a stored credential and uses that stored credential to manage the device.

Notes: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.

– Each time you manage a device using manually-entered credentials, a new stored credential is created for that device, even if another stored credential was created for that device during a previous management process.
– When you unmanage a device, XClarity Administrator does not delete stored credentials there were automatically created for that device during the management process.

Recovery account

If you specify a recovery password, XClarity Administrator disables the local CMM or management-controller user account and creates a new recovery user account (`RECOVERY_ID`) on the device for future authentication. If the management server fails, you can use the `RECOVERY_ID` account to log in to the device to take recovery actions to restore account-management functions on the device until the management node is restored or replaced.

If you unmanage a device that has a `RECOVERY_ID` user account, all local user accounts are enabled, and the `RECOVERY_ID` account is deleted.

- If you change the disabled local user accounts (for example, if you change a password), the changes have no effect on the `RECOVERY_ID` account. In managed-authentication mode, the `RECOVERY_ID` account is the only user account that is activated and operational.
- Use the `RECOVERY_ID` account only in an emergency, for example, if the management server fails or if a network problem prevents the device from communicating with XClarity Administrator to authenticate users.
- The `RECOVERY_ID` password is specified when you discover the device. Ensure that you record the password for later use.

For information about recovering a device management, see “Recovering management with a CMM after a management server failure” on page 206 and “Recovering rack or tower server management after a management server failure” on page 250.

Setting up an external LDAP authentication server

You can choose to use an external LDAP authentication server instead of the local Lenovo XClarity Administrator authentication server on the management node.

Before you begin

The initial setup of XClarity Administrator must be completed before setting up the external authentication server.

The following external authentication servers are supported:

- OpenLDAP
- Microsoft Active Directory. It must reside on an outboard Microsoft Windows server that is connected to the management network, data network, or both

Ensure that all ports that are required for the external authentication server are open on the network and firewalls. For information about port requirements, see Port availability in the XClarity Administrator online documentation.

You must create or rename role groups in the local authentication server to match the groups that are defined in the external authentication server.

Ensure that there are one or more users with **lxc-recovery** authority in the local authentication server. You can use this local user account to authenticate directly to XClarity Administrator when a communication error occurs with the external LDAP server.

Note: When XClarity Administrator is configured to use an external authentication server, the Users Management page in the XClarity Administrator web interface is disabled.

Attention: For Active Directory, to configure the binding method to use login credentials, the baseboard management controller for each managed server must be running firmware from September 2016 or later.

XClarity Administrator performs a connectivity check every 5 minutes to maintain connectivity to configured external LDAP servers. Environments with many LDAP servers might experience high CPU usage during this connectivity check. To achieve the best performance, ensure that most or all of the LDAP servers in the domain are reachable, or set the authentication-server selection method to **Use Pre-Configured Servers** and specify only known, reachable LDAP servers.

Procedure

To configure XClarity Administrator to use an external authentication server, complete the following steps.

Step 1. Set up the user-authentication method for Microsoft Active Directory or OpenLDAP.

If you choose to use non-secure authentication, no additional configuration is required. The Windows Active Directory or OpenLDAP domain controllers use non-secure LDAP authentication by default.

If you choose to use secure LDAP authentication, you must set up the domain controllers to allow secure LDAP authentication. For more information about setting configuring secure LDAP authentication in Active Directory, see the LDAP over SSL (LDAPS) Certificate article on the Microsoft TechNet website.

To verify that the Active Directory domain controllers are configured to use secure LDAP authentication:

- Look for the `LDAP over Secure Sockets layer (SSL) is now available` event in the domain controllers Event Viewer window.
- Use the **ldp.exe** Windows tool to test secure LDAP connectivity with the domain controllers.

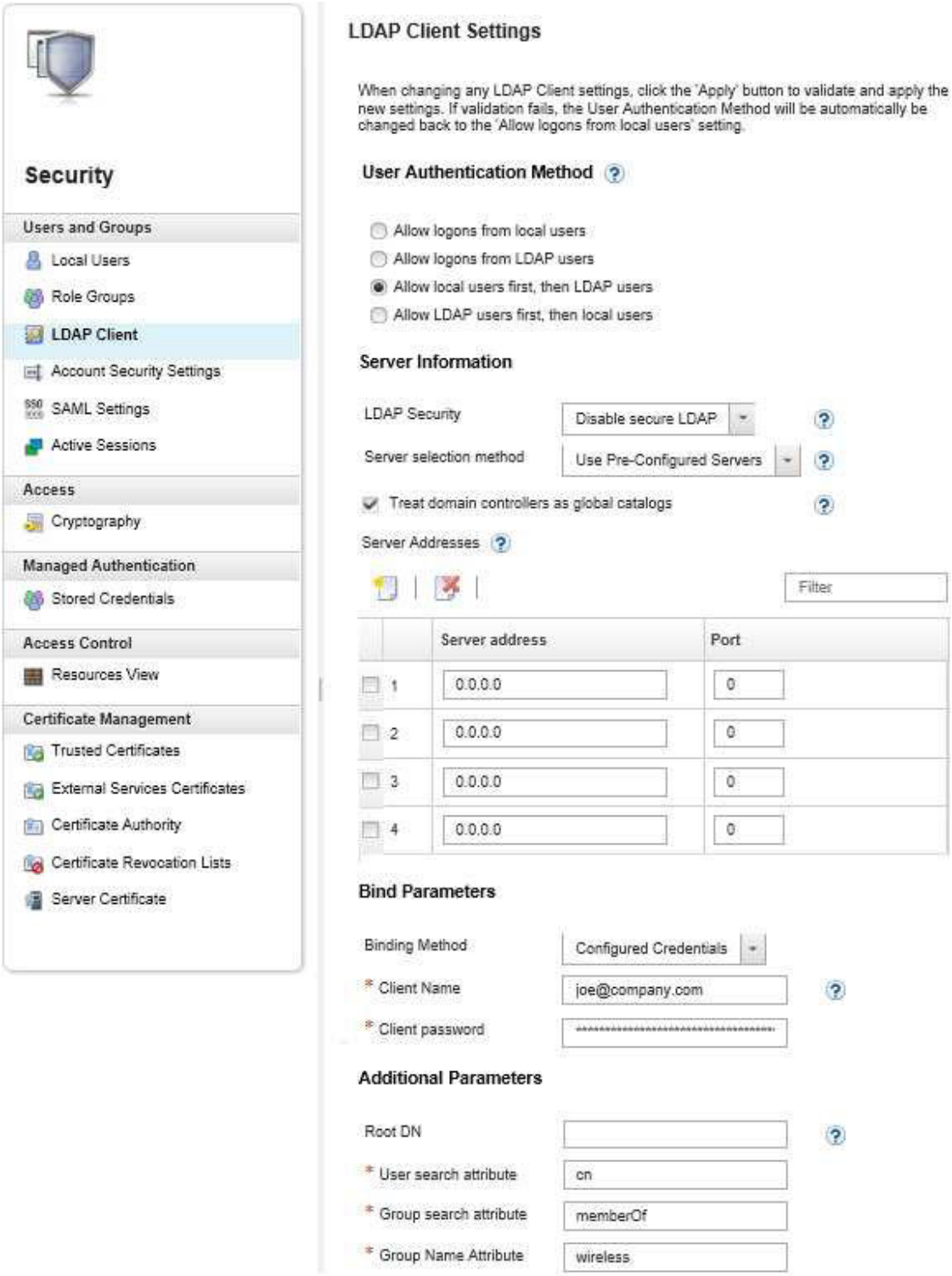
Step 2. Import the Active Directory or OpenLDAP server certificate or the root certificate of the certificate authority that signed the server certificate.

a. From the XClarity Administrator menu bar, click **Administration → Security**.
b. Click **Trusted Certificates** in the Certificate Management section.
c. Click the **Create** icon ( ) to add a certificate.
d. Browse for the file or paste the PEM-formatted certificate text.
e. Click **Create**.

Step 3. Configure the XClarity Administrator LDAP client:

a. From the XClarity Administrator menu bar, click **Administration → Security**.

b. Click **LDAP Client** under the Users and Groups section to display the LDAP Client Settings dialog.



c. Fill in the dialog based on the following criteria.

1. Select one of these user-authentication methods:

- **Allow logons from local users**. Authentication is performed using the local authentication. When this option is selected, all user accounts exist in the local authentication server on the management node.
- **Allow logons from LDAP users**. Authentication is performed by an external LDAP server. This method enables remote management of user accounts. When this option is selected, all user accounts exist remotely in an external LDAP server.
- **Allow local users first, then LDAP users**. The local authentication server performs the authentication first. If that fails, an external LDAP server performs the authentication.
- **Allow LDAP users first, then local users**. An external LDAP server performs the authentication first. If that fails, the local authentication server performs the authentication.

2. Choose whether to enable or disable secure LDAP:
   - **Enable secure LDAP**. XClarity Administrator uses the LDAPS protocol to connect securely to the external authentication server. When this option is selected, you must also configure trusted certificates for the purpose of enabling secure LDAP support.
   - **Disable secure LDAP**. XClarity Administrator uses an unsecure protocol to connect to the external authentication server. If you choose this setting, your hardware might be more vulnerable to security attacks.
3. Select one of these server-selection methods:
   - **Use Pre-Configured Servers**. XClarity Administrator uses the specified IP addresses and ports to discover the external authentication server.

     If you select this option, specify up to four pre-configured server IP addresses and ports. The LDAP client attempts to authenticate using the first server address. If authentication fails, the LDAP client attempts to authenticate using the next server IP address.

     If the port number for an entry *is not* explicitly set to `3268` or `3269`, the entry is assumed to identify a domain controller.

     When the port number is set to `3268` or `3269`, the entry is assumed to identify a global catalog. The LDAP client attempts to authenticate using the domain controller for the first configured server IP address. If this fails, the LDAP client attempts to authenticate using the domain controller for the next server IP address.

     Important: At least one domain controller must be specified, even if the global catalog is specified. Specifying only the global catalog seems to be successful but is not a valid configuration.

     When the cryptography mode is set to NIST-800-131A, XClarity Administrator might not be able to connect to an external LDAP server using a secure port (for example, using LDAPS over default port 636) if the LDAP server is not capable of establishing a Transport Layer Security (TLS) version 1.2 connection with the LDAP client in XClarity Administrator.
   - **Use DNS to find LDAP Servers**. XClarity Administrator uses the specified domain name or forest name to discover the external authentication server dynamically. The domain name and forest name are used to obtain a list of domain controllers, and the forest name is used to obtain a list of global catalog servers.

     Attention: When using DNS to find LDAP servers, ensure that the user account to be used to authenticate to the external authentication server is hosted on specified domain controllers. If the user account is hosted on a child domain controller, include the child domain controller in the service request list.

4. Select one of these binding methods:
   - **Configured Credentials**. Use this binding method to use the client name and password to bind XClarity Administrator to the external authentication server. If the bind fails, the authentication process also fails

     The client name can be any name that the LDAP server supports, including a distinguished name, AMAccountName, NetBIOS name, or UserPrincipalName. The client name must be a user account within the domain that has at least read-only privileges. For example:
     ```
     cn=administrator,cn=users,dc=example,dc=com
     example\administrator
     administrator@example.com
     ```

     Attention: If you change the client password in the external authentication server, ensure that you also updated the new password in XClarity Administrator. For more information, see Cannot log in to XClarity Administrator in the XClarity Administrator online documentation.
   - **Login Credentials**. Use this binding method to use an Active Directory or OpenLDAP user name and password to bind XClarity Administrator to the external authentication server.

     The user ID and password that you specify are used only to test the connection to the authentication server. If successful, the LDAP client settings are saved, but the test login credential that you specified are not save. All future binds use the user name and password that you used to log in to XClarity Administrator.

     Notes:

     – You must be logged in to XClarity Administrator using a fully-qualified user ID (for example, `administrator@domain.com` or `DOMAIN\admin`).

     – You must use a fully qualified test client name for the binding method.

     Attention: To configure the binding method to use login credentials, the management controller for each managed server must be running firmware from September 2016 or later.
5. In the **Root DN** field, it is recommended that you do not specify a root distinguished name, especially for environments with multiple domains. When this field is blank, XClarity Administrator queries the external authentication server for the naming contexts. If you use DNS to discover the external authentication server or if you specify multiple servers (for example, `dc=example,dc=com`), You can optionally specify the top-most entry in your LDAP directory tree. In this case, searches are started using the specified root distinguished name as the search base.
6. Specify the attribute to use to search for the user name.

   When the binding method is set to **Configured Credentials**, the initial bind to the LDAP server is followed by a search request that retrieves specific information about the user, including the user's DN, login permissions, and group membership. This search request must specify the attribute name that represents the user IDs on that server. This attribute name is configured in this field. If this field is left blank, the default is **cn**.
7. Specify the attribute name that is used to identify the groups to which a user belongs. If this field is left blank, the attribute name in the filter defaults to **memberOf**.
8. Specify the attribute name that is used to identify the group name that is configured by the LDAP server. If this field is left blank, the default is **uid**.

d. Click **Apply**.

The XClarity Administrator attempts to test the configuration to detect common errors. If the test fails, error messages are displayed that indicate the source of the errors. If the test succeeds and connections to the specified servers complete successfully, user authentication might still fail if:

- A local user with **lxc-recovery** authority does not exist.
- The root distinguished name is incorrect.
- The user is not a member of at least one group in the external authentication server that matches the name of a role group on the XClarity Administrator authentication server. XClarity Administrator cannot detect whether the root DN is correct; however, it can detect whether a user is a member of at least one group. If a user is not a member of at least one group, an error message is displayed when the user attempts to log in to XClarity Administrator. For more information about troubleshooting issues with the external authentication servers, see Connectivity Issues in the XClarity Administrator online documentation.

Step 4. Create an external user account that can access XClarity Administrator:

a. From the external authentication server, create a user account. For instructions , see the Active Directory or OpenLDAP documentation.

b. Create an Active Directory or OpenLDAP global group with the name of a predefined and authorized group. The group must exist within the context of the root distinguished name that is defined in the LDAP client.

c. Add the Active Directory or OpenLDAP user as a member of the security group that you created previously.

d. Log on to XClarity Administrator using the Active Directory or OpenLDAP user name.

e. **Optional:** Define and create additional groups. You can authorize these groups and assign roles to them from the Users and Groups page.

f. If secure LDAP is enabled, import trusted certificates to the external LDAP server (see Installing a customized, externally signed server certificate).

Results

XClarity Administrator validates the LDAP server connection. If the validation passes, user authentication occurs on the external authentication server when you log in to XClarity Administrator, CMM, and management controller.

If the validation fails, the authentication mode is automatically changed back to the **Allow logons from local users** setting, and a message that explains the cause of the failure is displayed.

Note: The correct role groups must be configured in XClarity Administrator, and user accounts must be defined as member of one of those role groups on the Active Directory server. Otherwise, user authentication fails.

Setting up an external SAML identity provider

You can choose to use a Security Assertion Markup Language (SAML) 2.0 identity provider to perform authentication and authorization for Lenovo XClarity Administrator.

Before you begin

The initial setup of XClarity Administrator must be completed before setting up the identity provider.

The identity provider must be Microsoft Active Directory Federated Service (AD FS) and can be connected to either the management network, data network, or both. Because authentication is done through your web browser, your web browser must be able to access XClarity Administrator and the SAML server.

You can download IDP metadata using the following URL: `https://<ADFS_IP_Address>/federationmetadata/2007-06/federationmetadata.xml`, where *<ADFS_IP_Address>* is the IP address for AD FS (for example, https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml).

You must create or rename role groups in the location authentication server to match the groups that are defined in the external authentication server.

To set up an SAML identity provider, you must be logged in as a user that is a member of the **lxc_admin** or **lxc_supervisor** group.

About this task

XClarity Administrator supports using a Security Assertion Markup Language 2.0 identity provider to authenticate and authorize users. In addition to entering a user name and password, the identity provider can be set up to require additional criteria to validate a user's identity, such as entering a PIN code, reading a smart card, and authenticating using a client certificate.

When XClarity Administrator is set up to use a identity provider, interactive login requests from the XClarity Administrator web interface are redirected to the identity provider for authentication. After the user is authenticated, the web browser is redirected back to XClarity Administrator.

Note: If the identity provider is enabled, you can bypass the identity provider and log in to XClarity Administrator using the local or external LDAP authentication server by opening your web browser to the XClarity Administrator login page (for example, `https://<ip_address>/ui/login.htm`).

When XClarity Administrator is configured to use an identity provider profile, the Users Management page in the XClarity Administrator web interface is not disabled. Local user accounts are required to directly log in to a managed chassis or server (except when Encapsulation is enabled on that device) and for PowerShell and REST API authentication.

Procedure

Complete the following steps to set up an external SAML identity provider (AD FS).

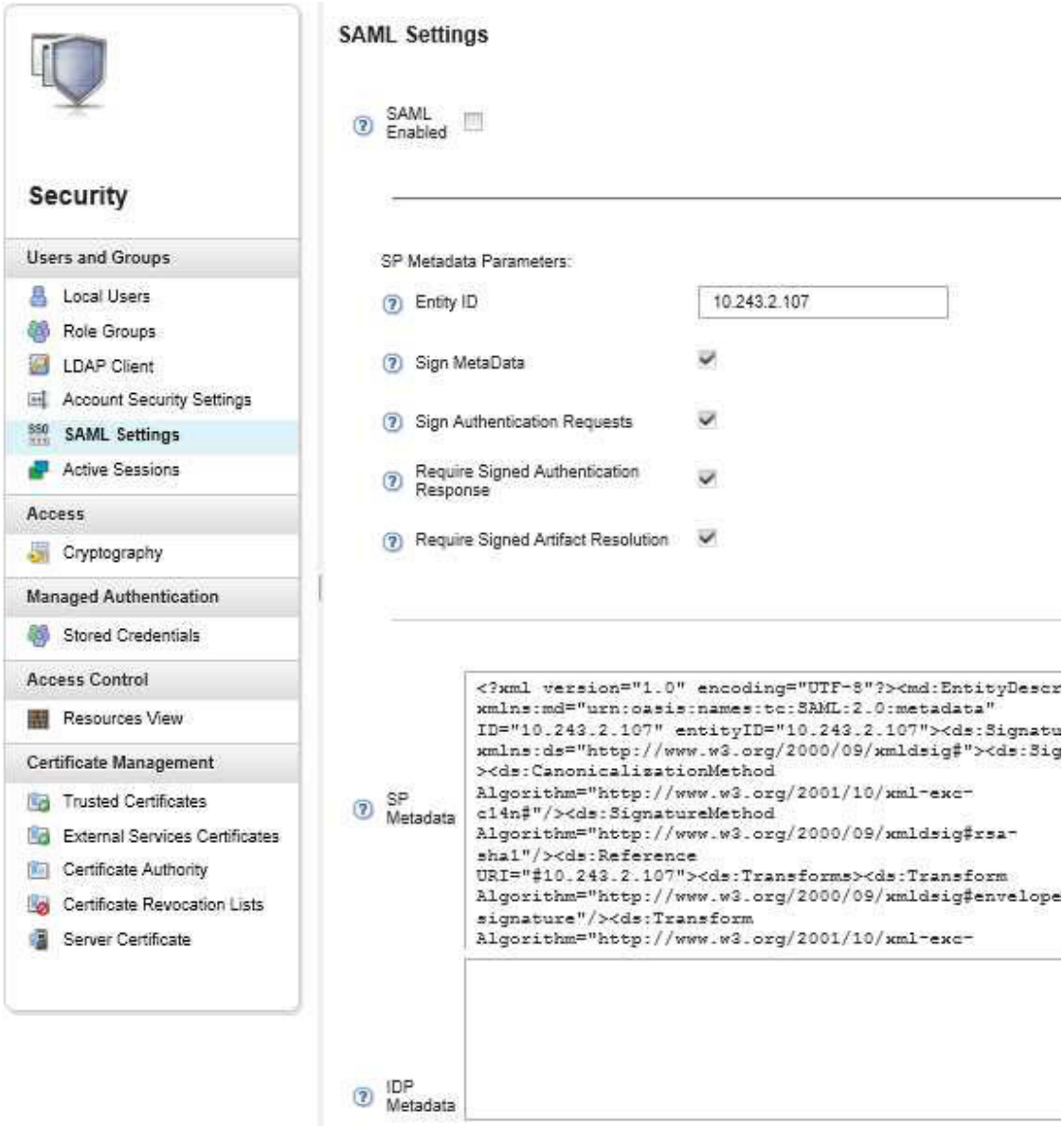
Step 1. Create a recovery user account that can be used to log in to XClarity Administrator if the identity provider becomes unavailable (see Managing user accounts).

Step 2. Retrieve the identity provider (IDP) metadata from the identity provider, and save the file on the XClarity Administrator host.

Step 3. Configure the XClarity Administrator SAML client.

   a. From the XClarity Administrator menu bar, click **Administration → Security**.

   b. Click **SAML Settings** under the Users and Groups section to display the SAML Settings dialog.



c. Fill in the fields on the SAML Settings page:
   1. Verify that the entity ID matches the IP address of the XClarity Administrator management server.
   2. Choose whether the generated metadata is to be digitally signed.
   3. Choose whether authentication requests are to be signed.
   4. Choose whether authentication responses must be signed.
   5. Choose whether the artifact-resolution requests that are sent to the remote identity provider must be signed.
   6. Paste the SAML identity provider (IDP) metadata that was generated by the identity provider and retrieved in step Step 2 3 on page 25 into the **IDP Metadata** field.
d. Click **Apply** to apply the changes and update the text in the SP Metadata field.

   Attention: *Do not* select **SAML Enabled** at this point. You will enable SAML in a later step to restart XClarity Administrator.

e. Copy and paste the data in the **SP Metadata** field to a file, and save the file with the .XML extension (for example, sp_metadata.xml). Copy this file to the AD FS host.

Step 4. Configure AD FS.

a. Open the AD FS Management tool.

b. Click **ADFS → Relying Party Trusts**.

c. Right click **Relying Party Trusts**, then click **Add Relying Party Trust** to display the wizard

d. Click **Start**

e. On the Select Data Source page, select **Import data about the relying party from a file**, and then select the SP metadata file that you saved in step 3e.

f. Enter a display name.

g. Click **Next** on all pages to choose the default values.

h. Click **Finish** to display the Claim Rules page

i. Leave **Send LDAP Attributes as Claims** as default, and click **Next**.

j. Enter a claim rule name.

k. Select **Active Directory** for the attribute store.

l. Add a mapping. On the left side select **SAM-Account-Name**, and on the right side, select **Name ID** for the outgoing claim type.

m. Add another mapping. On the left side, select **Token-Groups-Unqualified Names**, and on the right side select **Group** for the outgoing claim type

n. Click **OK**.

o. Locate the trust that you just created in the list of **Relying Party Trusts**.

p. Right-click the trust, and click **Select properties**. The trust Properties dialog is displayed.

q. Click the **Advanced** tab, and select `SHA-1` as the secure hash algorithm.

Step 5. Save the server certificate from AD FS.

a. Click **AD FS console → Service → Certificates**.

b. Select the **Certificate** under Token-signing.

c. Right-click the certificate, and click **View Certificate**.

d. Click the **Details** tab.

e. Click **Copy to File**, and save the certificate as a DER encoded binary X.509 (.CER) file.

f. Copy the server certificate .CER file to the XClarity Administrator host.

Step 6. Import the AD FS trusted certificate into XClarity Administrator web interface.

a. From the XClarity Administrator menu bar, click **Administration → Security**.

b. Click **Trusted Certificates** in the Certificate Management section.

c. Click the **Create** icon () to add a certificate.

d. Select the server certificate .CER file that you saved in the previous step.

e. Click **Create**.

Step 7. Click **SAML Settings** under the Users and Groups section to display the SAML Settings dialog.

Step 8. Select **SAML Enabled** to enable management of user accounts using an external identity provider. When this option is selected, all user accounts exist remotely in an identity provider.

Step 9. Click **Apply** to apply the changes and restart the management server.

Step 10. Wait a few minutes for XClarity Administrator to restart.

Attention: Do not restart the virtual appliance manually during this process.

Step 11. Close and reopen the web browser.

Step 12. Log in to the XClarity Administrator web interface from the identity provider.

Results

The XClarity Administrator attempts to test the configuration to detect common errors. If the test fails, error messages are displayed that indicate the source of the errors.

XClarity Administrator validates the identity provider connection. If the validation passes, user authentication occurs on the identity provider when you log in to XClarity Administrator.

Setting up an external identity-management system

An *identity-management system* is an external password vault that can optionally be used with Lenovo XClarity Administrator to store XClarity Administrator and XClarity Controller credentials. When an identity-management system is added to XClarity Administrator, XClarity Administrator retrieves passwords from the identity-management system, instead of the authentication servers.

About this task

XClarity Administrator supports the following identity-management system.

- CyberArk

Setting up a CyberArk identity-management system

CyberArk is an external password vault that optionally can be used with Lenovo XClarity Administrator to store Lenovo XClarity Controller credentials. After an account password is stored in CyberArk, the password is managed by CyberArk

About this task

If user accounts for a ThinkSystem or ThinkAgile server are onboarded onto CyberArk, when the server Is initially setup for management using managed authentication, XClarity Administrator retrieves the credentials to authenticate to the server from CyberArk. Before credentials can be retrieved from CyberArk, the CyberArk paths must be defined in XClarity Administrator and mutual trust must be established between CyberArk and XClarity Administrator using TLS mutual authentication through client certificates.

Procedure

To configure XClarity Administrator to use CyberArk, complete the following steps.

Step 1. Configure CyberArk.

1. From the XClarity Administrator menu bar, click **Administration → Security**.
2. Click **CyberArk** under the Identity Management section.
3. Click **Edit CyberArk Server Details** from the toolbar.
4. Specify the CyberArk hostname or IP address, and the port number.
5. Click **Apply**.

Step 2. Import the XClarity Administrator mutual-authentication certificate into CyberArk.

1. From the XClarity Administrator menu bar, click **Administration → Security**.
2. Click **Server Certificate** in the Certificate Management section.
3. Click **Client Certificate** tab.
4. Select **CyberArk** as the server type.

5. Click **Regenerate Certificate** to generate a new TLS mutual-authentication certificate for CyberArk.

   Attention: If you regenerate the TLS mutual-authentication certificate for CyberArk after a connection is established between XClarity Administrator and CyberArk, the connection is lost until you import the new certificate in CyberArk.
6. Click **Download Certificate**, and then click **Save as der** or **Save as pem** to save the certificate as a file to your local system.
7. Import the downloaded certificate into CyberArk.

Step 3. Import the CyberArk root CA certificate in to XClarity Administrator.

1. Download the root CA certificate from CyberArk.
2. From the XClarity Administrator menu bar, click **Administration → Security**.
3. Click **Trusted Certificates** in the Certificate Management section.
4. Click the **Create** icon ( ) to add a certificate.
5. Browse for the file or paste the PEM-formatted certificate text.
6. Click **Create**.

Step 4. Add paths that identify the location of onboarded user accounts in CyberArk.

1. From the XClarity Administrator menu bar, click **Administration → Security**.
2. Click **CyberArk** under the Identity Management section.
3. Click the **Paths** tab.
4. Click the **Create** icon ( ) to display the Create CyberArk Path dialog.



5. Optionally specify the application ID, safe and folder where the user accounts are stored in CyberArk.

   If you specify the application ID and safe and optionally the folder, XClarity Administrator attempt to find the user account in the specified location.

   If you specify a combination of fields other than application ID and safe (for example, if you specify only the application ID, only the safe and folder, or only the application ID and folder), XClarity Administrator filters the path using the specified values.
6. Click **Apply**.

What to do next

- Modify a selected CyberArk path by clicking the **Edit** icon ( ).
- Delete a selected CyberArk path by clicking the **Delete** icon ( ).

Determining the type of authentication method that is used by Lenovo XClarity Administrator

You can determine the type of authentication method that is used currently from the **LDAP Client** and **SAML Settings** tabs on the Security page.

About this task

The *authentication server* is a user registry that is used to authenticate user credentials. Lenovo XClarity Administrator supports three types of authentication servers:

- **Local authentication server**. By default, XClarity Administrator is configured to use the embedded Lightweight Directory Access Protocol (LDAP) server that resides in the management server.
- **External LDAP server**. Currently, only Microsoft Active Directory and OpenLDAP are supported. This server must reside on an outboard Microsoft Windows server that is connected to the management network. When an external LDAP server is used, the local authentication server is disabled.

  Attention: To configure the Active Directory binding method to use login credentials, the baseboard management controller for each managed server must be running firmware from September 2016 or later.
- **External identity-management system**. Currently only CyberArk is supported.

  If user accounts for a ThinkSystem or ThinkAgile server are onboarded onto CyberArk, when the server Is initially setup for management using managed authentication, XClarity Administrator retrieves the credentials to authenticate to the server from CyberArk. Before credentials can be retrieved from CyberArk, the CyberArk paths must be defined in XClarity Administrator and mutual trust must be established between CyberArk and XClarity Administrator using TLS mutual authentication through client certificates.
- **External SAML identity provider**. Currently, only Microsoft Active Directory Federation Services (AD FS) is supported. In addition to entering a user name and password, multi-factor authentication can be set up to enable additional security by requiring a PIN code, reading smart card, and client certificate. When an SAML identity provider is used, the local authentication server is not disabled. Local user accounts are required to log in directly to a managed chassis or server (unless Encapsulation is enabled on that device), for PowerShell and REST API authentication, and for recovery if external authentication is not available.

  You can choose to use both an external LDAP server and an external identity provider. If both are enabled, the external LDAP server is used to log in directly to the manage devices, and the identity provider is used to log in to the management server.

Procedure

To determine the type of authentication server that is being used by the management software, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **LDAP Client** under the Users and Groups section to display the LDAP Client Settings dialog.

Verify which user-authentication method is selected:

- **Allow logons from local users**. Authentication is performed using the local authentication. When this option is selected, all user accounts exist in the local authentication server on the management node.
- **Allow logons from LDAP users**. Authentication is performed by an external LDAP server. This method enables remote management of user accounts. When this option is selected, all user accounts exist remotely in an external LDAP server.
- **Allow local users first, then LDAP users**. The local authentication server performs the authentication first. If that fails, an external LDAP server performs the authentication.

- **Allow LDAP users first, then local users**. An external LDAP server performs the authentication first. If that fails, the local authentication server performs the authentication.

Step 3. Click **SAML Settings** under the Users and Groups section to display the SAML Settings page.

If **SAML Enabled** is selected, then a identity provider is used.

Accessing Lenovo XClarity Administrator after an external LDAP server failure

If you are using an external LDAP authentication server and that server fails or is not available, use the following procedure to recover access to the Lenovo XClarity Administrator web interface by using the local authentication server on the management node.

Procedure

To change the LDAP client setting, complete the following steps.

Step 1. Log in to the XClarity Administrator web interface using a user account with **lxc-recovery** authority. For more information about the client domain name, see Setting up an external LDAP authentication server.

Step 2. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 3. Click **LDAP Client** under the Users and Groups section to display the LDAP Client dialog.

Step 4. Select **Allow logons from local users** for the user authentication method to enable local management of user accounts. When this option is selected, all user accounts exist locally on the management server.

Step 5. Click **Apply**.

Results

You can now use the user accounts in the local authentication server to access the XClarity Administrator management server. After your external authentication server is restored and available to the management server, you can change the LDAP client setting back to the external authentication server.

Accessing Lenovo XClarity Administrator after an external SAML identity provider failure

If you are using an external SAML identity provider and that server fails or is not available, use the following procedure to recover access to the Lenovo XClarity Administrator web interface by using the XClarity Administrator local authentication server.

Procedure

Complete the following steps to change the SAML client setting.

Step 1. Open your web browser to the XClarity Administrator login page (for example, `https://<ip_address>/ui/login.html`).

Step 2. Log in to the XClarity Administrator web interface using a local recovery user account that you created when you set up the identity provider.

Step 3. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 4. Click **SAML Settings** under the Users and Groups section to display the SAML Settings dialog.

Step 5. Clear **Enable SAML** to disable the SAML identity provider. When this option is cleared, the local authentication server or external LDAP server (if configured) is used for authentication.

Step 6. Click **Apply**.

Results

You can now use the user accounts in the local authentication server to access the XClarity Administrator management server. After your external identity provider is restored and available to the management server, you can change the authentication method to the identity provider.

Managing user accounts

User accounts are used to log in and manage Lenovo XClarity Administrator and all chassis and servers that are managed by XClarity Administrator. XClarity Administrator user accounts are subjected to two interdependent processes: authentication and authorization.

About this task

Authentication is the security mechanism by which a user's credentials are verified. The authentication process uses the user credentials that are stored in the configured authentication server. It also prevents unauthorized management servers or rogue managed-system applications from accessing the resources. After authentication, a user can access XClarity Administrator. However, to access a specific resource or perform a specific task, the user must also have the appropriate authorization.

Authorization checks the permissions of the authenticated user and controls access to resources based on the users membership in a role group. *Role groups* are used to assign specific roles to a set of user accounts that are defined and managed in the authentication server. For example, if a user is a member of a role group that has Supervisor permissions, that user can create, edit, and delete user accounts from XClarity Administrator. If a user has Operator permissions, that user can only view user-account information.

Creating a user

User accounts are used to manage authorization and access to resources.

About this task

The first user account that you create must have the role of Supervisor and must be activated (enabled).

As an added measure of security, create at least two user accounts that have the role of **Supervisor**. Ensure that you record the passwords for these user accounts, and store them in a secure location in case you must restore the Lenovo XClarity Administrator.

Procedure

To add a user to XClarity Administrator, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Local Users** under the Users and Groups section to display the Users Management page.

Step 3. Click the **Create** icon ( ) to create a user. The Create New User dialog is displayed.

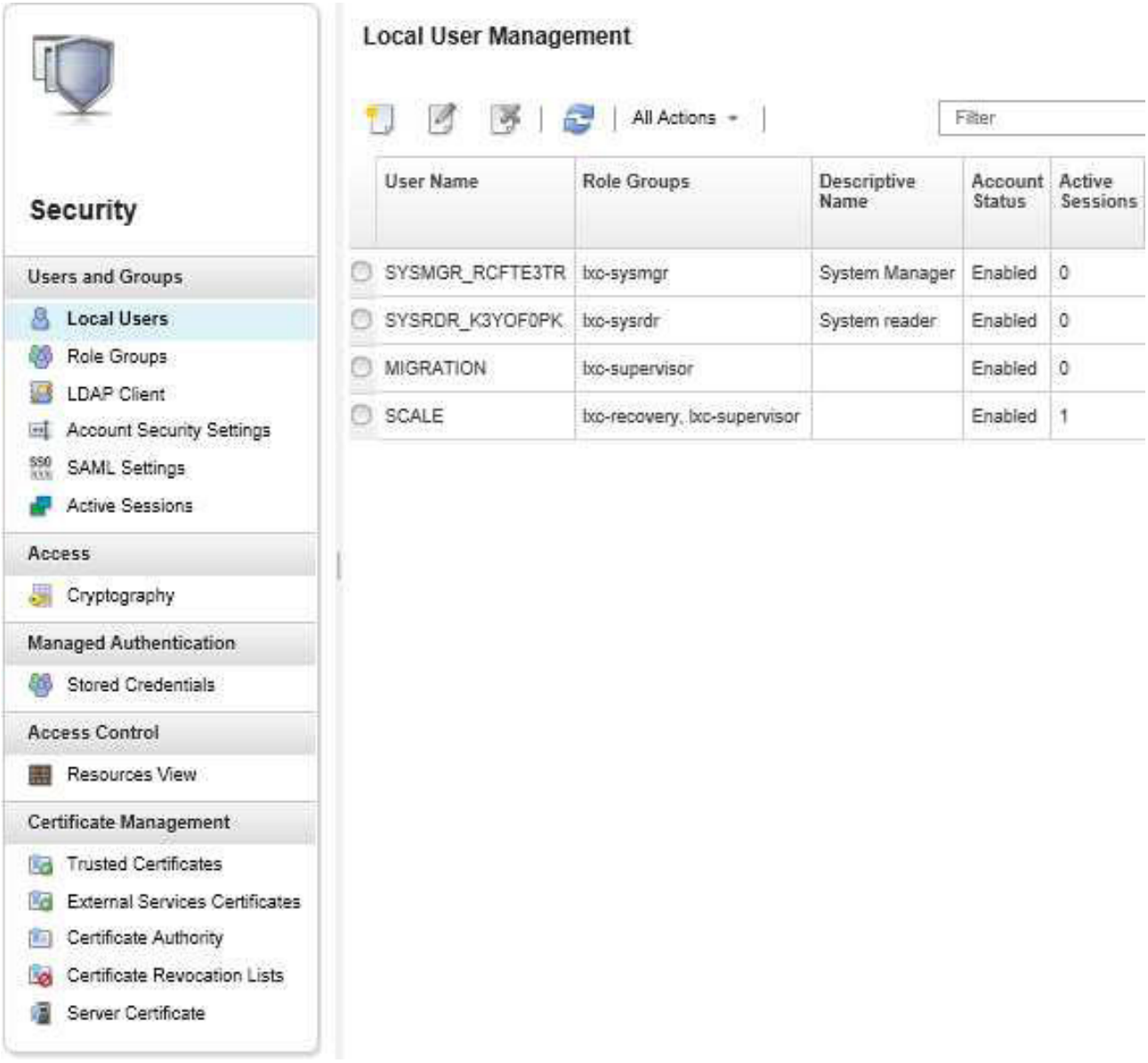
Step 4. Fill in the following information in the dialog.

- Enter a user name and description for the user.
- Enter the new and confirm new passwords. The rules for the passwords are based the current account-security settings.
- Select one or more role groups to authorize the user to perform appropriate tasks.For information about role groups and how to create custom role groups, see Creating a custom role group.
- (Optional) Set **Change password on first access** to `Yes` if you want to force the user to change the password the first time the user logs in to XClarity Administrator.

Step 5. Click **Create**.

What to do next

The user account is displayed in the Users Management table. The table shows the associated role groups and the account status for each user account.



After you create a user account, you can perform the following actions on a selected user account:

- Modify the user name, description, and role for a user account by clicking the **Edit** icon ( ).
- Delete the user account by clicking the **Delete** icon ( ).
- Reset the password for the user account (see Resetting the password for a user).
- Unlock the account (see Unlocking a user).
- Enable or disable a user account (see Enabling or disabling a user).

Enabling or disabling a user

You can change enable or disable a local user account in the authentication server.

Procedure

To enable or disable a user account, complete the following steps.

- If the local authentication server is used:
  1. From the Lenovo XClarity Administrator title bar, click **Administration → Security**.
  2. Click **Local Users** under the Users and Groups section to display the Users Management page.
  3. Select a user account.
  4. If the user account is enabled, click **All Actions → Disable selected account** to disable the user. The account status in the table changes to `Disabled`.
  5. If the user account is disabled, click **All Actions → Enable selected account** to enable the user. The account status in the table changes to `Enabled`.
- If an external LDAP server is used, enable or disable a user account in Microsoft Active Directory.
- If an external SAML identity provider is used, enable or disable a user account in the identity provider.

Logging off an active user

You can log off (terminate) an active user from Lenovo XClarity Administrator.

You must be logged on to XClarity Administrator using a user account with **lxc-supervisor** or **lxc-security-admin** authority.

Procedure

To log off an active user, complete the following steps.

Step 1. From the XClarity Administrator title bar, click **Administration → Security**.

Step 2. Click **Active Sessions** under the Users and Groups section to display the Active Sessions Management page.

Step 3. Select one or more user accounts.

Step 4. Click **Log Off User**.

Changing the password for your user account

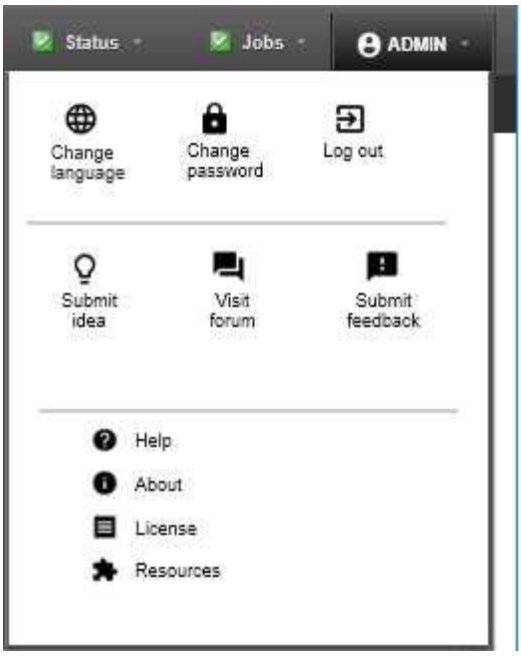
You can change the password for your user account.

Procedure

Complete the following steps to change your password.

- If the local authentication server is used:
  1. From the Lenovo XClarity Administrator title bar, click the user-actions menu (

), and then click **Change Password**. The Change Password dialog is displayed.



2. Enter the current password.
3. Enter the new and confirm-new passwords. The rules for the passwords are based the current account-security settings.
4. Click **Change**.

- If an external authentication server is used, change your password in Microsoft Active Directory.

  Attention: If you updated Microsoft Active Directory with a new password for the client account that is used to bind XClarity Administrator to the external authentication server, ensure that you also update the new password in the XClarity Administrator web interface (see Setting up an external LDAP authentication server).

- If an external SAML identity provider is used, change your password in the identity provider.

Resetting the password for a user

You can reset the password for any user account.

Procedure

To reset a password, complete the following steps.

- If the local authentication server is used, rest the password from the Lenovo XClarity Administrator web interface:
  1. From the XClarity Administrator menu bar, click **Administration → Security**.
  2. Click **Local Users** under the Users and Groups section to display the Users Management page.
  3. Select a user account from the table.
  4. If the user account is enabled, click the **All Actions → Reset Password for Selected User**. The Reset Password dialog is displayed.
     a. Enter the new and confirm new passwords. The rules for the passwords are based the current account security settings.
     b. Optionally set **Change on first access** to `Yes` if you want to force the user to change the password the first time the user logs in to XClarity Administrator.
     c. Click **Reset**.

- If an external LDAP server is used, reset the password in Microsoft Active Directory.
- If an external SAML identity provider is used, reset the password in the identity provider.
- If you cannot log in to XClarity Administrator using another supervisor account or if another supervisor account does not exist, you can reset the password for a local user with recovery or supervisor authority by mounting an ISO image that contains a configuration file with the new password. For more information, see Password for a local recovery or supervisor user is forgotten in the XClarity Administrator online documentation.

Unlocking a user

You can unlock a user account that is locked out of Lenovo XClarity Administrator. A user account can become temporarily locked if the user attempts too many logins that are not valid.

About this task

The user-account security settings control the amount of time that must pass before a user that was locked out can attempt to log back in again. If the **Lockout period after maximum login failures** setting is set to `0`, the user account remains locked until the administrator explicitly unlocks it. For more information about the lockout period for maximum login failures, see Changing the user-account security settings.

You can also permanently disable or enable a user account. For more information, see Enabling or disabling a user.

Note: You must have Supervisor authority to unlock a user account.

Tip: You can use XClarity Administrator to unlock user accounts that are managed using the local authentication server. You cannot unlock user accounts in an external authentication server by using the XClarity Administrator.

Procedure

To unlock a user account, complete the following steps.

- If the local authentication server is used:
  1. From the XClarity Administrator menu bar, click **Administration → Security**.
  2. Click **Local Users** under the Users and Groups section to display the Users Management page.
  3. Select the user account from the table.
  4. Click the **All Actions → Unlock Account for Selected User**.
- If an external LDAP server is used, unlock the user account in Microsoft Active Directory.
- If an external SAML identity provider is used, unlock the user account in the identity provider.

Monitoring active users

You can determine who is logged in to the Lenovo XClarity Administrator web interface from the Dashboard page.

Procedure

- You can get find a list of active users and their IP addresses by clicking **Dashboard** from the XClarity Administrator menu bar.

  The active user sessions are listed in the Activity section.



- You can get find a list of all active users (other than the current user) and their IP addresses by clicking **Administration → Security** from the XClarity Administrator menu bar, and then clicking **Active Sessions**.

  Note: In XClarity Administrator v2.2 and later, user sessions that are inactive for more than specific amount of time are logged out automatically. You can set the inactivity period by clicking **Administration → Security** from the XClarity Administrator menu bar, clicking Account Security Settings, and then adjusting the **Web inactivity session timeout** value. Note that the change does not affect active user sessions. It only affects user sessions that start after the setting is changed.



Managing stored credentials

Stored credentials are used to manage authorization and access to chassis and servers that are managed by Lenovo XClarity Administrator using local authentication.

Before you begin

You must have **lxc-supervisor** or **lxc-security-admin** authority to create, modify, or delete stored credentials.

About this task

A stored credential must be a local user account on a device or a user account in an Active Directory server.

If you choose to manage devices using local authentication instead of XClarity Administrator managed authentication, you must select a stored-credentials account during the management process.

Important: XClarity Administrator does not validate the user name and password that you specify for the stored credential. It is your responsibility to ensure that specified information corresponds to an active user account on the local device or Active Directory (if the managed device is configured to use Active Directory for authentication).

Attention: The stored credentials must have supervisor access or sufficient authority to make configuration changes on the device. If you attempt to manage a server with stored credentials that do not have sufficient authority on the device, the manage process might succeed but additional administrative inventory actions on the device might fail due to access-denied errors, which could lead to perceived connectivity problems with the device.

Procedure

To add a stored credential to XClarity Administrator, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**. The Security page is displayed.

Step 2. Click **Stored Credentials** under the Managed Authentication section to display the Stored Credential page.

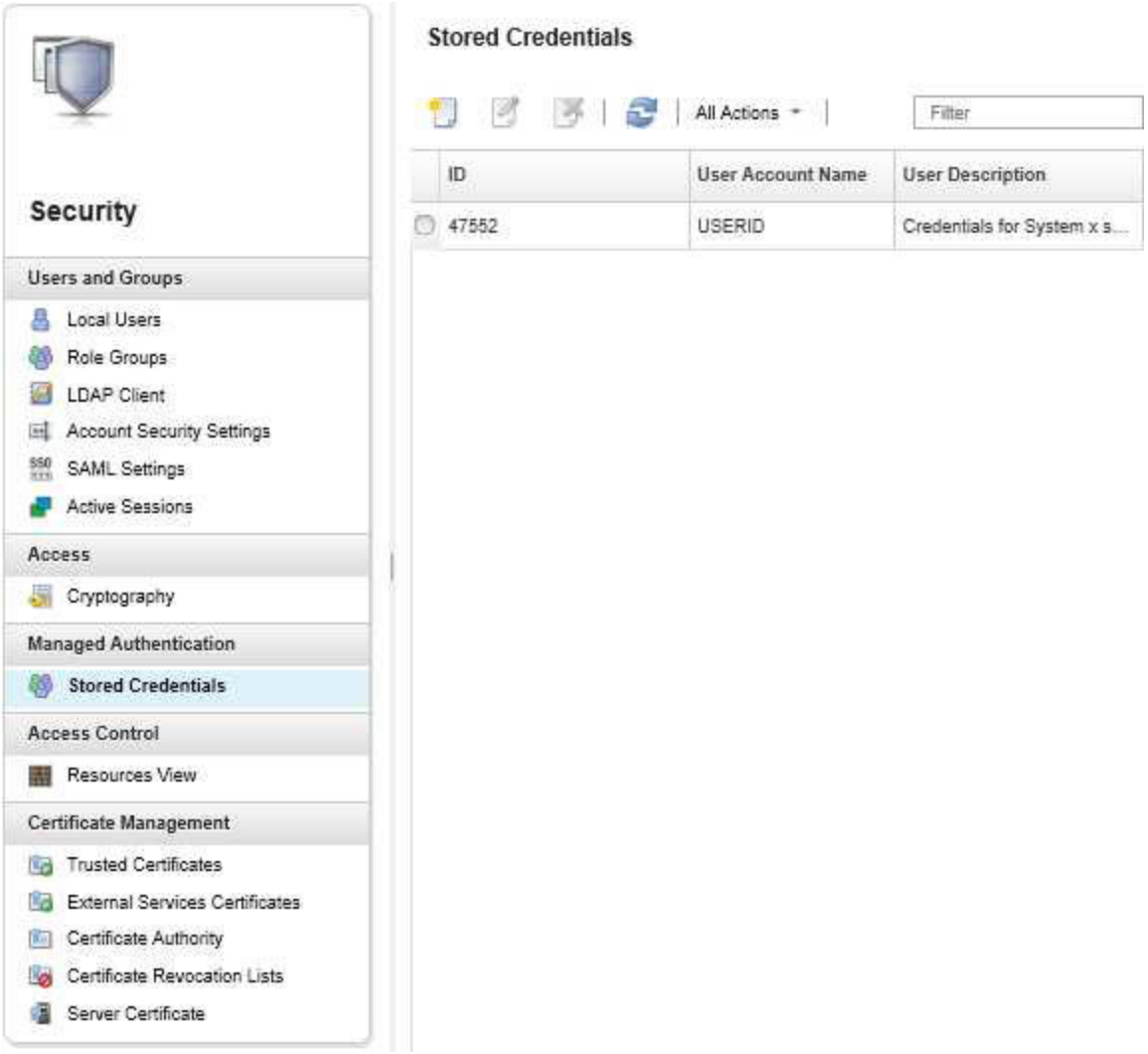
Step 3. Click the **Create** icon ( ) to create a stored credential. The Create New Stored Credentials dialog is displayed

Step 4. Fill in the following information in the dialog.
- Enter a user name and optional description for the stored credential.
- Enter and then confirm the password for the stored credential.
- Optionally enter and then confirm the password for the RECOVERY_ID stored recovery credentials.

Step 5. Click **Create Stored Credential**.

What to do next

The stored-credential account is displayed in the Stored Credential table. The table shows the associated ID and description for each stored-credential account.



From the Stored Credentials page, you can perform the following actions on a selected stored-credential account:

- Modify the user name, password, and description for a stored-credential account by clicking the **Edit** icon ( ).

  Note: If you manage a device using a stored credential and enable managed authentication, you cannot edit the stored credential.

- Delete the stored-credential account by clicking the **Delete** icon ( ).

To resolve stored credentials that have become expired or invalid, see Resolving expired or invalid stored credentials for a server.

Managing roles and role groups

A *role* is used to control user access to resources and limit the actions that users can perform on those resources. A *role group* is a collection of one or more roles and is used to assign those roles to multiple users. The roles that you configure for a role group determine the level of access that is granted to each user that is a member of that role group. Each Lenovo XClarity Administrator user must be a member of at least one role group.

Creating a custom role

A *role* is a set of *privileges*, or permissions to perform a specific action. Lenovo XClarity Administrator includes several predefined (default) roles. You can also create custom roles that enforce a unique set of privileges that users can perform

Before you begin

You must have **lxc-supervisor** or **lxc-security-admin** authority to perform this task.

About this task

To create a custom role, select one or more predefined roles that are closest in scope to the role that you want to create, and then clear the individual privileges that you want to restrict. This ensures that you get all of the intended privileges and that the role is constructed correctly with dependent privileges.

Some XClarity Administrator privileges depend on corresponding management-module privileges to perform actions on managed devices (see Management module v1 privileges and Management module v2 privileges). An XClarity Administrator privilege might allow you to request an action on a managed device, but the device will deny the request if you do not have the corresponding privileges for the CMM, IMM, or XCC. For example, if you create a custom role to perform power actions on managed devices, you would add the **lxc-inventory-modify-device-power-state** privilege and:

- For a ThinkSystem server in a rack, add the **mm-power-and-restart-access-v1** privilege.
- For an entire Flex System chassis (including devices in the chassis), add the **mm-power-and-restart-access-v1** privilege.
- For a ThinkSystem server in a chassis, add **mm-power-and-restart-access-v1**, **mm-blade-operator-v2**, and the **mm-blade-#-scope-v2** privilege that matches the target server.

All roles contain read-only privileges. No custom role can be more restrictive than the **lxc-operator** role.

If a user is does not have privileges to perform specific actions, menu items, toolbar icons, and buttons that perform those actions are disabled (greyed out).

XClarity Administrator provides a role group for each predefined role, using the same name as the role. Consider creating a role group for new roles that you create. For more information about role groups, see Creating a custom role group.

- **lxc-supervisor**. Users that are assigned this role can access, configure, and perform all available operations on the management server and all managed devices.Users that are assigned this role always have access to all managed devices. You cannot restrict access to devices for this role.
- **lxc-admin**. Users that are assigned this role can modify non-security related settings and perform all non-security related operations on the management server, including the ability to update and restart the management server. This role also provides the ability to view all configuration and status information about the management server and managed devices.
- **lxc-security-admin**. Users that are assigned this role can modify security settings and perform security-related operations on the management server and managed devices. This role also provides ability to view all configuration and status information about the management server and managed devices.

  Users that are assigned this role always have access to all managed devices. You cannot restrict access to devices for this role.
- **lxc-hw-admin**. Users that are assigned this role can modify non-security settings and perform non-security related operations on managed devices, including the ability to update and restart managed devices. This role also provides the ability to view all configuration and status information about the management server and all managed devices.
- **lxc-fw-admin**. Users that are assigned this role can create firmware policies and deploy those policies to managed devices. Users that are not assigned this role can only view policy information.

- **lxc-os-admin**. Users that are assigned this role can download and deploy operating systems and device-driver updates to managed servers. Users that are not assigned this role can only view operating-system and device-driver information.
- **lxc-service-admin**. Users that are assigned this role can collect and download service files for XClarity Administrator and managed devices. Users that are not assigned this role can collect but not download service data.
- **lxc-hw-manager**. Users that are assigned this role can discover new devices and place those devices under the management control of the XClarity Administrator. This role prohibits users from performing operations or modifying configurations settings on the management server and managed devices beyond those operations that are necessary to discover and manage new devices.
- **lxc-operator**. Users that are assigned this role can view all configuration and status information about the management server and managed devices. This role prohibits users from performing operations or modifying configurations settings on the management server and managed devices.
- **lxc-recovery**. Users that are assigned this role can modify security settings and perform security-related operations on the management server. These users can also authenticate directly to the XClarity Administrator even if the authentication method is set to external LDAP server. This role provides a recovery mechanism in case a communication error occurs with the external LDAP server that uses the "Login Credentials" configuration.

  Users that are assigned this role always have access to all managed devices. You cannot restrict access to devices for this role.

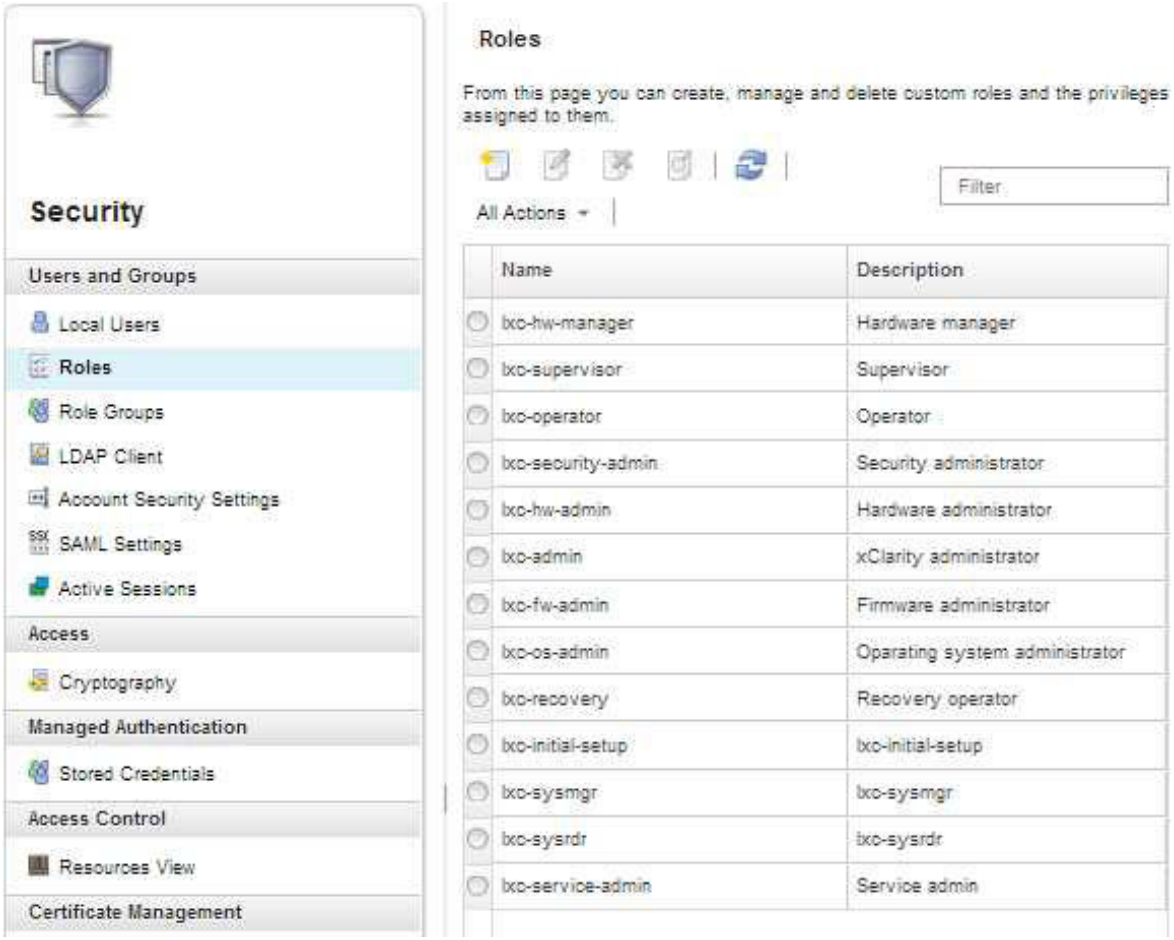
The following predefined roles are *reserved* and cannot be used to create new role groups or assigned to new users.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procedure

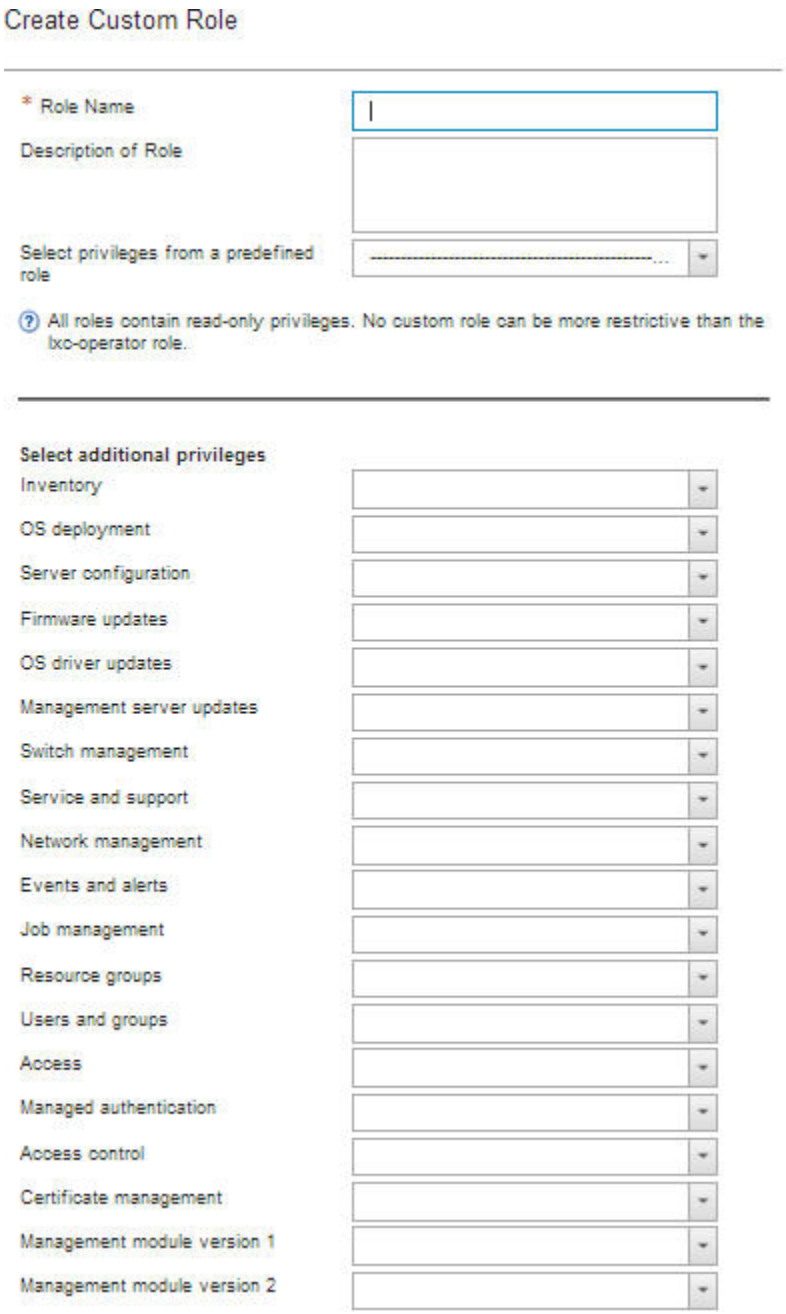
To create a custom role, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Roles** under the Users and Groups section to display the Roles Management page.



Step 3. Click the **Create** icon ( ) to create a role. The Create Custom Role dialog is displayed.



Step 4. Enter a role name and description.

Step 5. Optional: Select a predefined role to use as a starting point for this custom role.

If you select an existing role, the privileges that are associated with that role are selected in the dialog.

Step 6. Modify the privileges for this new role by selecting or clearing privileges from the **Select additional privileges** drop-down menus.

Note: If you select all privileges in specific category, and privileges are added to that category when you update or upgrade XClarity Administrator, the new privileges are automatically added to the custom role

Step 7. Click **Create**. The new role is added to the table on the Role Management page.

Results

You can also perform the following actions.

- View the privileges associated with a specific role by selecting the role and clicking the **View** icon ().
- Rename or edit the custom role by clicking the **Edit** icon (). When you edit a custom role, you can change selected privileges, the description, and list of users that are associated with the role.

  Note: You cannot modify a predefined role
- Delete the predefined or custom role by clicking the **Delete** icon ().
- Add or remove roles from a role group (see Adding and removing multiple users from a role group).
- Restore all predefined roles that were deleted by clicking **All Actions → Restore Default Roles**.

Predefined privileges

Lenovo XClarity Administrator provides a set of *privileges* (permissions) that allow a user to perform a specific action. The privileges are organized into categories based on the type of action.

Access privileges

These privileges provide permissions to modify cryptographic and SSL/TLS modes.

Privilege name	Privilege description	default roles
lxc-sec-apply-crypto-settings	Apply cryptography settings	lxc-recovery, lxc-security-admin, lxc-supervisor

Access control privileges

These privileges provide permissions to control access to resources.

Privilege name	Privilege description	default roles
lxc-sec-modify-resource-access-control	Edit resource access control settings	lxc-recovery, lxc-security-admin, lxc-supervisor

Certificate management privileges

These privileges provide permissions to manage security certificates in Lenovo XClarity Administrator.

Privilege name	Privilege description	dDefault roles
lxc-sec-add-external-certificates	Add an external certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-add-trusted-certificates	Add a trusted certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-certificate-signing	Generate certificate signing request	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-external-certificates	Delete an existing external certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-trusted-certificates	Delete an existing certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-ca	Download certificate authority root certificate	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilege name	Privilege description	dDefault roles
lxc-sec-download-server-certificate	Download server certificate	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-certificate-revocation-list	Modify or replace certificate revocation list	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-ca	Regenerate certificate authority root certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-download-ca	Regenerate certificate authority root certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-server-certificate	Regenerate server certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-resolve-untrusted-certificates	Resolve untrusted certificates	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-upload-server-certificate	Upload server certificate	lxc-recovery, lxc-security-admin, lxc-supervisor

Monitoring and events privileges

These privileges provide permissions to manage events and alerts.

Privilege name	Privilege description	Default roles
lxc-event-audit	Manage event and audit logs	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	Create and modify event forwarders	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-monitoring-create-edit-push-services	Create and modify push services	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-event-forwarders	Delete event forwarders	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-push-services	Delete push services	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-set-event-thresholds	Set event thresholds	lxc-admin, lxc-hw-admin, lxc-supervisor

Firmware updates privileges

These privileges provide permissions to manage and apply firmware updates and UpdateXpress System Packs.

Privilege name	Privilege description	default roles
lxc-fwUpdates-apply-assign-policy	Assign firmware compliance policy to devices	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-apply-perform-updates	Perform firmware updates	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-create-policies	Create, copy, edit, and import firmware compliance policies	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

Privilege name	Privilege description	default roles
lxc-fwUpdates-policies-delete-policies	Delete compliance policies	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-delete-packages	Delete firmware update packages	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-download-packages	Download and import firmware update packages and refresh catalog of firmware update packages	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-export-packages	Export firmware update packages	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

Resource group privileges

These privileges provide permissions to use resource groups.

Privilege name	Privilege description	Default roles
lxc-resource-create-edit-group	Create and modify resource groups	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-resource-delete-group	Delete resource groups	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

Inventory privileges

These privileges provide permissions to discover and manage devices, and view device inventory.

Privilege name	Privilege description	default roles
lxc-dm-manage-device	Manage Chassis, Servers, Storage and Switches	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-dm-modify-ip-settings	Enable or disable checking for duplicate IP addresses in the same subnet	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-power-state	Modify canisters, cmms, nodes, storage and switches power state	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-properties	Modify cabinets, canisters, chassis, cmms, nodes, storage and switches properties	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	Modify predicted failure alerts (PFA) configuration settings	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Jobs management privileges

These privileges provide permissions to manage jobs (tasks).

Privilege name	Privilege description	Default roles
lxc-tasks-remove-jobs	Delete jobs	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-tasks-schedule-jobs	Schedule jobs	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Managed authentication privileges

These privileges provide permissions to manage authentication, including stored credentials.

Privilege name	Privilege description	default roles
lxc-sec-delete-stored-credentials	Delete stored credentials	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-stored-credentials	Edit existing stored credentials	lxc-recovery, lxc-security-admin, lxc-supervisor

Management module v1 privileges

These privileges are associated with the LDAP permission bits (bitstrings) that are enforced by management modules for rack servers and entire Flex System chassis (including all devices in that chassis).

Lenovo XClarity Administrator does not enforce these permissions. The permissions are enforced by the managed devices that use an XClarity Administrator use account.

If the device is managed using *managed authentication* (using the local authentication server for authentication), the local authentication server uses these permissions to indicate to the managed devices which permissions to grant to the user when logging in to the device.

You would configure these same permissions in an external LDAP server. When using an external LDAP server with XClarity Administrator, ensure that you add groups in the external LDAP server with names that match the role group names in XClarity Administrator and that the external LDAP users are added to one or more of those groups. External LDAP users must be part of an LDAP group with a name that matches an XClarity Administrator role group that contains roles associated with the management module bits strings. XClarity Administrator uses these groups to tie the external LDAP users to the role groups in XClarity Administrator and to the bits strings that are enforced by the management module. Then, when a user logs into a managed device using an external LDAP user account, the management module knows whether to grant the user supervisor or operator privileges.

Note: Management module v1 privileges are not supported for FlexSystem switches that do not have Secure IOM enabled, RackSwitch switches, Storage devices, and ThinkServer servers.

For information about the LDAP permission bits for each management module, see the online documentation.

- Configuring LDAP in the CMM and CMM2 online documentation
- Configuring LDAP in the IMM and IMM2 online documentation
- Configuring LDAP in the XCC online documentation

Privilege name	Privilege description	default roles
mm-advanced-adaptor-configuration-v1	Advanced adaptor configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-basic-configuration-v1	Basic configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-clear-event-logs-v1	Clear event logs	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v1	Deny always	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilege name	Privilege description	default roles
mm-networking-and-security-v1	Networking and security	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-power-and-restart-access-v1	Power/restart access for servers and Flex switches	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-access-v1	Remote control access for servers	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	Remote console and virtual media access for servers	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-supervisor-v1	Supervisor access	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-user-account-management-v1	User management	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

Management module v2 privileges

These privileges are associated with the LDAP permission bits (bitstrings) that are enforced by management modules for individual FlexSystem and ThinkSystem devices in a chassis (chassis, servers and switches with Secure IOM enabled).

Lenovo XClarity Administrator does not enforce these permissions. The permissions are enforced by the managed devices that use an XClarity Administrator use account.

If the device is managed using *managed authentication* (using the local authentication server for authentication), the local authentication server uses these permissions to indicate to the managed devices which permissions to grant to the user when logging in to the device.

You would configure these same permissions in an external LDAP server. When using an external LDAP server with XClarity Administrator, ensure that you add groups in the external LDAP server with names that match the role group names in XClarity Administrator and that the external LDAP users are added to one or more of those groups. External LDAP users must be part of an LDAP group with a name that matches an XClarity Administrator role group that contains roles associated with the management module bits strings. XClarity Administrator uses these groups to tie the external LDAP users to the role groups in XClarity Administrator and to the bits strings that are enforced by the management module. Then, when a user logs into a managed device using an external LDAP user account, the management module knows whether to grant the user supervisor or operator privileges.

Notes:

- You must also specify management module v1 privileges for the entire chassis (seeManagement module v1 privileges).
- Management module v2 privileges are not supported for FlexSystem switches that do not have Secure IOM enabled.
- For Lenovo ThinkSystem chassis, ensure that IMM2 is set up to allow the custom role to have “Node administration.” If you want the custom role to have control of all devices in the Lenovo ThinkSystem chassis, ensure that IMM2 is set up to allow the custom role to have “Node X scope” as well

For information about the LDAP permission bits for each management module, see the online documentation.

- Configuring LDAP in the CMM and CMM2 online documentation
- Configuring LDAP in the IMM and IMM2 online documentation

- Configuring LDAP in the XCC online documentation

Privilege name	Privilege description	Default roles
mm-blade-1-scope-v2	Node 1 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-2-scope-v2	Node 2 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-3-scope-v2	Node 3 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-4-scope-v2	Node 4 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-5-scope-v2	Node 5 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-6-scope-v2	Node 6 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-7-scope-v2	Node 7 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-8-scope-v2	Node 8 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-9-scope-v2	Node 9 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-10-scope-v2	Node 10 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-11-scope-v2	Node 11 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-12-scope-v2	Node 12 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-13-scope-v2	Node 13 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-14-scope-v2	Node 14 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-administration-v2	Node administration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-configuration-v2	Node configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-operator-v2	Blade operator	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-remote-presence-v2	Node remote presence	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-administration-v2	Chassis administration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-configuration-v2	Chassis configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilege name	Privilege description	Default roles
mm-chassis-log-management-v2	Chassis log account management	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-operator-v2	Chassis operator	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-chassis-scope-v2	Chassis scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-user-account-management-v2	User management	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v2	Deny always	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-io-module-1-scope-v2	I/O module 1 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-2-scope-v2	I/O module 2 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-3-scope-v2	I/O module 3 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-4-scope-v2	I/O module 4 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-administration-v2	Switch administration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-configuration-v2	Switch configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-operator-v2	Switch operator	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-supervisor-v2	Supervisor access	lxc-admin, lxc-hw-admin, lxc-supervisor

Management server privileges

These privileges provide permissions to update management server.

Privilege name	Privilege description	default roles
lxc-mgmtserverupdates-delete-updates	Delete management server updates	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-download-updates	Download and import management server updates and refresh management server catalog	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-perform-updates	Perform management server updates	lxc-admin, lxc-fw-admin, lxc-supervisor

Network management privileges

These privileges provide permissions to configure network settings.

Privilege name	Privilege description	Default roles
lxc-network-edit	Modify network access	lxc-admin, lxc-supervisor

OS deployment privileges

These privileges provide permissions to manage and deploy operating systems.

Privilege name	Privilege description	Default roles
lxc-osdeploy-create-edit-remote-file-server	Create and edit a remote file server entry	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	Create, import, export, and edit OS images and custom files	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-os-files	Delete OS images and custom files	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-remote-file-server	Delete a remote file server entry	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-global-settings	Edit information in global settings dialog **Note:** Changing global IP-assignment settings affects the network settings; therefore, to make changes to the global IP-assignment settings, you must also have also have **lxc-osdeploy-edit-settings-and-deploy-os-images** privileges.	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	Modify deployment settings and deploy OS images to one or more servers	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

OS driver updates privileges

These privileges provide permissions to manage and apply OS device-driver updates.

Privilege name	Privilege description	default roles
lxc-osDriverUpdates-apply-assign-uxsp	Assign OS device drivers UXSP to devices	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	Check OS authentication	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	Check OS device driver compliance	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	Perform OS device driver updates	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	Delete OS device driver update packages	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	Download and import OS device driver update packages and refresh OS device driver UXSP catalog	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Users and groups privileges

These privileges provide permissions to manage user accounts and groups.

Privilege name	Privilege description	default roles
lxc-sec-apply-saml-settings	Apply SAML settings	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-role-groups	Delete a role group	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-roles	Delete a role	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-users	Delete a user	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-edit-account-settings	Modify account security settings	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-ldap-settings	Apply LDAP settings	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-role-groups	Modify a role group	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-roles	Modify a role	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-users	Modify a user	lxc-recovery, lxc-security-admin, lxc-supervisor

Server configuration privileges

These privileges provide permissions to provision or preprovision servers using Configuration Patterns.

Privilege name	Privilege description	Default roles
lxc-cp-edit-management-ip	Modify management IP addresses for chassis	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-edit-preferences	Set Configuration Patterns Preferences	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-address-pools	Manage Address Pools	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-patterns	Manage Patterns	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-placeholders	Manage Placeholders	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-profiles	Deploy patterns, deploy placeholder to chassis and manage profiles	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-other-server-config	Reset local storage and apply Intel Optane DCPMM security operation	lxc-admin, lxc-hw-admin, lxc-supervisor

Service privileges

These privileges provide permissions to define support contacts for each managed device, collect and send service files to Lenovo Support, set up automatic notification to service providers when certain serviceable events occur on specific devices, view service-ticket status and warranty information, and collect and forward service data.

Privilege name	Privilege description	Default roles
lxc-ss-alter-backup-credentials	Modify backup FFDC credentials	lxc-admin, lxc-hw-admin, lxc-service-admin, lxc-supervisor
lxc-ss-call-home	Perform Call Home	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-recovery-password	Change service recovery password	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-tickets	Modify service tickets	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-remove-service-tickets	Delete service tickets	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-run-service-forwarders	Run service forwarders	lxc-admin, lxc-hw-admin, lxc-supervisor

Switch configuration privileges

These privileges provide permissions to configure switches and backup and restore switch configuration data.

Privilege name	Privilege description	default roles
lxc-netcfg-template-management	Create, modify, delete, and deploy switch-configuration templates, and delete a switch-configuration deployment	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-config-management	Backup, restore, delete, export, and import switch configuration-data files	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-port-management	Modify switch port status	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Creating a custom role group

A *role group* is a set of roles and a set of users that are members of the same set of roles. The level of access that is granted to each user in the role group is based on the roles that are assigned to that role group. XClarity Administrator provides the following predefined role groups, which correspond to each of the predefined roles. You can also create custom role groups.

About this task

Each XClarity Administrator user must be a member of at least one role group.

The following role groups are predefined in XClarity Administrator.

- **LXC-SUPERVISOR**. Includes the **lxc-supervisor** role.
- **LXC-ADMIN**. Includes the **lxca-admin** role.
- **LXC-SECURITY-ADMIN**. Includes the **lxc-security-admin** role.
- **LXC-HW-ADMIN**. Includes the **lxc-hw-admin** role.
- **LXC-FW-ADMIN**. Includes the **lxc-fw-admin** role.
- **LXC-OS-ADMIN**. Includes the **lxc-os-admin** role.
- **LXC-SERVICE-ADMIN**. Includes the **lxc-service-admin** role.
- **LXC-HW-MANAGER**. Includes the **lxc-hw-manager** role.

- **LXC-OPERATOR**. Includes the **lxc-operator** role.
- **LXC-RECOVERY**. Includes the **lxc-recovery** role.

The following predefined roles are *reserved* and cannot be used to create new role groups or assigned to new users.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procedure

To create a role group, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Role Groups** under the Users and Groups section to display the Group Management page.

Step 3. Click the **Create** icon () to create a role group. The Create New Role Group dialog is displayed.

Step 4. Enter a group name and description.

Note: Tip: For the group name, you can use letters, numbers, white space, underscore, dashes, and periods.

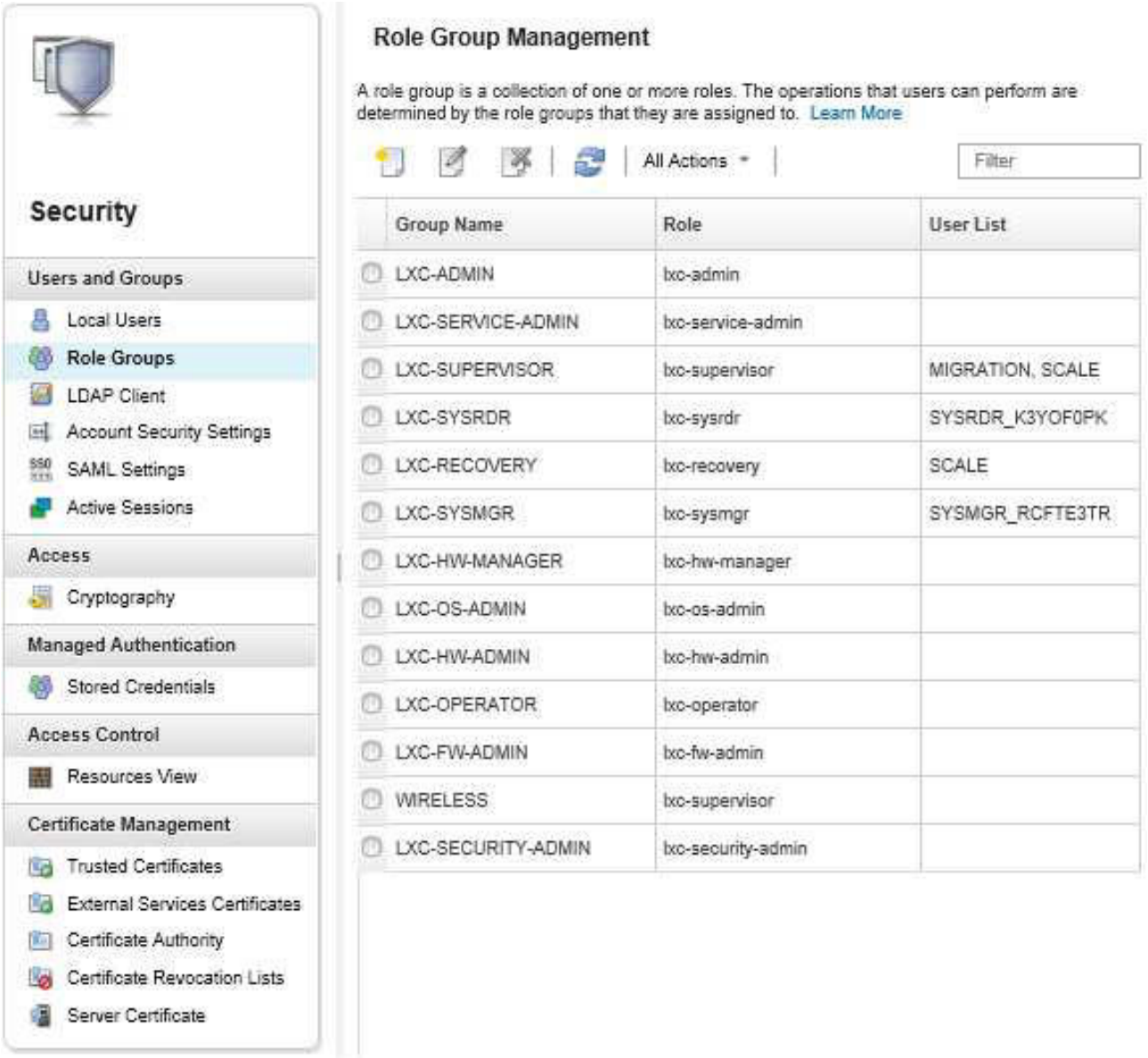
Step 5. Select one or more roles to assign to this role group.

Step 6. Select one or more users as members of this role group.

Step 7. Click **Create**. The new role group is added to the table on the Group Management page.

Results

The role group is displayed in the Role Groups table. The table shows the associated authorization roles and the members for each role group.



After you create a role group, you can perform the following actions on a selected role group:

- Add or remove roles that are assigned to this role group by clicking the **Edit** icon ( ).
- Add or remove users as members of the role group (see “Adding and removing multiple users from a role group” on page 55).
- Export information about the role groups, including access permissions, by clicking **All Actions → Export as CSV**.
- Delete the role group by clicking the **Delete** icon ( ).You cannot delete predefined role groups.

After a role group is created, edited, or deleted, the change is immediately provisioned to each managed device.

Adding and removing multiple users from a role group

You can change membership in a role group by adding or removing multiple users.

Procedure

Complete the following steps to add and remove users from a role group.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Role Groups** under the Users and Groups section to display the Group Management page.

Step 3. Click the **Edit** icon ( ) modify the role group. The Edit Role Group dialog is displayed.

Step 4. Click the **User List** drop down list, and select the users to include or clear user to exclude from this role group.

Step 5. Click **Save**. The **User List** column displays the current user membership in the role group.

Managing access to devices

Access-control to devices is disabled by default and does not take effect until you enable it

When devices are initially managed by Lenovo XClarity Administrator, a predefined set of role groups have permission to access the devices by default. This predefined set is empty by default until it is configured.

You change the role groups that can access specific managed devices. When permission is given to certain role groups, only users that are members of those role groups can see and act on those specific devices.

Controlling access to specific devices

When devices are initially managed by Lenovo XClarity Administrator, a predefined set of role groups have permission to access the devices by default. You change the role groups that can access specific managed devices. When permission is given to certain role groups, only users that are members of those role groups can see and act on those specific devices.

Before you begin

Only users with **lxc-supervisor**, **lxc-security-admin**, or **lxc-recovery** authority can perform this action.

About this task

Access control is set on individual devices. It is not set for containers, such as racks and resource groups.

For components in a chassis or enclosure, users must have at least read-only access to the chassis or enclosure to the view components in that chassis or enclosure. If users do not have at least read-only access to the chassis or enclosure, those users might see the components in some views but are not guaranteed to see them in all views.

Users with **lxc-supervisor** authority can view and take actions on all resources regardless of whether they are in a role group that has specifically been given access to that resource. You cannot remove access to any resources for the **lxc-supervisor** role group.

If a user is not a member of a role group that has access to a specific managed device, the user cannot see or act on that specific device. This includes launching the management controller web interface through Lenovo XClarity Administrator. For Flex and System x devices, users also cannot directly log in to a CMM or management controller for which they do not have access.

The default access-control settings are used to set access permissions on devices when they are initially managed by XClarity Administrator and when resetting access permissions for a specific device to the default settings. Changing the default access-control settings does not automatically change access permissions on devices that are already managed.

Important:

- If a user is a member of more than one role group, and the role groups are assigned to different devices, then the actions that the user is allowed to perform on each device might be different. For example, if the user is a member of default role groups LXC-FW-ADMIN and LXC-OS-ADMIN, and if LXC-FW-ADMIN is granted access to Server A but LXC-OS-ADMIN has not been granted access to Server A, then that user would be able to update the firmware on Server A but would not be able to deploy an operating system to Server A. If LXC-OS-ADMIN had been granted access to Server B but LXC-FW-ADMIN had not been granted access to server B, then that same user would be able to deploy an operating system to Server B but would not be able to update the firmware on Server B.
- When limiting access to a device that has a parent resource (such as a server or switch in a Flex chasis), a user must have at least read-only permissions to the parent resource to interact fully with the device. If a user has at least read-only access to the device but not the parent, the user will not able be see the device inventory views, but might be able to see about the device in some views, such as jobs and events.

  For example, you can create a role group for the parent and assign that role group the **lxc-operator** role. Include all users who should be able to access any of the children (such as a server or switch in a Flex chasis), in that role group. Then, include that role group as one of the groups that has access to the parent.

Procedure

Complete the following procedures to control access to specific devices by associating role groups with those devices.

Step 1. From the main Lenovo XClarity Administrator menu, click **Administration → Security**.

Step 2. Click **Resource View** in the left navigation pane. The Resource View page is displayed.

You can sort the table columns to make it easier to find specific devices. In addition, you can select a device type in the **Resource Type** drop-down menu, select a role group in the **Role Groups** drop-down menu, select a resource group in the **Resource Groups**drop-down menu, and enter text (such as a resource name or type) in the **Filter** field to list only those devices that meet the selected criteria.

Step 3. Select one or more devices to which you want to control access.

Step 4. Click the **Edit** icon (). The Edit Resource dialog is displayed with the target devices listed in the **Resource Name** field.

Step 5. From the **Role Groups** drop-down list, select the role groups for which you want to allow access to the target devices.

Note: If the device has a parent resource (for example, a server or switch in a Flex chassis), you can specify access for both the device (right column) and the parent resource (left column).

Step 6. Set **Public Access** to `No`. This means that only users that are members of the selected role groups can access the target devices.

Step 7. Click **Save**.

Step 8. After you finish assigning permissions, click click the **Disabled** toggle to change **Resource Access Control** to enabled.

You can enable resource-access control at any time, either before or after configuring access to specific devices. When this setting is enabled, the configuration displayed in the table takes effect, including denying non-supervisor users access to any devices that do not have any groups configured to access them.

What to do next

You can also control access to devices by performing the following actions:

- Change the permissions to the default role groups and public access setting by clicking the **Edit** icon () and then clicking **Rest to Defaults**.
- Change the default role group and public access setting (see Changing the default permissions.).
- Disable resource-access control by clicking the **Enabled** toggle to change **Resource Access Control** to disabled. This means that all role groups can access all managed devices.

Disabling resource-access control

You disable access control for all devices or specific devices so that all users can view and act on those devices.

About this task

Only users with **lxc-supervisor**, **lxc-security-admin**, or **lxc-recovery** authority can perform this action.

Procedure

Complete the following steps to disable resource-access control.

- For all managed devices
  1. From the main Lenovo XClarity Administrator menu, click **Administration → Security**.
  2. Click **Resource View** in the left navigation pane. The Resource View page is displayed.
  3. Click the **Enabled** toggle to change **Resource Access Control** to disabled.
- For specific managed devices
  1. From the main XClarity Administrator menu, click **Administration → Security**.
  2. Click **Resource View** in the left navigation pane. The Resource View page is displayed.

     You can sort the table columns to make it easier to find specific devices. In addition, you can select a device type in the **Resource Type** drop-down menu, select a role group in the **Role Groups** drop-down menu, select a resource group in the **Resource Groups** drop-down menu, and enter text (such as a resource name or type) in the **Filter** field to list only those devices that meet the selected criteria.
  3. Select one or more devices to which you want to change access.
  4. Click the **Edit** icon (). The Edit Resource dialog is displayed with the selected devices listed in the **Resource Name** field.
  5. Set **Public Access** to `Yes`. This means that all role groups can access the target devices regardless of the roles groups that are listed in the **Role Groups** drop-down list.
  6. Click **Save**.

Changing the default permissions

There are two settings that determine whether role groups can access devices when they are initially managed by Lenovo XClarity Administrator: public access and role groups. The public-access setting determines whether all or only a specific set of role groups can access the target devices. By default, this setting is set to `Yes`, which means that all role groups can access the target devices. You can change the default behavior by changing the public-access setting to `No` and then selecting the set of role groups that can access the target devices

About this task

Only users with **lxc-supervisor**, **lxc-security-admin**, or **lxc-recovery** authority can perform this action.

Users with the **lxc-supervisor**, **lxc-security-admin**, or **lxc-recovery** authority can access all managed devices. You cannot remove access to any device for these role groups.

The default access-control settings are used to set access permissions on devices when they are initially managed by XClarity Administrator and when resetting access permissions for a specific device to the default settings. Changing the default access-control settings does not automatically change access permissions on devices that are already managed.

Procedure

Complete the following procedures to change the default access controls.

Step 1. From the main XClarity Administrator menu, click **Administration → Security**.

Step 2. Click **Resource View** in the left navigation pane. The Resource View page is displayed.

You can sort the table columns to make it easier to find specific devices. In addition, you can select a device type in the **Resource Type** drop-down menu, select a role group in the **Role Groups** drop-down menu, select a resource group in the **Resource Groups**drop-down menu, and enter text (such as a resource name or type) in the **Filter** field to list only those devices that meet the selected criteria.

Step 3. Click **All Actions → Edit Default Resources**. The Edit Default Resources dialog is displayed.

Step 4. From the **Role Groups** drop-down list, select the role groups that you want to define as the default set.

Step 5. Select the default **Public Access** setting.

- **Yes**. When a device is initially managed, all role groups can access that device regardless of the roles groups that are listed in the **Role Groups** drop-down list.
- **No**. When a device is initially managed, only role groups that are listed in the **Role Groups** drop-down list can access that device by default.

Step 6. Click **Save**.

Implementing a secure environment

It is important that you evaluate the security requirements in your environment, understand all security risks, and minimize those risks. Lenovo XClarity Administrator includes several features that can help you secure your environment. Use the following information to help you implement the security plan for your environment.

About this task

Important: You are responsible for the evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls for your system environment. Implementing the security features that are described in this section does not secure your environment completely.

Consider the following information when you are evaluating the security requirements for your environment:

- The physical security of your environment is important; limit access to rooms and racks where systems-management hardware is kept.
- Use a software-based firewall to protect your network hardware and data from known and emerging security threats such as viruses and unauthorized access.
- Do not change the default security settings for the network switches and pass-thru modules. The manufacturing default settings for these components disable the use of unsecure protocols and enable the requirement for signed firmware updates.
- The management applications for the CMMs, baseboard management controllers, FSPs, and switches permit only signed firmware-update packages for these components to ensure that only trusted firmware is installed.

- Only the users who are authorized to update firmware components should have firmware-update authority.
- At a minimum, ensure that critical firmware updates are installed. After making any changes, always back up the configuration.
- Ensure that all security-related updates for DNS servers are installed promptly and kept up to date.
- Instruct your users to not accept any untrusted certificates. For more information, see Working with security certificates.
- Tamper-evident options are available for the Flex System hardware. If the hardware is installed in an unlocked rack or located in an open area, install the tamper-evident options to deter and identify intrusions. See the documentation that comes with your Flex System products for more information about the tamper-evident options.
- Where possible and practical, place the systems-management hardware in a separate subnet. Typically, only administrators should have access to the systems-management hardware, and no basic users should be given access.
- When you choose passwords, do not use expressions that are easy to guess, such as “password” or the name of your company. Keep the passwords in a secure place, and ensure that access to the passwords is restricted. Implement a password policy for your company.

  Important: Always change the default user name and password. Strong password rules should be required for all users.
- Establish power-on passwords for users as a way to control who has access to the data and setup programs on the servers. See the documentation that comes with your servers for more information about power-on passwords.
- Use the various authorization levels that are available for different users in your environment. Do not allow all users to work with the same supervisor user ID.
- Ensure that your environment meets the following NIST 800-131A criteria to support secure communications:
  - Use Secure Sockets Layer (SSL) over the TLS v1.2 protocol.
  - Use SHA-256 or stronger hashing functions for digital signatures and SHA-1 or stronger hashing functions for other applications.
  - Use RSA-2048 or stronger, or use NIST approved Elliptic Curves that are 224 bits or stronger.
  - Use NIST-approved symmetric encryption with keys at least 128 bits in length.
  - Use NIST-approved random-number generators.
  - Where possible, support Diffie-Hellman or Elliptic Curve Diffie-Hellman key-exchange mechanisms.

  For more information about cryptography settings, see Configuring cryptography settings. For more information about NIST settings, see Implementing NIST SP 800-131A compliance.

Changing the user-account security settings

The user-account security settings control the password complexity, account lockout, and web session inactivity timeout. You can change the values of the settings.

Procedure

Complete the following steps to override the user-account security settings that are in place.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Account Security Settings** under the Users and Groups section to display the Users Management page.

Step 3. For each of the following setting that needs to change, select the new value.

Table 1. Account Security settings

Security setting	Description	Values
Password expiration period	The amount of time, in days, that a user can use a password before it must be changed. Smaller values reduce the amount of time for attackers to guess passwords. If set to 0, passwords never expire. The default is 90 days. **Note:** This setting applies only when the user accounts are managed using the local authentication server. They are not used when the external authentication server is used.	0 – 365
Password expiration warning period	The amount of time, in days, before the password expiration date that users begin to receive warnings about the impending expiration of the user password. If set to 0, users are never warned. The default is 5 days. **Note:** This setting applies only when the user accounts are managed using the local authentication server. They are not used when the external authentication server is used.	0 – *maximum password expiration setting*
Minimum password reuse cycle	The minimum number of times that a user must enter a unique password when changing the password before the user can start to reuse passwords. If set to 0, users can reuse passwords immediately. The default is 5 occurrences.	0 – 10
Minimum password change interval	The minimum amount of time, in hours, that must elapse before a user can change a password again after it was previously changed. The value specified for this setting cannot exceed the value specified for the password expiration period. If set to 0, users can change passwords immediately. The default is 24 hours.	0 – 1440
Maximum number of login failures	The maximum number of times that a user can attempt to log in with an incorrect password before the user account is locked out. The number specified for the lockout period after maximum login failures determines how long the user account is locked out. Accounts that are locked cannot be used to gain access to the system even if a valid password is provided. If set to 0, accounts are never locked. The failed login counter is reset to zero after a successful login. The default is 20 occurrences.	0 – 100

Table 1. Account Security settings (continued)

Security setting	Description	Values
Lockout period after maximum login failures	The minimum amount of time, in minutes, that must pass before a user that was locked out can attempt to log back in again. If set to 0, the account remains locked until an administrator explicitly unlocks it. A setting of 0 might make your system more exposed to serious denial of service attacks, where deliberate failed login attempts can leave accounts permanently locked. The default is 60 minutes. **Tip:** Any user with the role of Supervisor can unlock a user account. For more information, see Unlocking a user. **Note:** This setting applies only when the user accounts are managed using the local authentication server. They are not used when the external authentication server is used.	0 – 2880
Web inactivity session timeout	The amount of time, in minutes, that a user session that is established with XClarity Administrator can be inactive before the user is logged out. If set to 0, the web session never expires. The default is 1440 minutes. **Note:** When changing this value, only user sessions that start after the setting is changed are affected.	0 – 1440
Minimum password length	The minimum number of characters that can be used to specify a valid password. The default is 8 characters.	8 – 20
Maximum active sessions for a specific user	The maximum number of active sessions for a specific user that is allowed at any given time. If set to 0, the number of allowed active sessions for a specific user is unlimited. The default is 3 sessions.	1 – 20
Force user to change password on first access	Determine if a user is required to change the password when the user logs in to XClarity Administrator for the first time. The default is to require a user to change the password the first time that the user logs in.	Yes or No

Step 4. Click **Apply**.

What to do next

When successfully saved, the new settings take effect immediately. If you change the setting for web inactivity session timeout, active sessions are affected.

If you change password policies, those policies are enforced the next time a user logs in or changes the password.

Configuring cryptography settings

Cryptographic management is composed of communication modes and protocols that control the way that secure communications are handled between Lenovo XClarity Administrator and the managed systems.

About this task

The *cryptographic mode* determines how secure communications are handled between XClarity Administrator and all managed systems. If secure communications are implemented, it sets the encryption-key lengths to be used.

Note: Regardless of the cryptography mode that you select, NIST-approved Digital Random Bit Generators are always used, and only 128-bit or longer keys are used for symmetric encryption.

When you change the cryptographic mode in the XClarity Administrator, the cryptographic mode for all CMMs and baseboard management controllers in the managed devices are changed to the same setting automatically. Consider the following implications of changing the cryptographic mode:

- If you switch from compatibility mode to NIST SP 800-131A mode and the current certificate authority on the managed CMMs and baseboard management controllers use RSA-2048/SHA-1 (the default), an RSA-2048/SHA-256 certificate is regenerated on each managed chassis and server. This causes a mismatch between the newly generated server certificates on the CMMs and baseboard management controllers and the server certificate that is stored in the XClarity Administrator trust store. To resolve this issue, go to the Chassis page and Servers page, and click **All Actions → Resolve Untrusted Certificate** for each device (see Resolving an untrusted server certificate in the XClarity Administrator online documentation).
- Not all Flex switches support NIST SP 800-131A mode. If a Flex switch does support NIST SP 800-131A mode, you might need to change the configuration for the switches through the Flex switch interface. For information about support for NIST SP 800-131A and about switching Flex switches between compatibility mode and NIST SP 800-131A mode, see the product documentation that is available for the Flex switches. For more information, see CMM Reset in the Flex Systems online documentation.

Procedure

To change the cryptography settings, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Choose one of the following the cryptographic modes to use for secure communications:

- **Compatibility**. This mode is the default. It is compatible with older firmware versions, browsers, and other network clients that do not implement strict security standards that are required for compliance with NIST SP 800-131A.
- **NIST SP 800-131A**. This mode is designed to comply with the NIST SP 800-131A standard. XClarity Administrator is designed to always use strong cryptography internally and, where available, to use strong cryptography network connections. However, in this mode, network connections using cryptography that is not approved by NIST SP 800-131A is not permitted, including rejection of Transport Layer Security (TLS) certificates that are signed with SHA-1 or weaker hash.

  If you select this mode:

  – Event notifications might not be successfully pushed to some mobile-device subscriptions (see Forwarding events to mobile devices). External services, such as Android and iOS, present certificates that are signed with SHA-1, which is an algorithm that does not conform to the stricter requirements of NIST SP 800-131A mode. As a result, any connections to these services might fail with a certificate exception or a handshake failure.

  For more information about NIST SP 800-131A compliance, see Implementing NIST SP 800-131A compliance.

Step 3. Choose the minimum TLS protocol version to use for client connections to other servers (such as the LDAP client). There are two options:

- **TLSv1.2**. Enforces TLS v1.2 or later cryptography protocols on both XClarity Administrator and all managed endpoints used.

Step 4. Choose the minimum TLS protocol version to use for server connections (such as the web server). There are two options:

- **TLSv1.2**. Enforces TLS v1.2 or later cryptography protocols on both XClarity Administrator and all managed endpoints used.

Step 5. Choose the minimum TLS protocol version to use for the XClarity Administrator operating-system deployment and OS device-driver updates. There are two options:

- **TLSv1.2**. TLS v1.2 and later can be used.

  Only operating systems with an installation process that supports TLS 1.2 and strong cryptographic algorithms can be deployed and updated through XClarity Administrator.

Step 6. Choose the devices to which you want to apply changes.
- **Apply to management server only**.
- **Apply to managed devices only**
- **Apply to management server and managed devices**

  When you apply the cryptographic-settings changes to managed devices, XClarity Administrator provisions the new settings to all managed devices and attempts to resolve any new certificates on those devices.

Step 7. Click **Apply**.

Step 8. If you applied the cryptographic-settings changes to the management server, restart XClarity Administrator (see Restarting Lenovo XClarity Administrator).

What to do next

If you receive an alert that the server certificate is not trusted for a managed device, see Resolving an untrusted server certificate.

Working with security certificates

Lenovo XClarity Administrator uses SSL certificates to establish secure, trusted communications between XClarity Administrator and its managed devices (such as chassis and service processors in the System x servers) as well as communications with XClarity Administrator by users. By default, XClarity Administrator, CMMs, and baseboard management controllers use XClarity Administrator-generated certificates that are self-signed and issued by an internal certificate authority.

About this task

The default server certificate, which is uniquely generated in every instance of XClarity Administrator, provides sufficient security for many environments. You can choose to let Lenovo XClarity Administrator manage certificates for you, or you can take a more active role and customize or replace the server certificates. XClarity Administrator provides options for customizing certificates for your environment. For example, you can choose to:

- Generate a new server key and certificate that uses values that are specific to your organization.
- Generate a certificate signing request (CSR) that can be sent to your choice of certificate authority to create a signed certificate that can then be uploaded to XClarity Administrator trust store.
- Download the certificate to your local system so that you can import that certificate into your web browser's list of trusted certificates.

Lenovo XClarity Administrator provides a number of services that accept incoming Transport Layer Security (TLS) connections. When a client, such as a managed device or a web browser, connects to one of these services, Lenovo XClarity Administrator provides its *server certificate* to authenticate itself to the client. The client should maintain a list of certificates that it trusts. If Lenovo XClarity Administrator's server certificate is not included in the client's list, the client disconnects from Lenovo XClarity Administrator to avoid exchanging any security sensitive information with an untrusted source.

Lenovo XClarity Administrator acts as a client when communicating with managed devices and external services. When Lenovo XClarity Administrator connects to a device or external service, the device or external service provides its server certificate to authenticate itself to Lenovo XClarity Administrator. Lenovo XClarity Administrator maintains a list of certificates that it trusts. If the *trusted certificate* that is provided by the managed device or external service is not listed, Lenovo XClarity Administrator disconnects from the managed device or external service to avoid exchanging any security sensitive information with an untrusted source.

The following certificates are used by Lenovo XClarity Administrator:

- **Trusted Certificates**. These certificates verify that Lenovo XClarity Administrator can trust a device or server (in most cases) when that Lenovo XClarity Administrator acts as a client to establish a secure connection to another device or server. For example, certificates in this trust store are used when establishing a secure connection to managed devices and trusted LDAP servers. Additionally, the Lenovo XClarity Administrator internal CA certificate as well as the CA certificate of a customized externally-signed server certificate (if one is installed) are present in this trust store to support internal Lenovo XClarity Administrator communication.
- **External Services Certificates**. These certificates verify that Lenovo XClarity Administrator can trust another Lenovo server or other external server only for specific external services. This trust store is used when connecting to Lenovo to look up warranty status information. It is also used to connect to the Apple and Google push-notification server if Lenovo XClarity Mobile push notifications are enabled for an iOS or Android device. Certificates in this trust store are not trusted when establishing connections for other services (such as LDAP) unless you also add them to the main Trusted Certificates trust store. Removing certificates from this trust store prevents successful operation of these services.
- **Internally-Signed Certificates**. During the initial setup of Lenovo XClarity Administrator, a unique key and self-signed certificate are generated. These are used as the default certificate authority, which can be managed on the Certificate Authority page in the Lenovo XClarity Administrator security settings. It is not necessary to regenerate this certificate unless the key has been compromised or if your organization has a policy that all certificates must be replaced periodically (see Regenerating or restoring the Lenovo XClarity Administrator internally-signed server certificate).

  Also during the initial setup, a separate key is generated and a certificate is created that is signed by the internal certificate authority. This certificate used as the default Lenovo XClarity Administrator server certificate. It automatically regenerated each time Lenovo XClarity Administrator detects that the networking addresses (IP or DNS addresses) have changed to ensure that the certificate contains the correct addresses for the server. It can be customized and generated on demand (see Regenerating or restoring the Lenovo XClarity Administrator internally-signed server certificate).

  If you do not install an externally-signed server certificate, it is recommended that you perform the following steps to avoid certificate error messages in your browser:

  1. Download the internally-signed CA certificate using the download button on the Certificate Authority page and to install it into your web browser as a trusted root authority (see Importing the Certificate Authority certificate into a web browser).
  2. Regenerate the server certificate, following the help guidance when deciding whether to use an IP address or a hostname as the Common Name (see Regenerating or restoring the Lenovo XClarity Administrator internally-signed server certificate).

- **Externally-Signed Certificates**. You can choose to generate a certificate signing request (CSR) for signing by your organization's certificate authority or a third-party certificate authority. After the CSR is signed, you can import the full certificate chain and use it in place of the unique default internally signed certificates (see Installing a customized, externally signed server certificate).
- **OS Deploy Certificate**. A separate certificate is used by the operating-system deployment service to ensure that the operating-system installer can connect securely to deployment service during the operating-system installation process. The key and certificate that are used by this service are regenerated during every Lenovo XClarity Administrator boot. If the key has been compromised, you can regenerate it by restarting the management server.

Lenovo XClarity Administrator supports PKCS 1.5 RSA-2048/SHA-256 certificate signatures and ECDSA p256/SHA-256 signatures in all product configurations. Other algorithms such as SHA-1 stronger or SHA hashes might be supported depending on your configuration. Consider the selected cryptographic mode in Lenovo XClarity Administrator (see Configuring cryptography settings) and the capabilities of other software and devices in your environment. ECDSA certificates that are based on some elliptic curves (including p256), but not all elliptic curves, are supported on the Trusted Certificates page and in the signing chain of the Lenovo XClarity Administrator certificate but *are not* currently supported for use by the Lenovo XClarity Administrator server certificate.

Note: Only PKCS 1.5 RSA-2048/SHA-256 signatures are supported. RSA-PSS signatures are not supported at this time.

Installing a customized, externally signed server certificate

You can choose to use a server certificate that was signed by a private or commercial certificate authority (CA). To use an externally signed server certificate, generate a certificate signing request and then upload the resulting server certificate to replace the existing certificate in the Lenovo XClarity Administrator trust store that is used by the authentication, HTTPS, and CIM servers.

Before you begin

Ensure that all managed devices have the latest firmware installed before starting any task that might impact connections between the managed devices. To upgrade firmware on managed devices, see Updating firmware on managed devices.

Ensure that XClarity Administrator is successfully communicating with all managed devices by clicking **Hardware** and then clicking the device type (Chassis or Server). A page is displayed with a tabular view of all managed devices of that type. If any device has a status of "Offline," ensure that network connectivity is working between the management server and the device, and resolve untrusted server certificates if needed (see Resolving an untrusted server certificate).

About this task

When you install a customized externally signed server certificate in XClarity Administrator or a baseboard management-controller or CMM, you must provide the certificate bundle that contains the entire CA signing chain.

When you install a customized server certificate in a chassis or server that is not managed by XClarity Administrator, install the certificate bundle on the CMM before installing it on all management controllers in the CMM.

When you install a customized server certificate to a managed chassis, you first add the CA signing chain to the XClarity Administrator trust store, install the server certificate on every management controller and CMM, and then upload the server certificate to XClarity Administrator.

Tip: If the new server certificate has not been signed by a trusted third party, the next time that you connect to XClarity Administrator, your browser displays a security message and dialog prompting you to accept the new certificate into the browser. To avoid the security messages, you can import a downloaded server certificate into your web browser's list of trusted certificates. For more information about importing server certificates, see Importing the Certificate Authority certificate into a web browser.

Deploying customized server certificates to Lenovo XClarity Administrator

You can choose to generate a certificate signing request (CSR) for signing by your organization's certificate authority or a third-party certificate authority. The CSR creates a full certificate chain that you can import and use in place of the unique default internally signed certificates.

About this task

Attention: If NIST SP 800-131A is enabled (see Implementing NIST SP 800-131A compliance) and you are using or plan to use custom or externally signed certificates in an NIST, all certificates in the chain must be based on SHA-256 hashing functions.

When the server certificate is uploaded, XClarity Administrator attempts to provision the new CA certificate to all managed devices. If the provisioning process succeeds, XClarity Administrator begins using the new server certificate immediately. If the process fails, error messages are provided that direct you to correct any problems manually before applying the newly imported server certificate. After the errors are corrected, complete the installation of the previously uploaded certificate.

Note: If XClarity Administrator was already using a certificate signed by the same root authority, the CA does not need to be sent to devices, and XClarity Administrator begins to use the certificate immediately.

After uploading a certificate in XClarity Administrator v1.1.0 and earlier, the web server restarted and automatically terminated all browser sessions. XClarity Administrator v1.1.1 and later begin using the new certificate without terminating existing sessions. Any new sessions are established using the new certificate. To see the new certificate in use, restart your web browser.

Procedure

To generate and deploy a customized externally signed server certificate to Lenovo XClarity Administrator, complete the following steps.

Step 1. Create and download a certificate signing request (CSR) for XClarity Administrator.

a. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page

b. Click **Server Certificate** under the Certificate Management section to display the Server Certificate page.

c. Click the **Generate Certificate Signing Request (CSR)** tab.

d. Fill in the fields for the request.
- Country or Region
- State or Province
- City or Locality
- Organization
- Organization Unit (optional)
- Common Name

Attention: Select a common name that matches the IP address or hostname that XClarity Administrator uses to connect to the managed device. Failure to select the correct value might result in connections that are not trusted.

e. Customize the Subject Alternative Names (SANs) that are added to the X.509 "subjectAltName" extension when the CSR is generated.

By default, XClarity Administrator automatically defines Subject Alternative Names (SANs) for the CSR based on the IP address and hostname that are discovered by the XClarity Administrator guest operating system's network interfaces. You can customize, delete, or add to these SAN values.

The name that you specify must be valid for the selected type:
- **directoryName** (for example, `cn=lxca-example,ou=dcg,dc=company,dc=com`)
- **dNSName** (for example, `lxca-example.dcg.company.com`)
- **ipAddress** (for example, `192.0.2.0`)
- **registeredID** (for example, `1.2.3.4.55.6.5.99`)
- **rfc822Name** (for example, `example@company.com`)
- **uniformResourceIdentifier** (for example, `https://lxca-dev.dcg.company.com/example`)

Note: All SANs that are listed in the table are validated, saved, and added to the CSR only after you generate the CSR in the next step.

f. Click **Generate CSR File**. The server certificate is displayed in the Certificate Signing Request dialog.

g. Click **Save to File** to save the server certificate to the host server.

Step 2. Provide the CSR to a trusted certificate authority (CA). The CA signs the CSR and responds with a server certificate.

Step 3. Upload the externally signed server certificate to XClarity Administrator. The certificate content must be a bundle containing the CA's root certificate, any intermediate certificates, and the server certificate.

a. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

b. Click **Server Certificate** under the Certificate Management section.

c. Click the **Upload Certificate** tab.

d. Click **Upload Certificate** to display the Upload Certificate dialog.

e. Specify a certificate bundle file in PEM, DER or PKCS7 format, or paste the certificate bundle in PEM format.

f. Click **Upload** to upload the server certificate and store the certificate in the XClarity Administrator trust store.

Deploying customized server certificates to managed devices

You can deploy customized server certificates to managed devices by uploading and installing the externally-signed certificate bundle using the CMM and management controller for those devices.

Before you begin

Ensure that the latest firmware is installed on all managed devices (see Updating firmware on managed devices).

When generating a certificate signing request (CSR) for custom certificates, ensure that you select a common name that matches the IP address or hostname that is used to identify the device. Failure to select the correct value might result in connections that are not trusted.

Ensure that you obtain a certificate bundle that contains the entire signing chain, from the end-server certificate to the root (base) certificate of the trusted CA that can be used to verify the complete certificate chain of trust.

Do not change the Lenovo XClarity Administrator server certificate while a managed device is “Offline.” You must repair the connection before modifying Lenovo XClarity Administrator, otherwise additional steps might be required to repair the connectivity issues (see Resolving an untrusted server certificate).

About this task

This section contains recommendations for ensuring continued successful communication between Lenovo XClarity Administrator and the managed devices. For detailed instructions about how to generate a CSR and import a signed certificate, see your device documentation.

If Lenovo XClarity Administrator is managing one or more chassis, rack servers, and tower servers, and the default Lenovo XClarity Administrator internally signed certificates are currently installed on Lenovo XClarity Administrator and the managed devices, you can deploy customized server certificate.

If the externally signed server certificate is installed on the device *before* the you attempt to manage the device by Lenovo XClarity Administrator, no additional steps are needed. To deploy a custom server certificate to devices that are managed under Lenovo XClarity Administrator management, you must perform one of the following steps to ensure continued connectivity between the management server and the managed devices.

Procedure

Complete one of the following options to deploy the customized externally signed server certificate to managed chassis or servers.

- If Lenovo XClarity Administrator uses a certificate that is signed by the same certificate authority as the managed devices, perform the steps in Deploying customized server certificates to Lenovo XClarity Administrator *before* installing the certificates on managed devices. Installing the Lenovo XClarity Administrator certificate chain from the same CA first ensures that the certificate chain is in the Lenovo XClarity Administrator trust store and that Lenovo XClarity Administrator is able to trust the devices after the externally signed certificates are installed there.
- Add the externally signed certificates in the CA signing chains to the Lenovo XClarity Administrator trust store.

  You must add the CA root certificate and all intermediate certificates, one at a time, to the Lenovo XClarity Administrator trust store. The order does not matter. Each certificate must be installed once, so if all devices use the same CA and intermediate certificates, then the CA and each intermediate certificate must be installed in the Lenovo XClarity Administrator trust store one time. If more than one CA or an intermediate CA is used, ensure that each unique CA root certificate or intermediate certificate that is used in the signing chain of a managed device is imported the following these steps.

  Note: Do not add the end, non-CA server certificates during these steps.

  Perform the following steps for each certificate in the bundle.

  1. From the Lenovo XClarity Administrator menu bar, click **Administration → Security** to display the Security page.
  2. Click **Trusted certificates** under Certificate Management in the left navigation.
  3. Click the **Create** icon ( ) to display the Add Certificate dialog.
  4. Specify a certificate file in PEM or DER format, or paste the certificate in PEM format.
  5. Click **Create** to create the certificate.

  After the CA signing chain is installed, Lenovo XClarity Administrator trusts connections to CIM servers on the CMM and management controller on which the externally signed server certificate is installed.
- Import the externally signed certificates into the managed devices.

Note: If the necessary certificates are not present in the Lenovo XClarity Administrator trust store, connectivity is lost between Lenovo XClarity Administrator and the managed device. Perform the steps in Resolving an untrusted server certificate to repair the connection.

Important: This option involves temporary connectivity loss; therefore, one of the previous options is recommended.

Regenerating or restoring the Lenovo XClarity Administrator internally-signed server certificate

You can generate a new certificate authority or server certificate to replace current internally-signed certificates or to reinstate a Lenovo XClarity Administrator-generated certificate if XClarity Administrator currently uses a customized externally-signed server certificate. The new internally-signed server certificate is then used by the authentication, HTTPS, and CIM servers on the XClarity Administrator. It is also automatically provisioned to all managed devices.

Before you begin

When you regenerate or upload the XClarity Administrator certificate, XClarity Administrator is restarted.

If a new CA certificate is generated, the new CA certificate is automatically deployed to the trust store in each CMM and baseboard management controller in all managed chassis, rack servers, and tower servers to maintain trusted authentication-server connections. If an error occurs while deploying the CA root certificate, download it from the Certificate Authority page and import it manually into the trust store of any managed devices to which it was not successfully provisioned before generating a new server certificate.

If you plan to regenerate the CA certificate, reserve time to regenerate the CA, resolve any provisioning errors, and regenerate the server certificate within a short period of time.

After generating a new CA root certificate, communication errors might occur or you might not be able to log in to a device until after the server certificate is regenerated and signed.

Important: For XClarity Administrator v1.1.1 and earlier, you must import the CA root certificate into the trust store of each CMM and management controller. See the documentation for the CMM and management controller for more information about importing the CA root certificate

Procedure

Complete the following steps to restore an internally-signed server certificate on XClarity Administrator.

Note: The server certificate that is currently in use on XClarity Administrator, whether internally-signed or externally-signed, remains in use until new server certificate is regenerated and signed.

Step 1. Optional: **Optional:** Generate a new CA root certificate.

a. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

b. Click **Certificate Authority** under the Certificate Management section.

c. Click **Regenerate Certificate Authority Root Certificate**.

If the CA key and certificate are successfully regenerated, then a dialog is displayed showing the status of jobs to provision that certificate as an LDAP trusted certificate to all CMMs and management controllers (for Converged, NeXtScale, and System x servers). This dialog as well as the job monitoring page shows the success or failure of each of those provisioning jobs.

If any of the provisioning jobs fail, complete the following steps to download the CA root certificate, then manually import the root certificate as a trusted LDAP certificate in any device for which the job failed.

Step 2. Optional: **Optional:** Download the CA root certificate to the host system and import it into your web browser.

a. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

b. Click **Certificate Authority** under the Certificate Management section.

c. Click **Download Certificate Authority Root Certificate**. The current CA root certificate is displayed in the Certificate Authority Root Certificate dialog.

d. Click **Save to File** to save the CA root certificate to the host system.

e. Follow the instructions for your web browser and the web browser of other users who will access XClarity Administrator to import the certificate as a trusted root authority.

Step 3. Regenerate a new server certificate and sign the certificate with the new CA root certificate.

a. From the Security page, click **Server Certificate** under the Certificate Management section.

b. Click the **Regenerate Server Certificate** tab.

c. Fill in the fields in the Regenerate Server Certificate page:
- Country or Region
- State or Province
- City or Locality
- Organization
- Organization Unit
- Common Name
- Not valid before date
- Not valid before time
- Not valid after date
- Not valid after time

d. Click **Regenerate Certificate**.

e. If regenerating self-signed certificates on the managed CMMs and management controllers (for Converged, NeXtScale, ThinkSystem, and System x servers), after regenerating the certificate on each device, import the new device certificate into the XClarity Administrator trust store (see Resolving an untrusted server certificate). Alternatively, you can manually download the certificate from the device and import it into XClarity Administrator on the Trusted Certificates page.

For XClarity Administrator v1.1.0 and earlier, the web server restarts and automatically terminates all browser sessions after regenerating a certificate. For XClarity Administrator v1.1.1 and later, XClarity Administrator begins using the new certificate without terminating existing sessions. New sessions are established using the new certificate. To see the new certificate in use, restart your web browser.

Step 4. If regenerating self-signed certificates on the managed CMMs and management controllers (for Converged, NeXtScale, ThinkSystem, and System x servers), after regenerating the certificate on each device, import the new device certificate into the XClarity Administrator trust store (see Resolving an untrusted server certificate). Alternatively, you can manually download the certificate from the device and import it into XClarity Administrator on the Trusted Certificates page.

Resolving an untrusted server certificate

The server certificate that is used to establish a secure connection to a managed device can become untrusted. If the problem is due to a down-level version of the device CA root certificate or device self-signed

certificate in the Lenovo XClarity Administrator trust store, XClarity Administrator can resolve the untrusted server certificate.

About this task

If a managed device becomes untrusted, XClarity Administrator prevents communication with that device, preventing you from performing management or inventory operations on that device.

Procedure

To resolve an untrusted server certificate for a managed device, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware**, and then click the device type (**Chassis**, **Server**, **Storage**, or **Switch**). A page is displayed with a tabular view of all managed devices of that type.

Step 2. Select a specific device in the “Offline” state.

Step 3. Click **All Actions → Security → Resolve Untrusted Certificates**.

Step 4. Click **Install Certificate**.

XClarity Administrator retrieves the current certificate from the target device. If that certificate is different from the trusted certificate for that device in the XClarity Administrator trust store, the new certificate is placed in the XClarity Administrator trust store, overriding the previous certificate for that device.

If this does not resolve the issue, ensure that network connectivity is working between XClarity Administrator and the device.

Downloading the server certificate

You can download a copy of the current server certificate, in PEM or DER format, to your local system. You can then import the certificate into your web browser or another applications (such as Lenovo XClarity Mobile or Lenovo XClarity Integrator).

Procedure

Complete the following steps to download the server certificate.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

Step 2. Click **Server Certificate** under the Certificate Management section. The Server Certificate page is displayed.

Step 3. Click the **Download Certificate** tab.

Step 4. Click **Download Certificate**.

Step 5. Click **Save as der** or **Save as pem** to save the server certificate as a DER or PEM file on your local system.

Importing the Certificate Authority certificate into a web browser

To avoid security warning messages from your web browser when you access Lenovo XClarity Administrator, you can download a copy of the current Certificate Authority (CA) certificate, in PEM or DER format, to your local system, and then import that certificate into your web browser's list of trusted certificates.

About this task

Lenovo XClarity Administrator supports PKCS 1.5 RSA-2048/SHA-256 certificate signatures and ECDSA p256/SHA-256 signatures in all product configurations. Other algorithms such as SHA-1 stronger or SHA

hashes might be supported depending on your configuration. Consider the selected cryptographic mode in Lenovo XClarity Administrator (see Configuring cryptography settings) and the capabilities of other software and devices in your environment. ECDSA certificates that are based on some elliptic curves (including p256), but not all elliptic curves, are supported on the Trusted Certificates page and in the signing chain of the Lenovo XClarity Administrator certificate but *are not* currently supported for use by the Lenovo XClarity Administrator server certificate.

Note: Only PKCS 1.5 RSA-2048/SHA-256 signatures are supported. RSA-PSS signatures are not supported at this time.

Procedure

To download the server certificate, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

Step 2. Click **Certificate Authority** under the Certificate Management section. The Certificate Authority page is displayed.

Step 3. Click **Download Certificate Authority Root Certificate**.

Step 4. Click **Save as der** or **Save as pem** to save the server certificate as a DER or PEM file on your local system.

Step 5. Import the downloaded certificate into the list of trusted root authority certificates for your browser.

- **Firefox:**
  1. Open the browser, and click **Tools → Options → Advanced**.
  2. Click the **Certificates** tab.
  3. Click **View certificates**.
  4. Click **Import**, and browse to the location where the certificate was downloaded.
  5. Select the certificate, and click **Open**.
- **Internet Explorer:**
  1. Open the browser and click **Tools → Internet Options → Content**.
  2. Click **Certificates** to see a list of all certificates that are currently trusted.
  3. Click **Import** to display the Certificate Import wizard.
  4. Complete the wizard to import the certificate.

Adding and replacing a certificate revocation list

A *certificate revocation list* is a list of certificates that have been revoked and are no longer trusted. A certificate might be revoked if it was incorrectly issued from by the CA or if its key is compromised, lost, or stolen.

Procedure

Complete the following steps to add a new certificate revocation list or to replace an existing certificate revocation list.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

Step 2. Click **Certificate Revocation Lists** under Certificate Management in the left navigation. The Certificate Revocation Lists page is displayed with a list of all certificate revocation lists.

Step 3. Click **Add / Replace CLR** to add a certificate revocation list, or select a certificate revocation list and click the **Add / Replace CLR** to replace the CRL.

Step 4. Specify a certificate revocation list file, in PEM or DER format, or paste the certificate in PEM format.

Step 5. Click **Create** to create the certificate revocation list.

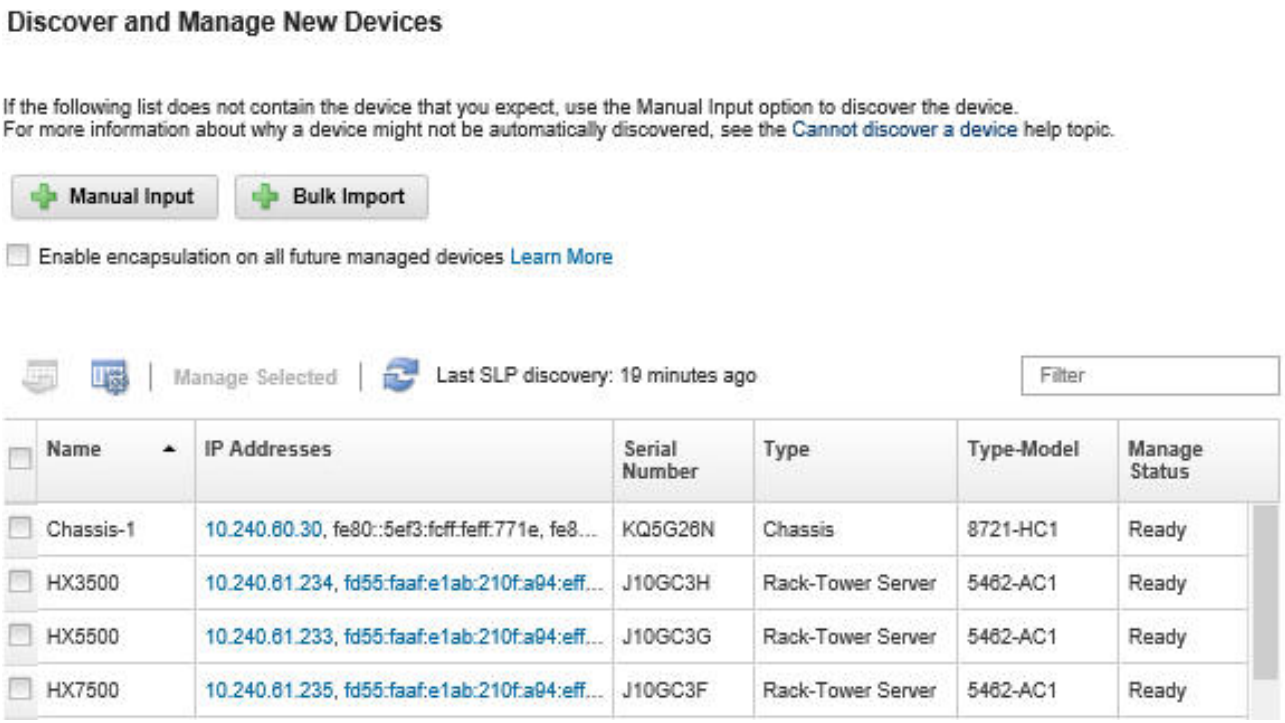
Enabling encapsulation

When you manage Lenovo chassis and servers in Lenovo XClarity Administrator, you can configure Lenovo XClarity Administrator to change the firewall rules for the devices so that incoming requests are accepted only from Lenovo XClarity Administrator. This is referred to as *encapsulation*. You can also enable or disable encapsulation on chassis and servers that are already managed by Lenovo XClarity Administrator.

When enabled on devices that support encapsulation, Lenovo XClarity Administrator changes the device encapsulation mode to “encapsulationLite,” and changes the firewall rules on the device to limit incoming requests from only this Lenovo XClarity Administrator.

When disabled, the encapsulation mode is set to “normal”. If encapsulation was previously enabled on the devices, the encapsulation firewall rules are removed.

You can enable or disable encapsulation globally for all devices during the management process by selecting the **Enable encapsulation on all future managed devices** checkbox on the Discover and Manage New Devices page. The encapsulation is disabled by default.



You can also enable or disable encapsulation individually for specific managed devices at any time by navigating to the device summary page, selecting the device, and clicking **Actions → Enable Encapsulation** or **Actions → Disable Encapsulation**.

Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.

Note: Encapsulation is not supported on switches, storage devices, and non-Lenovo chassis and servers.

Implementing NIST SP 800-131A compliance

If you must be compliant with NIST SP 800-131A, you can begin to work toward a fully compliant environment using Lenovo XClarity Administrator.

About this task

The National Institute of Standards and Technology Special Publication 800-131A (NIST SP 800-131A) specifies the way that secure communications should be handled. The standard strengthens algorithms and increases key lengths to improve security. The NIST SP 800-131A standard requires that users be configured for strict enforcement of the standard.

Notes: The following Flex System components do not currently support NIST SP 800-131A. Communications between XClarity Administrator or the CMM and these components are not compliant:

- Flex System EN4023 10 Gb Scalable Switch
- Flex System EN6131 40 Gb Ethernet Switch
- Flex System FC3171 8 Gb SAN Switch
- Flex System FC5022 16 Gb SAN Scalable Switch
- Flex System IB6131 Infiniband Switch
- Flex System v7000 Storage Node

Note: When an SAML identity provider is used for authentication, XClarity Administrator uses SHA-1 to sign the signature in the metadata. Using the SHA-1 algorithm for digital signatures is not NIST SP 800-131A compliant.

Procedure

To implement NIST SP 800-131A compliance, complete the following steps.

Step 1. Ensure that your devices meet the following criteria:

- Use Secure Sockets Layer (SSL) over the TLS v1.2 protocol.
- Use SHA-256 or stronger hashing functions for digital signatures and SHA-1 or stronger hashing functions for other applications.
- Use RSA-2048 or stronger, or use NIST approved Elliptic Curves that are 224 bits or stronger.
- Use NIST-approved symmetric encryption with keys at least 128 bits in length.
- Use NIST-approved random-number generators.
- Where possible, support Diffie-Hellman or Elliptic Curve Diffie-Hellman key-exchange mechanisms.

Step 2. Configure the cryptographic settings on Lenovo XClarity Administrator. There are two settings that are related to NIST SP 800-131A compliance:

- The *SSL/TLS mode* specifies the protocols that are to be used for secure communications. The XClarity Administrator supports a setting of **TLS 1.2 Server and Client** to restrict the cryptography protocol to TLS 1.2 on XClarity Administrator and all managed devices.
- If secure communications are implemented, the *cryptographic mode* sets the encryption key lengths that are to be used. You can set the cryptographic mode as **NIST SP 800-131A**. However, you might not be able to deploy some operating systems through XClarity Administrator because some operating-system installers do not support the restricted settings. To support operating system deployment, you can choose to allow an exception for operating-system deployment.

When you change any cryptographic settings, XClarity Administrator provisions the new settings to all managed devices and attempts to resolve any new certificates on those devices.

Note: You must manually restart XClarity Administrator after cryptographic settings are changed for the changes to take effect and to restore any lost services (see Restarting Lenovo XClarity Administrator).

For more information about these settings, see Configuring cryptography settings.

Step 3. Use a web browser that supports the TLS1.2 protocol and SHA-256 hashing functions, and enable those settings in your web browser.

Note: If you use or plan to use custom or externally signed certificates, all certificates in the chain must be based on SHA-256 hashing functions.

Step 4. Use encrypted protocols for all communications. Do not enable unencrypted protocols, such as Telnet, FTP, SSH, and VNC for remote communications with XClarity Administrator managed devices.

Using VMware Tools

The VMware Tools package is installed in the virtual machine's guest operating system when you install Lenovo XClarity Administrator in VMware ESXi-based environments. This package provides a subset of the VMware tools that support optimized virtual-appliance backup and migration while preserving application state and continuity.

For information about using the VMware Tools, see Using the VMware Tools Configuration Utility in the VMware vSphere Documentation Center website.

Configuring network access

When you initially set up Lenovo XClarity Administrator, you configure up to two network interfaces. In addition, you must specify which of those interfaces is to be used to deploy operating systems. After the initial setup, you can modify these settings.

Before you begin

Attention:

- Changing the XClarity Administrator IP address after managing devices might cause the devices to be placed in offline state in XClarity Administrator. Ensure that all devices are unmanaged before changing the IP address.
- You can enable or disable checking for duplicate IP addresses in the same subnet by clicking the **Duplicate IP address checking** toggle. It is disabled by default.

  When enabled, XClarity Administrator raises an alert if you attempt to change the IP address of XClarity Administrator or manage a device that has the same IP address as another device that is under management or another device found in the same subnet.
- If the network interface for the management network is configured to use the Dynamic Host Configuration Protocol (DHCP), the management-interface IP address might change when the DHCP lease expires. If the IP address changes, you must unmanage the chassis, rack and tower servers, and then manage them again. To avoid this problem, either change the management interface to a static IP address, or ensure that the DHCP server configuration is set so that the DHCP address is based on a MAC address or that the DHCP lease does not expire.
- If you *do not* intend to use XClarity Administrator to deploy operating system or update OS device drivers, you can disable Samba and Apache servers by changing the network interface to use the **discover and manage hardware only** option. Note that the management server is restarted after changing the network interface

About this task

XClarity Administrator has two separate network interfaces (eth0 and eth1) that can be defined for your environment, depending on the network topology that you implement.

- When only one network interface (eth0) is present:
  - The interface must be configured to support the device discovery and management (such as server configuration and firmware updates). It must be able to communicate with the CMMs and Flex switches in each managed chassis, the baseboard management controller in each managed server, and each RackSwitch switch.
  - If you intend to acquire firmware and OS device-driver updates using XClarity Administrator, the network interface must be connected to the Internet, preferably through a firewall. Otherwise, you must manually import updates into the repository.
  - If you intend to collect service data or use automatic problem notification (including Call Home), the interfaces must be connected to the Internet, preferably through a firewall.
  - If you intend to deploy operating-system images and update OS device drivers, the interface must have IP network connectivity to the server network interface that is used to access the host operating system.

    Note: If you implemented a separate network for OS deployment and OS device-driver updates, you can configure the second network interface to connect to that network instead of the data network. However, if the operating system on each server does not have access to the data network, configure an additional interface on the servers to provide connectivity from the host operating system to the data network for OS deployment and OS device-driver updates, if needed
- When two network interfaces (eth0 and eth1) are present:
  - The first network interface (typically the Eth0 interface) must be connected to the management network and configured to support the device discovery and management (including server configuration and firmware updates. It must be able to communicate with the CMMs and Flex switches in each managed chassis, the management controller in each managed server, and each RackSwitch switch.
  - The second network interface (typically the eth1 interface) can be configured to communicate with an internal data network, a public data network, or both.
  - If you intend to acquire firmware and OS device-driver updates using XClarity Administrator, the interface that you use for the management network must be connected to the Internet, preferably through a firewall. Otherwise, you must import updates into the repository.
  - If you intend to collect service data or use automatic problem notification (including Call Home and Lenovo Upload Facility), at least one of the network interfaces must be connected to the Internet, preferably through a firewall.
  - If you intend to deploy operating-system images and update device drivers, you can choose to use either eth1 or eth0 interface. However, the interface that you use must have IP network connectivity to the server network interface that is used to access the host operating system.

    Note: If you implemented a separate network for OS deployment and OS device-driver updates, you can configure the second network interface to connect to that network instead of the data network. However, if the operating system on each server does not have access to the data network, configure an additional interface on the servers to provide connectivity from the host operating system to the data network for OS deployment and OS device-driver updates, if needed
  - Other XClarity Administrator functions (including discovery and hardware management, server configuration, firmware downloads and updates, service-data collection, automatic problem notification, and warranty data retrieves) can be performed from either interface.

The following table shows possible configurations for the XClarity Administrator network interfaces based on the type of network topology that has been implemented in your environment. Use this table to determine how to define each network interface.

Table 2. Role of each network interface based on network topology

Network topology	Role of interface 1 (eth0)	Role of interface 2 (eth1)
Converged network (management and data network with support for OS deployment and OS device-driver updates)	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval • OS deployment • OS device-driver updates	None
Separate management network with support for OS deployment and OS device-driver updates and data network	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval • OS deployment • OS device-driver updates	Data network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval
Separate management network and data network with support for OS deployment and OS device-driver updates	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval	Data network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval • OS deployment • OS device-driver updates

Table 2. Role of each network interface based on network topology (continued)

Network topology	Role of interface 1 (eth0)	Role of interface 2 (eth1)
Separate management network and data network without support for OS deployment and OS device-driver updates	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval	Data network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval
Management network only (OS deployment and OS device-driver updates is not supported)	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval	None

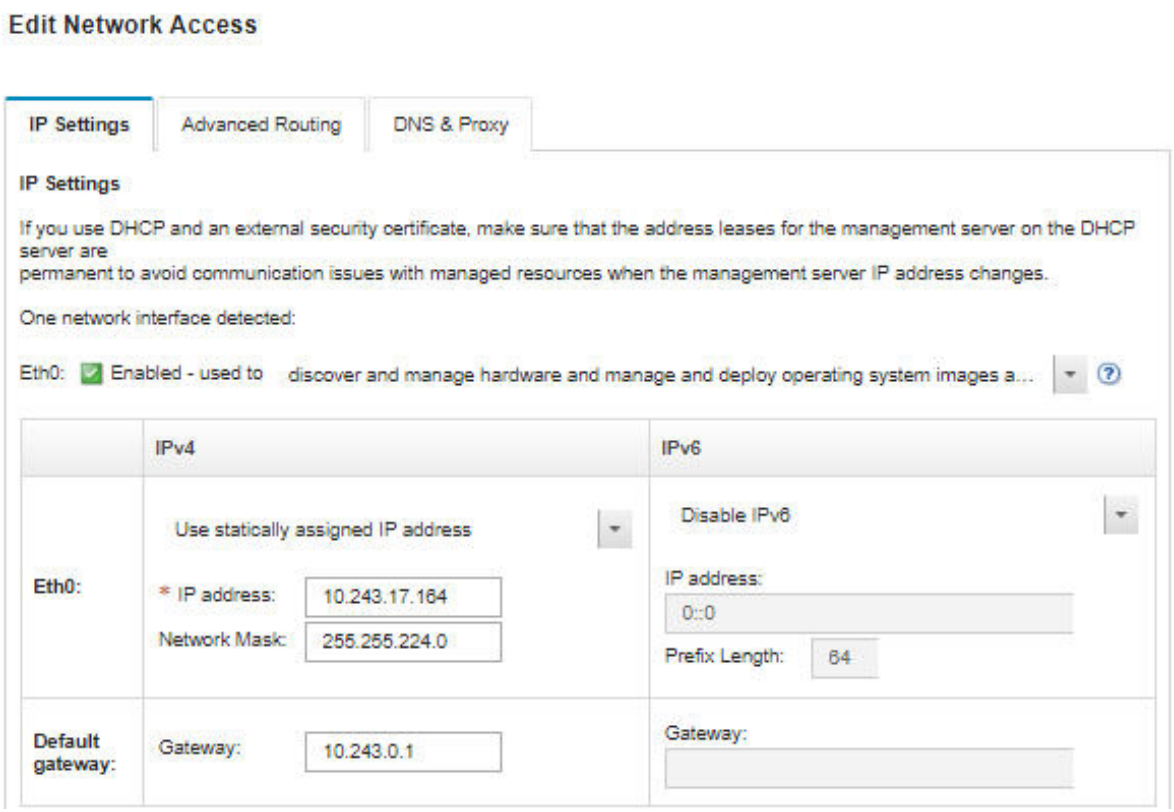
For more information about XClarity Administrator network interfaces including IPv6 address limitations, see Network considerations in the XClarity Administrator online documentation.

Procedure

To configure network access, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Network Access**. The currently defined network settings are displayed.
- Network topology
- Eth0 IP settings
- Eth1 IP settings (if the Eth1 interface exists)
- Routing settings
- Hostname and domain for virtual appliance
- DNS search order

Step 2. Click **Edit Network Access** to display the Edit Network Access page.



Step 3. If you intend to deploy operating-systems and update OS device drivers using XClarity Administrator, choose the network interface to use for managing operating systems.

- If only one interface is defined for XClarity Administrator, choose whether that interface is to be used to discover and manage hardware only, or whether it is also to be used to manage operating systems.
- If two interfaces are defined for XClarity Administrator (Eth0 and Eth1), determine which interface is to be used to manage operating systems. If you choose “None”, you *cannot* deploy operating-system images or update OS device drivers to managed servers from XClarity Administrator.

Step 4. Modify the IP Settings.

a. For the first interface, specify the IPv4 address, IPv6 address, or both.

- **IPv4**. You must assign an IPv4 address to the interface. You can choose to use a statically assigned IP address or obtain an IP address from a DHCP server.
- **IPv6**. Optionally, you can assign an IPv6 address to the interface using one of the following assignment methods:
  - Use statically assigned IP address
  - Use stateful address configuration (DHCPv6)
  - Use stateless address auto configuration

  Note: For information about IPv6 address limitations, see IPv6 configuration limitations in the XClarity Administrator online documentation.

b. If a second interface is available, specify the IPv4 address, the IPv6 address, or both.

Note: The IP addresses that are assigned to this interface must be in a different subnet from the IP addresses that are assigned to the first interface. If you choose to use DHCP to assign IP addresses for both interfaces (Eth0 and Eth1), the DHCP server must not assign the same subnet for the IP addresses of the two interfaces.

- **IPv4**. You can choose to use a statically assigned IP address or obtain an IP address from a DHCP server.
- **IPv6**. Optionally, you can assign an IPv6 address to the interface using one of the following assignment methods:
  - Use statically assigned IP address
  - Use stateful address configuration (DHCPv6)
  - Use stateless address auto configuration

c. Specify the default gateway.

If you specify a default gateway, it must be a valid IP address and must use the same network mask (the same subnet) as the IP address for one of the network interfaces (Eth0 or Eth1). If you use a single interface, default gateway must be on the same subnet as network interface.

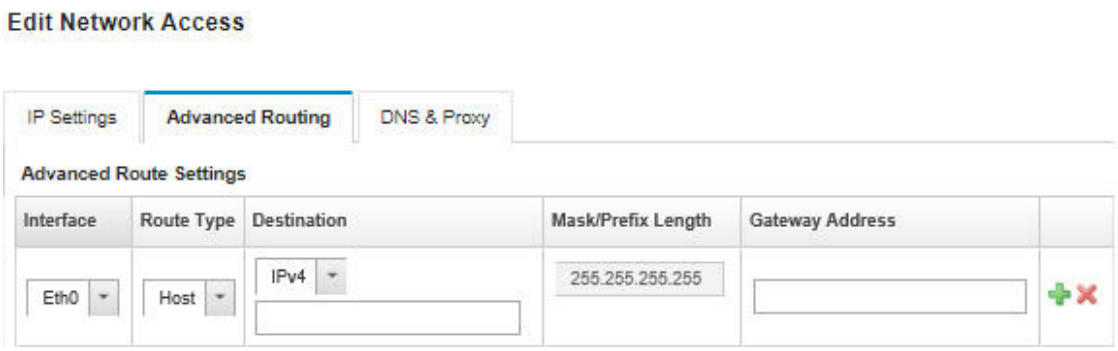
Tip: The default gateway must use the same network mask (the same subnet) as at least one enabled interface. Therefore, if you assign the default gateway to be on the same subnet as the second interface and then change the IP address assignment method or disable the second interface, the default gateway might not be reachable.

If either interface uses DHCP to obtain an IP address, the default gateway also uses DHCP.

d. Click **Save IP Settings**.

Step 5. Optionally, modify the advanced settings.

a. Click the **Advanced Routing** tab.



b. Specify one or more route entries in the **Advanced Route Settings** table to be used by this interface.

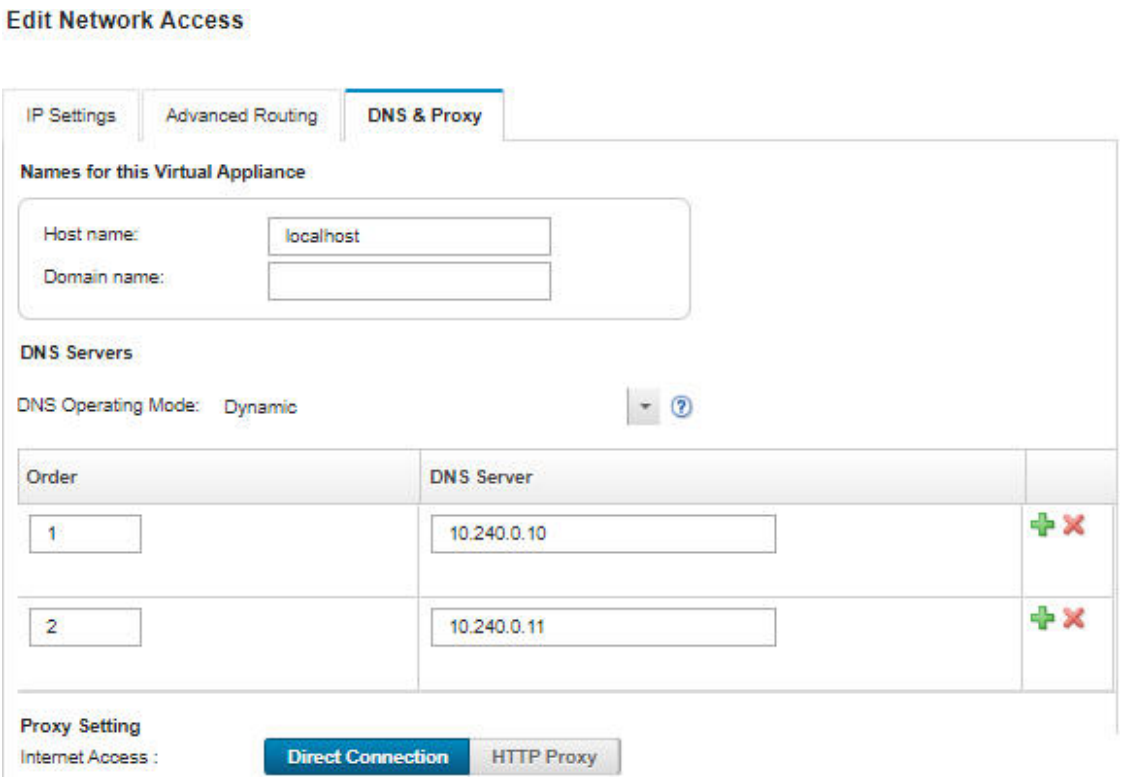
To define one or more route entries, complete the following steps.

1. Choose the interface.
2. Specify the route type, which can be a route to another host or to a network.
3. Specify the destination host or network address to which you are directing the route.
4. Specify the subnet mask for the destination address.
5. Specify the gateway address to which packets are to be addressed.

c. Click **Save Advanced Routing**.

Step 6. Optionally, modify the DNS and proxy settings.

a. Click the **DNS & Proxy** tab.



b. Specify the hostname and domain name to be used for XClarity Administrator.

c. Select the DNS operating mode. This can be **Static** or **DHCP**.

   Note: If you choose to use a DHCP server to obtain the IP address, any changes that you make to the **DNS Server** fields are overwritten the next time XClarity Administrator renews the DHCP lease.

d. Specify the IP address of one or more Domain Name System (DNS) servers to be used, and the priority order for each.

e. Specify whether to access the Internet using a direct connection or an HTTP proxy (if XClarity Administrator has access to the Internet).

   Notes: If using a HTTP proxy, ensure that the following requirements are met.
   - Ensure that the proxy server is set up to use basic authentication.
   - Ensure that the proxy server is set up as a non-terminating proxy.
   - Ensure that the proxy server is set up as a forwarding proxy.
   - Ensure that load balancers are configured to keep sessions with one proxy server and not switch between them.

   If you choose to use an HTTP proxy, complete the required fields:
   1. Specify the proxy server hostname and port.
   2. Choose whether to use authentication, and specify the user name and password if required.
   3. Specify the proxy test URL.
   4. Click **Text Proxy** to verify that the proxy settings are configured and working correctly.

f. Click **Save DNS & Proxy**.

Step 7. Click **Restart** to restart the management server.

Step 8. Click **Test Connection** to verify the network settings.

Setting the date and time

You can set the date and time to be used for Lenovo XClarity Administrator.

Before you begin

You must use at least one (and up to four) Network Time Protocol (NTP) server to synchronize the time stamps for all events that are received from managed devices with XClarity Administrator.

Tip: The NTP server must be accessible over the management network (typically the Eth0 interface). Consider setting up the NTP server on the host where XClarity Administrator is running.

If you change the time on the NTP server, it might take a while for XClarity Administrator to synchronize with the new time.

Attention: The XClarity Administrator virtual appliance and its host must be set to synchronize to the same time source to prevent inadvertent time mis-synchronization between XClarity Administrator and its host. Typically, the host is configured to have the its virtual appliances time-sync to it. If XClarity Administrator is set to synchronize to a different source than its host, you must disable the host time synchronization between XClarity Administrator virtual appliance and its host.

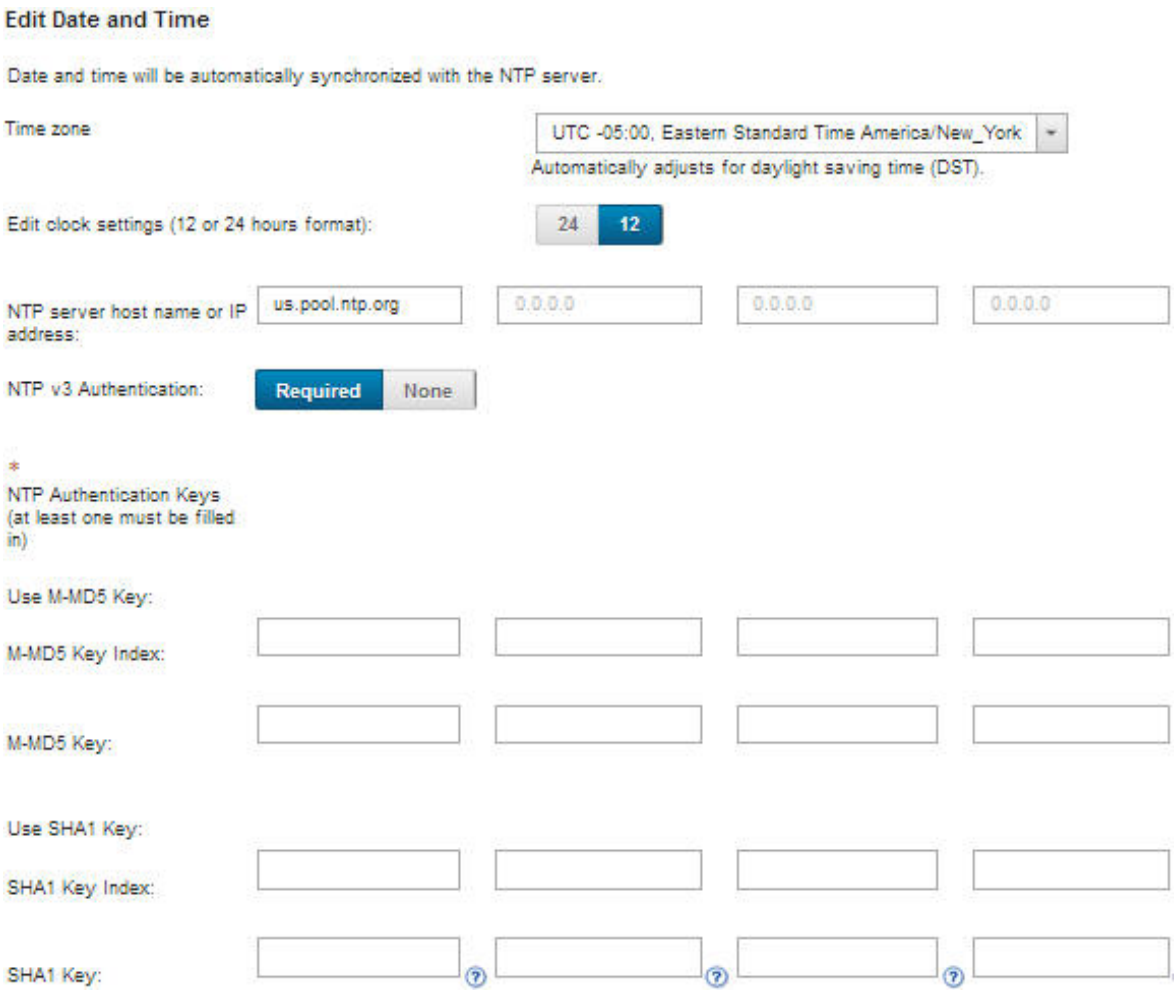
- For ESXi, following instructions on the VMware – Disabling Time Synchronization webpage.
- For Hyper-V, from Hyper-V Manager, right-click the XClarity Administrator virtual machine, and then click **Settings**. In the dialog, click **Management > Integration Services** in the navigation pane, and then clear **Time synchronization**.

Procedure

Complete the following steps to set the date and time for XClarity Administrator.

Step 1. From the XClarity Administrator menu bar, click **Administration → Date and Time**. The Date and Time page is displayed. This page shows the current date and time for XClarity Administrator.

Step 2. Click **Edit Date and Time** to display the Edit Date and Time page.



Step 3. Fill in the date and time dialog.

1. Choose the time zone where the host for XClarity Administrator is located.

   If the selected time zone observes daylight saving time (DST), the time is automatically adjusted for DST.

2. Choose to use a 12-hour or 24-hour clock.
3. Specify the hostname or IP address for each NTP server within your network. You can define up to four NTP servers.
4. Select **Required** to enable NTP v3 authentication, or select **None** to use NTP v1 authentication between XClarity Administrator and the NTP servers within your network.

   You can use v3 authentication if the managed Flex System CMMs and baseboard management controllers have firmware that require v3 authentication, and if NTP v3 authentication is required between XClarity Administrator and one or more NTP servers within your network

5. If you enabled NTP v3 authentication, set the authentication key and index for each applicable NTP server. You can specify an M-MD5 key, SHA1 key, or both. If both M-MD5 or SHA1 keys are specified, XClarity Administrator pushes either M-MD5 or SHA1 key to the managed Flex System CMMs and management controllers that support it. The XClarity Administrator uses the key to authenticate to the NTP server

   - For the M-MD5 key, specify an ASCII string that includes only upper and lower case letters (a-z, A-Z), digits (0–9) and the following special characters @# .

- For the SHA1 key, specify a 40-character ASCII string, including only 0–9 and a-f.
- The specified key index and authentication key must match the key ID and password values that is set on the NTP server. For example, if the key index of the entered SHA1 key in the NTP server is 5, the specified key index of the XClarity Administrator SHA1 key is also 5. For information about setting the key ID and password, see your NTP server documentation.
- You must specify the key for each NTP server that uses v3 authentication, even if two or more NTP servers use the same key.
- If you enable v3 authentication but do not provide an authentication key and index for an NTP server, v1 authentication is used by default.
- If you specified multiple NTP servers, the NTP servers must be either all v3-authenticated or all v1-authenticated. A mix of v3-authenticated or and v1-authenticated NTP servers was not supported.
- If you specified multiple NTP servers with v3-authentication, the key indices must be unique if the keys are not the same. For example, NTP server 1 and 2 cannot have the SHA1 key index of 1 if the SHA1 keys are different in the NTP server 1 and 2. You must reconfigure one of the NTP servers to accept the key with a different key index than the other NTP server; otherwise, that last defined key that was associated with a key index will be configured for all NTP servers with the same key index.

Step 4. Click **Save**.

Setting inventory preferences

You can set inventory preferences for managed devices, including the property to use to display the device name.

Procedure

Complete the following steps to set the inventory preferences for managed devices.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Inventory Preferences**. The Inventory Preferences page is displayed.

Step 2. Select the property to use for the device name that is displayed in the Lenovo XClarity Administrator user interface. You can select one of the following properties.
- **Predefined sequence (default)**
- **User-defined name**
- **DNS hostname**
- **Hostname**
- **IPv4 address**
- **Serial number**

If **Predefined sequence** is selected, the device name that is displayed is chosen based on the sequence of properties in the previous list. For example, if a device has a user-defined name, that name is displayed. If a device does not have a user-defined name, then the DNS host name is displayed. If a device does not have a user-defined name or DNS host name, the hostname is displayed.

Note: Selecting a value other than the default changes that the name that is displayed in the Lenovo XClarity Administrator user interface for all devices to the selected property. The user-defined name that is assigned to the device does not change.

Step 3. Optionally click **Enable** to choose to sort grids (tables) using the value that is selected for the device name.

Step 4. Select the rack numbering order preference, either top to bottom (for example, 1 – 52) or bottom to top (for example, 52 – 1).

Note: Changing the number order preference does not change the location of a device in the rack.

Step 5. Click **Apply**.

What to do next

You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level (see Setting threshold preferences for generating alerts and events).

Setting threshold preferences for generating alerts and events

You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level.

Procedure

Complete the following steps to forward specific service files to the service provider.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts** to display the Alerts page.

Step 2. Click the **Threshold Settings** icon ( ) to display the Threshold Settings dialog.

Step 3. Modify the warning or critical thresholds for the remaining life of SSDs in ThinkSystem and ThinkServer servers.

Remaining life of SSDs is calculated using vendor SMART counters. The default values are 30% for the warning threshold and 20% for the critical threshold.

Step 4. Select the **Enabled** toggle to generate an alert and event when each threshold is reached.

Step 5. Click **Apply**.

Setting up automatic problem notification to Lenovo Support (Call Home)

You can create a service forwarder that automatically sends service data for any managed device to Lenovo Support using the Call Home when certain serviceable events, such as an unrecoverable memory, are received from specific managed devices so that the issue can be addressed. This service forwarded is named “Default Call Home.”

Lenovo is committed to security. When enabled, Call Home automatically contacts Lenovo to open a service ticket and sends in service data collected from a managed device when that device reports a hardware failure or when you choose to initiate a manual Call Home. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later; your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel.

Before you begin

Attention: You must accept the Lenovo Privacy Statement before you can transfer data to Lenovo Support.

Ensure that all ports that are required by Lenovo XClarity Administrator (including ports that are required for Call Home) are available before you enable Call Home. For more information about ports, see Port availability in the XClarity Administrator online documentation.

Ensure that a connection exists to the Internet addresses that are required by Call Home. For information about firewalls, see Firewalls and proxy servers in the XClarity Administrator online documentation.

If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is configured to use basic authentication and is set up as a non-terminating proxy. For more information about setting up the proxy, see Configuring network accessConfiguring network access in the XClarity Administrator online documentation.

About this task

A *service forwarder* defines information about where to send the service data files when a serviceable event occurs. You can define up to 50 service forwarders.

Note: For XClarity Administrator v2.3 and later, service requests are no longer routed directly to IBM. When Call Home is enabled, service requests are first routed to the Lenovo Support, and then forwarded to IBM, if appropriate for certain devices.New DNS names and IP addresses are required to use Call Home to route service requests to Lenovo Support in for XClarity Administrator v2.3.0 and later. The old DNS names and IP addresses are no longer required to use Call Home; however, they are needed to retrieve status for open service tickets that were submitted prior to updating to v2.3.0.

If a Call Home service forwarder is not configured, you can manually open a service ticket and send service files to the Lenovo Support Center by following the instructions on the New Service Request webpage. For information about collecting and downloading service files, see Downloading XClarity Administrator diagnostic files and Collecting and downloading diagnostic files for a device in the XClarity Administrator online documentation.

If a Call Home service forwarder is configured but not enabled, you can *manually* open a service ticket using the Call Home function to collect and transfer service files to the Lenovo Support Center at any time. For more information, see Opening a service ticket in the XClarity Administrator online documentation.

When a Call Home service forwarder is configured and enabled, XClarity Administrator *automatically* opens a service ticket and transfers service files to the Lenovo Support Center when a serviceable event occurs so that the issue can be addressed.

Note: When a Call Home service forwarder is enabled in Lenovo XClarity Administrator, Call Home is disabled on each managed device to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices or if you intend to disable Call Home in XClarity Administrator, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time. For information about re-enabling Call Home on all managed devices when the service forwarder for Call Home is disabled, see Re-enabling call home on all managed devices in the XClarity Administrator online documentation..Although XClarity Administrator supports Call Home for ThinkAgile and ThinkSystem devices, the baseboard management controller for some ThinkAgile and ThinkSystem devices does not include Call Home support. Therefore, you cannot enable or disable Call Home on those devices themselves. Call Home can be enabled only for those devices at the XClarity Administrator level.

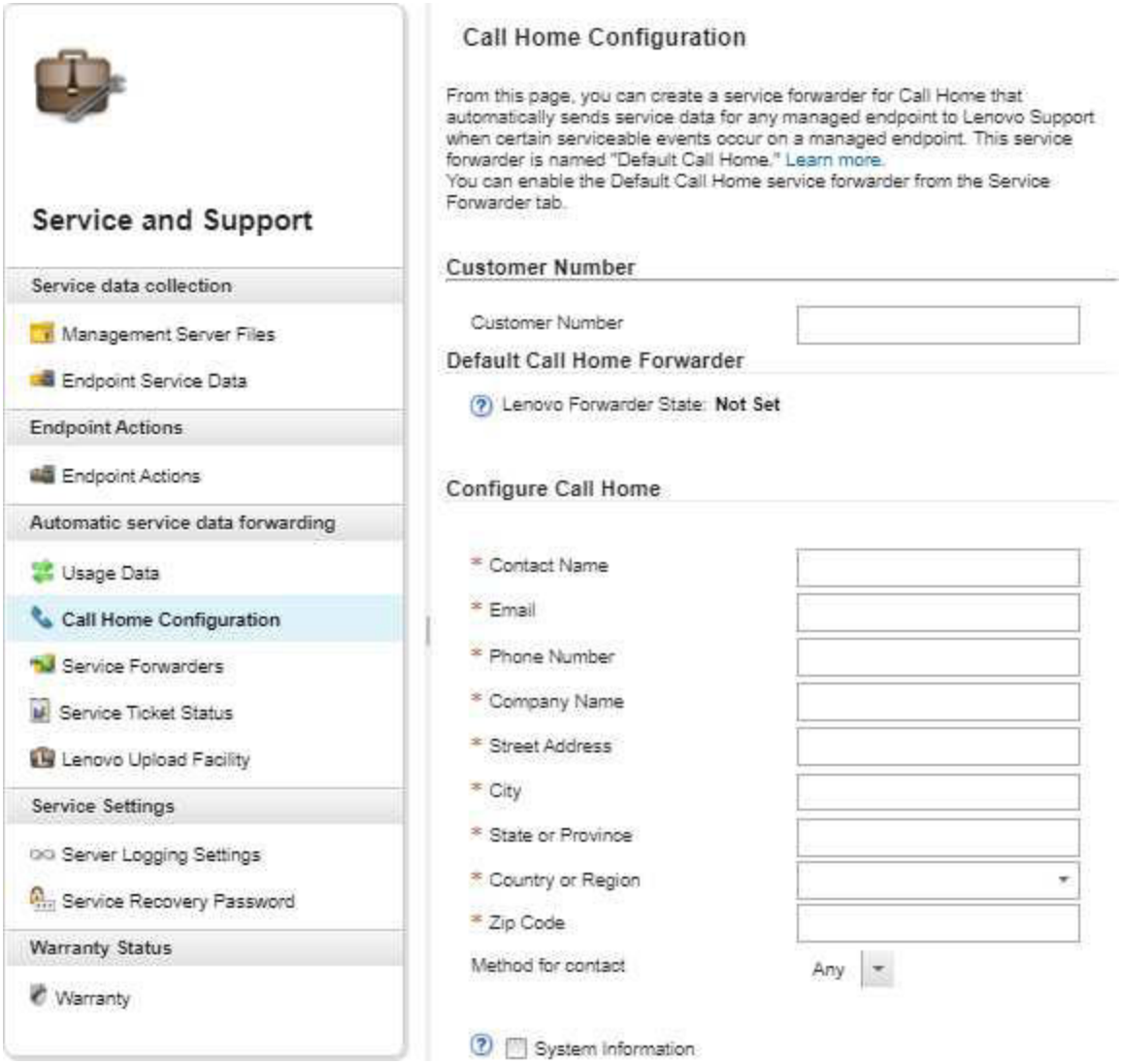
Call home is suppressed for repeated events for any device if a service ticket is open for that event on that device. Call Home is also suppressed for similar events for any ThinkAgile and ThinkSystem device if a service ticket is open for an event on that device. ThinkAgile and ThinkSystem events are 16-characters strings in the following format *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (for example, `806F010D0401FFFF`). Events are similar if they have the same reading type, sensor type, and entity ID. For example, if a service ticket is open for event 806F010D0401FFFF on a specific ThinkAgile or ThinkSystem device, any events that occur on that device with event IDs like *xx*`6F01`*xx*`04`*xxxxxx*, where *x* is any alphanumeric character, are suppressed.

For information about viewing service tickets that were opened automatically by a Call Home service forwarder, see Viewing problem records and status in the XClarity Administrator online documentation.

Procedure

Complete the following steps to setup a service forwarded for Call Home.

- Setup Call Home for all managed devices (current and future):
  1. From the XClarity Administrator menu bar, click **Administration → Service and Support**.
  2. Click **Call Home Configuration** in the left navigation to display the Call Home Configuration page.



  3. (Optional) Specify the default Lenovo customer number to use when reporting problems with XClarity Administrator.

     Tip: You can find your customer number in the proof-of-entitlement email that you received when you purchased Lenovo XClarity Pro.
  4. Fill in the contact and location information.
  5. Select the preferred method of contact by Lenovo Support.
  6. (Optional) Fill in the system information.
  7. Click **Apply**.

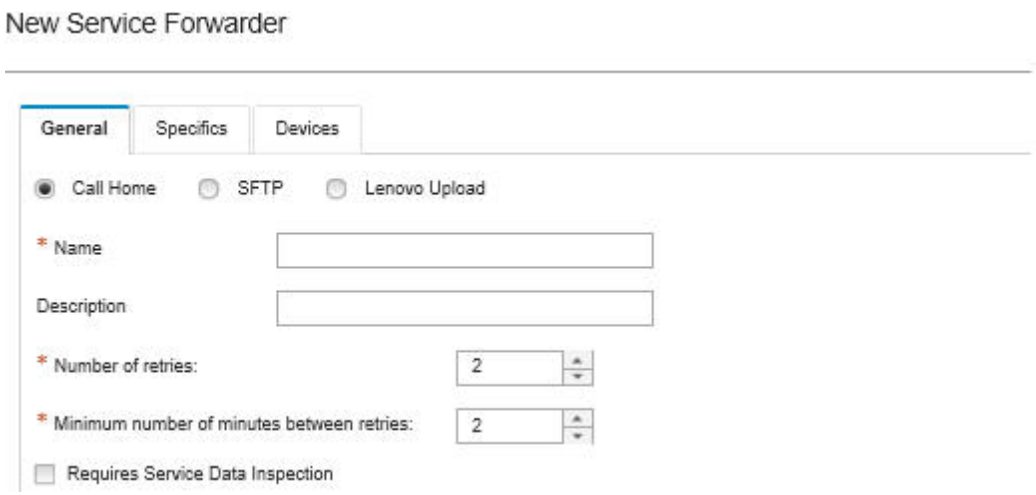
A Call Home service forwarder named “Default Call Home” is created for all managed devices using the specified contact information.

8. Enable and test the “Default Call Home” service forwarder.
   a. Click **Service Forwarder** in the left navigation to display the Service Forwarders page.
   b. Select **Enable** in the **Status** column for the “Default Call Home” service forwarder.
   c. Select the “Default Call Home” service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with the Lenovo Support Center.

      You can monitor the test progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

      Note: The service forwarder must be enabled before it can be tested

- Setup Call Home for specific managed devices:
  1. From the XClarity Administrator menu bar, click **Administration → Service and Support**.
  2. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.
  3. Click the **Create Service Forwarder** icon ( ) to display the New Service Forwarder dialog.
  4. Click the **General** tab.



     a. Select **Call Home** as the service forwarder:
     b. Enter the name of the service forwarder and a description.
     c. Specify the number of automatic-notification retries. The default is 2.
     d. Specify the minimum number of minutes between retries. The default is 2.
     e. (Optional) Click **Requires Service Data Inspection** if you want to inspect the service-data files before they are transferred, and optionally specify the e-mail address of the contact to be notified when service files must be inspected.
  5. Click the **Specific** tab, and fill in the contact and system information.

     Tip: To use the same contact and location information that is configured on the Call Home Configuration page, select **General Configuration** in the **Configuration** drop-down menu.
  6. Click the **Devices** tab, and select the managed devices and resource groups for which you want this service forwarder to forward service files.

     Tip: To forward service files for all managed devices (current and future), select the **Match all devices** checkbox.

7. Click **Create**. The service forwarder is added to the Service and Support page.
8. On the Service Forwarders page, select **Enable** in the **Status** column to enable the service forwarder.
9. Select the service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with the Lenovo Support Center.

   You can monitor the test progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

   Note: The service forwarder must be enabled before it can be tested.

What to do next

From the Service and Support page, you can also perform the following actions:

- If **Requires Service Data Inspection** is selected and a serviceable event was received from one of the managed devices that is associated with the service forwarder, you must inspect service files before the files are forwarded to the service provider. For more information, see Transferring diagnostic files to Lenovo Support in the XClarity Administrator online documentation.
- Determine whether Call Home is enabled or disabled on a managed device by clicking **Device Actions** in the left navigation and verifying the state in the **Call Home Status** column.

  Tip: If “Unknown State” is displayed in the **Call Home Status** column, refresh the web browser to display the correct status.
- Define the support contact and location information for a specific managed device by clicking **Device Actions** in the left navigation, selecting the device, and then clicking the **Create Contact Profile** icon ( ) or **Edit Contact Profile** icon ( ). The contact and location information for the managed device is included in the service ticket that Call Home sends to the Lenovo Support Center. If unique contact and location information is specified for a managed device, that information is included in the service ticket. Otherwise, general information that is specified for the XClarity Administrator Call Home configuration (on the **Call Home Configuration** page or **Service Forwarders** page) is used. For more information, see Lenovo Support Center. For more information, see Defining the support contacts for a device in the XClarity Administrator online documentation.
- View service tickets that have been submitted to the Lenovo Support Center by clicking **Service Ticket Status** in the left navigation. This page lists service tickets that have been opened automatically or manually by a Call Home service forwarder, the status, and service files that were transmitted to the Lenovo Support Center. For more information, see Viewing problem records and status in the XClarity Administrator online documentation.
- Collect service data for a specific device by clicking **Device Actions** in the left navigation, selecting the device, and then clicking the **Collect Service Data** icon ( ). For more information, see Collecting and downloading diagnostic files for a device in the XClarity Administrator online documentation.
- Manually open a service ticket in the Lenovo Support Center, collect service data for a specific device, and send those files to the Lenovo Support Center by clicking **Device Actions** in the left navigation, selecting the device, and then clicking **All Actions → Perform Manual Call Home**.If the Lenovo Support Center requires additional data, the Lenovo Support might instruct you to recollect service data for that device or for another device.

  For more information, see Opening a service ticket in the XClarity Administrator online documentation.
- Re-enable Call Home on all managed devices by clicking **Device Actions** in the left navigation, and then clicking **All Actions → Enable Call Home on all devices**.

  When a Call Home service forwarder is enabled in Lenovo XClarity Administrator, Call Home is disabled on each managed device to avoid duplicate problem records from being created. If you intend to

discontinue using XClarity Administrator to manage your devices or if you intend to disable Call Home in XClarity Administrator, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time.

For more information, see Re-enabling call home on all managed devices in the XClarity Administrator online documentation.

Setting up automatic problem notification to a preferred service provider

You can configure Lenovo XClarity Administrator to automatically send diagnostic files for a specific set of managed devices to your preferred service provider (including Lenovo Support using Call Home) when certain serviceable events are received from managed devices (such as an unrecoverable memory error) so that the issue can be addressed.

Before you begin

Attention: You must accept the Lenovo Privacy Statement before you can transfer data to Lenovo Support.

Ensure that all ports that are required by XClarity Administrator (including ports that are required for call home) are available before you setup a service forwarder. For more information about ports, see Port availability in the XClarity Administrator online documentation.

Ensure that a connection exists to the Internet addresses that are required by the service provider.

If you choose to use Lenovo Support, ensure that a connection exists to the Internet addresses that are required by Call Home. For information about firewalls, see Firewalls and proxy servers in the XClarity Administrator online documentation.

If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is set up as a non-terminating proxy. For more information about setting up the proxy, see Configuring network accessConfiguring network access in the XClarity Administrator online documentation.

About this task

A *service forwarder* defines information about where to send the service data files when a serviceable event occurs. You can define up to 50 service forwarders

For each service forwarder, you can choose to automatically transfer service data to Lenovo Support (called *Call Home*), to the Lenovo Upload Facility, or to another service provider using SFTP. For information about setting up a service forwarder for Call Home, see Setting up automatic problem notification to Lenovo Support (Call Home) and Setting up automatic problem notification to a preferred service provider. For information about setting up a service forwarder for the Lenovo Upload Facility, see Setting up automatic problem notification to the Lenovo Upload Facility in the XClarity Administrator online documentation.

If a service forwarder is configured and enabled for SFTP, XClarity Administrator *automatically* transfers service files to the specified SFTP site for your preferred service provider.

Note: If multiple SFTP service forwarders are set up for the same device, only one of the service forwarders transfers service data. The address and port that is used depends on which service forwarder is triggered first.

Procedure

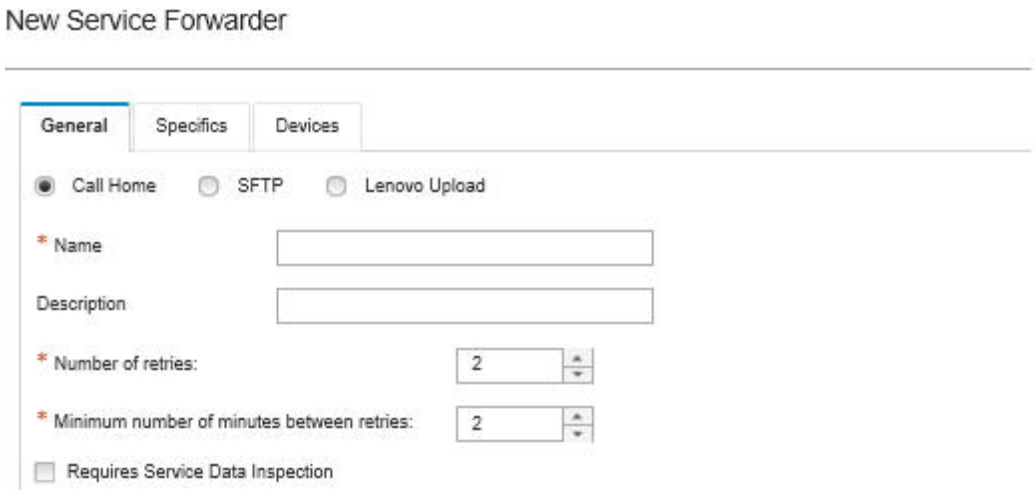
Complete the following steps to define and enable a service forwarder.

Step 1. From the XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.

Step 2. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.

Step 3. Click the **Create Service Forwarder** icon ( ) to display the New Service Forwarder dialog.

Step 4. Click the **General** tab.



1. Select **SFTP** for the service forwarder:
2. Enter the name of the service forwarder and a description.
3. Specify the number of automatic-notification retries. The default is 2.
4. Specify the minimum number of minutes between retries. The default is 2.
5. (Optional) Click **Requires Service Data Inspection** if you want to inspect the service files before they are transferred, and optionally specify the e-mail address of the contact to be notified when service files must be inspected.

Step 5. Click the **Specific** tab, and fill in the following information:
- IP address and port number of the SFTP server
- User ID and password for authentication to the SFTP server

Step 6. Click the **Device** tab, and select the managed devices and resource groups for which you want this service forwarder to forward service data.

Tip: To forward service data for all managed devices (current and future), select the **Match all devices** checkbox.

Step 7. Click **Create**. The service forwarder is added to the Service and Support page

Step 8. On the Service and Support page, select **Enable** in the **Status** column to enable the service forwarder.

Step 9. Optional: To prevent serviceable events that are in the list of excluded events from automatically opening problem reports, select **No** next to the question **Do you want excluded events to open problem reports?**.

Step 10. Select the service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with each service provider.

Note: The service forwarder must be enabled before it can be tested.

What to do next

From the Service and Support page, you can also perform the following actions:

- If **Requires Service Data Inspection** is selected and a serviceable event was received from one of the managed devices that is associated with the service forwarder, you must inspect and service files before the files are forwarded to the service provider. For more information, see Inspecting diagnostic files in the XClarity Administrator online documentation.
- Modify the service-forwarder information by clicking **Service Forwarders** in the left navigation and clicking the **Edit Service Forwarder** icon ( ).
- Enable or disable a service provider by clicking **Service Forwarders** and selecting **Enable** or **Disable** in the **Status** column.
- Delete the service provider by clicking **Service Forwarders** and clicking the **Delete Service Forwarder** icon ( ).
- Define the support contact and location information for a specific managed device by clicking **Device Actions** in the left navigation, selecting the device, and then clicking the **Create Contact Profile** icon ( ) or **Edit Contact Profile** icon ( ). The contact and location information for the managed device is included in the problem record that call home creates in the Lenovo Support Center. If unique contact and location information is specified for a managed device, that information is included in the problem record. Otherwise, general information that is specified for the XClarity Administrator call-home configuration (on the **Call Home Configuration** page or **Service Forwarders** page) is used. For more information, see Defining the support contacts for a device in the XClarity Administrator online documentation.
- Collect service data for a specific device by clicking **Device Actions**, selecting the device, and then clicking the **Collect Service Data** icon ( ). For more information, see Collecting and downloading diagnostic files for a device in the XClarity Administrator online documentation.

For more information about these service and support tasks, see Working with service and support in the XClarity Administrator online documentation.

Backing up and restoring system data and settings

You can use Lenovo XClarity Administrator to backup and restore system data and settings and imported files such as operating-system images, firmware updates, and OS device drivers.

Backing up Lenovo XClarity Administrator

If you already have backup procedures in place for virtual hosts, ensure that your procedures include Lenovo XClarity Administrator.

Before you begin

Attention: Ensure that you notify all active users before you initiate the backup procedure. XClarity Administrator is quiesced during the procedure to prevent data from being modified. Therefore, you cannot access XClarity Administrator while the backup procedure is running.

Download the Certificate Authority certificate from the XClarity Administrator virtual appliance and import the certificate into your web browser (see Importing the Certificate Authority certificate into a web browser).

Ensure that all running jobs are complete and that there are no pending jobs. If jobs are running, you can choose to stop the running jobs and continue creating the backup.

Ensure that the DNS servers are set up correctly; otherwise SMTP and NTP might not work correctly after the backup is restored.

Ensure that there is enough disk space available in the management server for the backup. If not, free up disk space by deleting XClarity Administrator resources, including previous backups, that are no longer needed

(see Managing disk space) or choose to create a new backup without including operating-system images, firmware updates, and OS device drivers.

About this task

Always back up XClarity Administrator after performing the initial setup and after making significant configuration changes, including:

- Before you update XClarity Administrator
- When you manage new chassis or rack servers
- When you add users to XClarity Administrator
- When you create and deploy new Configuration Patterns

Ensure that you back up XClarity Administrator on a regular basis.

It is recommended that you download backups to your local system. If the host operating system shuts down unexpectedly, you might not be able to authenticate with XClarity Administrator after the host operating system is restarted. To resolve this problem, restore XClarity Administrator from the last backup on your local system (see Restoring Lenovo XClarity Administrator.).

Procedure

Complete the following steps to back up XClarity Administrator.

Step 1. From the XClarity Administrator menu bar, click **Administration → Back Up and Restore Data**. The Back Up and Restore Data page is displayed.

Step 2. Click the **Back Up** icon (). The Back Up Data and Settings dialog is displayed.

Step 3. Enter a description for this backup.

Step 4. Choose the location where you want to create the backup. This can be the local repository or a remote share.

The backup is created in the local repository by default. You can copy a backup from the local repository to a remote share by clicking the **Copy Backup** icon ().

If you choose a remote share, the backup is first created in the local repository. Then, the backup is copied to the selected remote share, and the local copy is deleted. For more information, see Managing remote shares.

Step 5. Optionally select to include operating-system images, firmware updates, and OS device drivers.

Step 6. Specify the encryption passphrase for the backup.

Attention: Record the encryption passphrase. The passphrase is needed to restore the backup to this or another XClarity Administrator instance. If you forget the passphrase, there is no way to recover it.

Step 7. Click **Back Up** to backup data and settings immediately, or click **Schedule** to schedule this backup to run at a later time.

Attention: If you choose to back up immediately, do not close or refresh the web browser tab or window before the process completes. Otherwise, the backup might not be generated.

Generating the backup might take a while. A progress bar shows the status of the job.

If you chose to create the backup on a remote share, you can monitor progress from the Jobs page (see Monitoring jobs).

If you schedule a backup, the management server is shut down temporarily during the backup process. After the management server comes back online, you can monitor the status of the backup process from the Jobs page.

Step 8. Log in to the XClarity Administrator to continue managing your devices.

What to do next

From the Back Up and Restore Data page, you can perform the following actions:

- Copy XClarity Administrator backups to or from a remote share clicking the **Copy Backup** icon ( ).
- Delete selected backups from the local repository or remote shares that are no longer needed by clicking the **Delete Backup** icon ( ).
- Restore system data and settings to this management server (see Restoring Lenovo XClarity Administrator).
- Import or export backups from the local system by clicking the **Import Backup** icon ( ) or **Export Backup** icon ( ), respectively.
- Push the selected backup to a new XClarity Administrator instance (see Migrating data and settings to another Lenovo XClarity Administrator instance).

Restoring Lenovo XClarity Administrator

You can use backed up data and settings to restore Lenovo XClarity Administrator to a previous state.

Before you begin

Attention: Ensure that you notify all active users before you initiate the backup procedure. XClarity Administrator is quiesced during the procedure to prevent data from being modified. Therefore, you cannot access XClarity Administrator while the backup procedure is running

Download the Certificate Authority certificate from the XClarity Administrator virtual appliance and import the certificate into your web browser (see Importing the Certificate Authority certificate into a web browser).

Ensure that all running jobs are complete and that there are no pending jobs.

About this task

Attention:

- All changes since when the backup was created will be lost.
- To restore data, the virtual appliance is reset to its original clean state. All current settings, device inventory and files (operating-system images, firmware updates, and OS device drivers) are deleted before restoring data in the backup. Data and settings in the backup are not mixed with the virtual appliance's current data and settings. If you choose not to restore device inventory, operating-system images, firmware updates, and OS device drivers, only the default XClarity Administrator data is present after the restore operation completes.

Restoring a backup does not delete backups in the XClarity Administrator instance.

Restoring a backup does not change data or settings on the managed devices. For example, if you unmanage a device and then restore a previous backup when the device was still managed on XClarity Administrator, you might have connectivity issues with that device after the restore operation is complete. Likewise, if you manage a device and then restore a previous backup when the device was still unmanaged,

you might need to manually modify the device's configuration to undo its managed status or use the **Force** option when trying to manage it in XClarity Administrator again.

You can restore a backup only in the same XClarity Administrator version that was used to create the backup.

Procedure

Complete the following steps to restore XClarity Administrator.

Step 1. From the XClarity Administrator menu bar, click **Administration → Back Up and Restore Data**. The Back Up and Restore Data page is displayed.

Step 2. If you exported the backup package to your local system and deleted it from XClarity Administrator, complete the following steps.

a. From the Backup and Restore Data page, click the **Import Backup** icon ( ) to display the Import Backup dialog.

b. Click **Browse** to find the backup that you exported from a XClarity Administrator instance.

c. Click **Import** to upload the backup to the XClarity Administrator.

Importing the backup might take a while. A progress bar shows the status of the job.

Attention: If you close or refresh the web browser tab or window before the upload completes, the process might fail.

d. When the import is complete, specify the encryption passphrase for the backup.

Note: If you do not have the encryption passphrase, you will need to create a new backup in XClarity Administrator (see Backing up Lenovo XClarity Administrator).

Step 3. Select the backup to restore, and click the **Restore Backup** icon ( ). The Restore Data dialog is displayed.

Step 4. Specify the encryption passphrase for the backup.

Step 5. Click **Confirm**.

Step 6. In the Confirm Data Restore dialog, verify that the information in the dialog is correct.

Step 7. In the Restore Options dialog, optionally choose to import operating-system images, firmware updates, OS device drivers, network settings, and device inventory.

Attention: Ensure that you carefully read all warning that are displayed in this dialog.

Step 8. Click **Confirm** to begin data restore.

Restoring the data and settings might take a while. A progress bar shows the status of the job.

When the restore process is complete, you are redirected to the login page.

Attention: If you close or refresh the web browser tab or window before the process completes, process might fail.

Step 9. Log in to the XClarity Administrator to continue managing your devices.

Migrating data and settings to another Lenovo XClarity Administrator instance

You can migrate the backed up system data and settings to a new Lenovo XClarity Administrator that is in the same or different network.

Before you begin

Attention: Ensure that you notify all active users before you initiate the backup procedure. XClarity Administrator is quiesced during the procedure to prevent data from being modified. Therefore, you cannot access XClarity Administrator while the backup procedure is running

Download the Certificate Authority certificate from the XClarity Administrator virtual appliance and import the certificate into your web browser (see Managing disk space in the XClarity Administrator online documentation).

Ensure that all running jobs are complete and that there are no pending jobs.

Backups in the source management server backup repository are not migrated to the target management server. Before migrating data and settings, export any backups you might need to your local system.

About this task

Attention: The target management server must be a new XClarity Administrator virtual appliance with the same version as the source management server and must be in the Initial Setup wizard, with no steps completed.

Any changes to the source management server after the backup was created is not migrated to the target management server.

Restoring a backup does not change data or settings on the managed devices. For example, if you unmanage a device and then restore a previous backup when the device was still managed on XClarity Administrator, you might have connectivity issues with that device after the restore operation is complete. Likewise, if you manage a device and then restore a previous backup when the device was still unmanaged, you might need to manually modify the device's configuration to undo its managed status or use the **Force** option when trying to manage it in XClarity Administrator again.

You can restore a backup only in the same XClarity Administrator version that was used to create the backup. Install a new XClarity Administrator virtual appliance of the same version as the one you used to create your backup data package. Instructions vary based on the type of hypervisor and network setup in your environment. For more information, see Installing and setting up XClarity Administrator in the XClarity Administrator online documentation.

Procedure

Complete the following steps to restore XClarity Administrator.

Step 1. If the source and target XClarity Administrator are in the same network, complete the following steps.

a. From the XClarity Administrator menu bar, click **Administration → Back Up and Restore Data**. The Back Up and Restore Data page is displayed.

b. Click the **Push Backup** icon () to display the Push Data dialog.

c. Specify the current IP address of the target XClarity Administrator.

d. Click **Continue** to upload the backup to the target XClarity Administrator.

Uploading the backup might take a while. A progress bar shows the status of the job.

Attention: If you close or refresh the web browser tab or window before the upload completes, the package might not be uploaded.

Step 2. If the source and target XClarity Administrator *are not* in the same network, complete the following steps

a. From the source XClarity Administrator menu bar, click **Administration → Back Up and Restore Data**. From the Back Up and Restore Data page, click the **Export Backup** icon ( ) to export the backup to the local system.

   Exporting the backup might take a while.

b. Copy the exported backup from the source management server to a system in the same network as the target management server

c. From the Wizard page on the target XClarity Administrator, click the **Import Backup** icon ( ) to display the Import Data Package dialog.

d. Click **Browse** to find the backup that you exported from the source XClarity Administrator.

e. Click **Upload** to import the backup to the target XClarity Administrator.

   Importing the backup might take a while. A progress bar shows the status of the job.

   Attention: If you close or refresh the web browser tab or window before the upload completes, the process might fail.

Step 3. When the import is complete, specify the encryption passphrase for the backup.

Note: If you do not have the encryption passphrase, you will need to create a new backup in the source XClarity Administrator (see Backing up Lenovo XClarity Administrator.

Step 4. In the Confirm Data Restore dialog, verify that all information is correct.

Step 5. Click **Confirm** to begin loading system data and settings.

Step 6. In the Restore Options dialog, optionally choose to import operating-system images, firmware updates, OS device drivers, network settings, and device inventory.

Attention: Ensure that you carefully read all warning that are displayed in this dialog.

Step 7. If you chose to import network settings or device inventory, shut down the source management server from the source XClarity Administrator by clicking **Administration → Shutdown Management Server → Shutdown**.

Confirm that the source virtual appliance has shut down before continuing

Step 8. On the target XClarity Administrator, click **Confirm** to begin loading data and settings from the package

If you chose to import network settings, after migration is complete the IP addresses from the source XClarity Administrator are reassigned to the target XClarity Administrator.

Attention: If the source XClarity Administrator uses DHCP, you must bind the target XClarity Administrator MAC addresses to the corresponding source XClarity Administrator IP addresses on the DHCP server. Wait at least 15 minutes after the DHCP server is modified before continuing.

Step 9. Wait for the Load Data and Settings from Package progress bar to complete.

When the data-migration process is complete, you are redirected to the login page.

Attention: If you close or refresh the web browser tab or window before the upload completes, the process might fail.

Step 10. Log in to the target XClarity Administrator to continue managing your devices.

Managing disk space

You can manage the amount of disk space that is used by Lenovo XClarity Administrator by moving large data files that are not immediately needed to a remote share or by deleting resources that are no longer needed.

About this task

To determine how much disk space is currently being used, click **Dashboard** from the XClarity Administrator menu bar. The disk space usage on the repository and remote shares is listed in the XClarity Administrator Activity section.

Procedure

Complete one or more of the following steps to free up disk space by moving backup to a remote share and delete unneeded resources.

- **Delete unneeded resources**

  You can quickly delete files from the local repository that are no longer needed by completing the following steps.

  1. From the XClarity Administrator menu bar, click **Administration → Disk Cleanup** to display the Disk Cleanup page.
  2. Select the files that you want delete. The section header identifies the amount of space that will be freed when the files are deleted.
     - **Operating system related files**

       You can delete OS Images, boot-option files, and software files.
     - **Firmware updates**

       You can delete payload files for all OS device drivers that are associated with UpdateXpress System Packs (UXSPs) and individual device drivers that are in the Downloaded state.

       You can delete payload files for individual firmware updates that are in the Downloaded state and are not used in a firmware-compliance policy.

       You can delete payload files for management-server updates that are in the Downloaded state.
     - **Service data files**

       When service event occurs on a device, service data is collected automatically for that device. Service data is automatically captured for the management server every time an exception occurs in the XClarity Administrator. It is recommended that you periodically delete these archives if XClarity Administrator and the managed devices are running without issues.

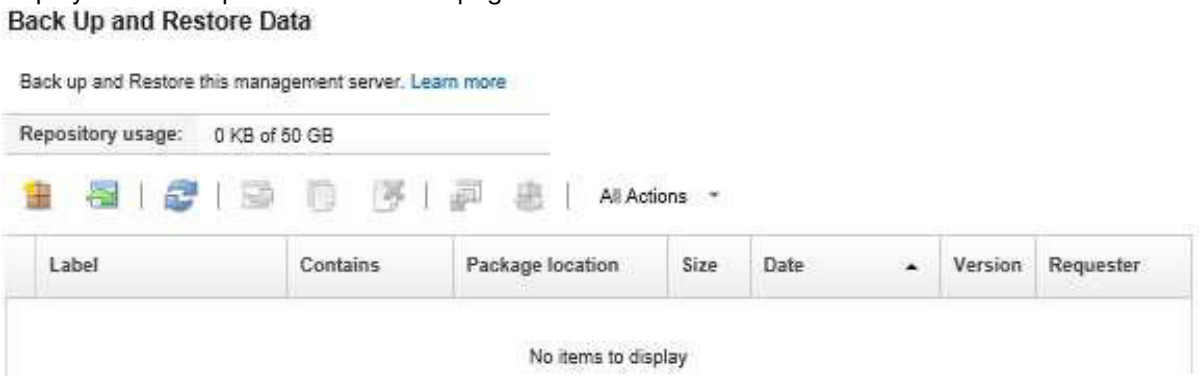
       When management-server updates are successfully applied, the update files are automatically removed from the repository.
  3. Click **Delete Selected**.
  4. Review the list of files that you selected, and click **Delete**.

- **Move XClarity Administrator backups to a remote share**

  You can free up disk space that is available to the XClarity Administrator local repository by moving XClarity Administrator backups to a remote share. However, you cannot use the files directly on the remote share. To use the files, you must move them back to the XClarity Administrator local repository. For more information about remote shares, see Managing remote shares.

Important: It is recommended that you download backups to your local system or copy backups to a remote share before deleting the backups in XClarity Administrator.

1. From the XClarity Administrator menu bar, click **Administration → Back Up and Restore Data** to display the Back Up and Restore Data page.



   The **Package location** column identifies whether the backup is stored, either locally in the XClarity Administrator local repository or on a remote share.

2. Select the backup, and click the **Copy Backup** icon ( ) to displays the Copy Backup dialog.
3. Choose the remote share to store the backup.
4. Click **Copy**.
5. Monitor the copy progress on the Jobs page. When the copy is complete, select the backup again, and click the **Delete Backup** icon ( ) to display the Delete Backup dialog.
6. Select “Local” for the location.
7. Click **Delete**.

Managing remote shares

You can mount remote shares over SSH File System (SSHFS). You then can move Lenovo XClarity Administrator backups from the XClarity Administrator local repository to the remote shares to manage disk space that is available to XClarity Administrator.

Before you begin

You must have **lxc-supervisor** authority to mount or unmount a remote share.

When using SSH public key authentication to mount a remote share, you must import the SSH public key for the remote server to XClarity Administrator.

About this task

Note: You cannot use the files directly on a remote share. To use the files, you must move them back to the XClarity Administrator local repository.

Currently, only SSHFS is supported.

Procedure

To add a remote share, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Remote Share**. The Remote Share page is displayed.

Step 2. Click the **Create** () icon to create a remote share. The Create Remote Share dialog is displayed.

Step 3. Specify the IP address of the remote server that hosts the remote share.

Step 4. Specify the stored credential to use to access the remote share.

Tip: To create a stored credential, see Managing stored credentials.

Step 5. Specify the mount point (local directory) on the management server to use for mounting the remote share.

Important: The path must start with "/mnt".

Step 6. Specify the shared directory (remote server path) to mount as the remote share on the management server.

Step 7. If authentication is required, enable **SSH Key Authentication**.

Step 8. Click **Create**.

Step 9. If you chose to use SSH key authentication, select the remote share from the Remote Share page, and click the **Import** () icon to import the SSH public key from the server that hosts the shared directory to XClarity Administrator.

Notes:

- If the SSH public key already exists, regenerating the key might cause you to lose connectivity to the existing remote share.
- You must have **lxc-supervisor** authority to regenerate an SSH key.

Step 10. From the Remote Share page, click the **Test** () icon to verify the connection to the remote share.

What to do next

- Unmount the remote share by selecting the remote share and clicking the **Delete** () icon.
- Move files to and from a remote share (see Managing disk space).

Changing the language of the user interface

You can change the language of the user interface after you are logged in.

Procedure

From the Lenovo XClarity Administrator title bar, click the user-actions menu (

), and then click **Change language**. Select the language that you want to display, and then click **Close**.

Note: The help system displays in the same language that is set for the user interface.

Shutting down Lenovo XClarity Administrator

When Lenovo XClarity Administrator shuts down, connectivity to Lenovo XClarity Administrator is lost.

Before you begin

Ensure that no jobs are currently running. Any jobs that are currently running are canceled during the shutdown process. To view the jobs log, see Monitoring jobs.

Procedure

Complete the following steps to shut down Lenovo XClarity Administrator.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Shut Down Management Server**.

A confirmation dialog is displayed with a list of jobs that are currently running. When you shut down Lenovo XClarity Administrator, the jobs are canceled.

Step 2. Click **Shut down**.

What to do next

To restart Lenovo XClarity Administrator after a shutdown, see Restarting Lenovo XClarity Administrator.

Restarting Lenovo XClarity Administrator

You can restart Lenovo XClarity Administrator from the web interface or from the hypervisor after a shutdown.

Before you begin

Ensure that no jobs are currently running. Any jobs that are currently running are canceled during the restart process. To view the jobs log, see Monitoring jobs.

About this task

There are certain situations when you are required to restart Lenovo XClarity Administrator:
- When regenerating a server certificate
- When uploading a new server certificate

Procedure

Complete the following steps to restart Lenovo XClarity Administrator.

- Restart Lenovo XClarity Administrator from the web interface:
  1. From the Lenovo XClarity Administrator menu bar, click **Administration → Shut Down Management Server**.

     A confirmation dialog is displayed with a list of jobs that are currently running. When you restart Lenovo XClarity Administrator, the jobs are canceled.
  2. Click **Restart**.

     When Lenovo XClarity Administrator shuts down, connectivity to Lenovo XClarity Administrator is lost.
  3. Wait a few minutes for Lenovo XClarity Administrator to restart, and then log in again.
- Restart Lenovo XClarity Administrator from the hypervisor after a shutdown:
  - Microsoft Hyper-V
    1. From the Server Manager Dashboard, click **Hyper-V**.
    2. Right-click the server, and click **Hyper-V Manager**.
    3. Right-click the virtual machine, and click **Start**. When the virtual machine is started, the IPv4 and IPv6 addresses are listed for each interface, as shown in the following example.

       The XClarity Administrator eth0 management port uses a DHCP IP address by default. At the end of the XClarity Administrator boot process, you can choose to set a static IP address for the eth0 management port by entering 1 when prompted, as shown in the example below. The prompt is

available for 150 seconds, until the login prompt is displayed. To proceed to the login prompt without delay, enter x at the prompt.

Important:

- When changing the static IP address settings, you have a maximum of 60 seconds to enter the new settings. Ensure that you have the required IP information before continuing.
  - For IPv4 settings, you must have the IP address, subnet mask, and gateway IP address
  - For IPv6 settings, you must have the IP address and prefix length
- If you are not using a DHCP server, you can use a configuration file to specify the IP settings for the XClarity Administrator eth0 management port. that you want to use to access the XClarity Administrator. For more information, see the "What to do next" section below.
- If you change the IP address settings from the console, XClarity Administrator is restarted to apply the new settings.
- No action is required to log in. Ignore the console login message. The console interface is not for customer use.
- You might see the message `TCP: eth0: Driver has suspect GRO implementation, TCP performance may be compromised` on the console. The performance of the virtual machine is not impacted, and you can ignore this warning.

Attention: Changing the IP address of the XClarity Administrator management port after managing devices might cause the devices to be placed in offline state in XClarity Administrator. If you choose to change the IP address after XClarity Administrator is up and running, ensure that all devices are unmanaged before changing the IP address.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0     Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56
         inet addr: 192.0.2.10  Bcast 192.0.2.55  Mask 255.255.255.0
         inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link

eth1     Link encap:Ethernet  HWaddr 2001:db8:64:23:45:67
         inet addr: 192.0.2.20  Bcast 192.0.2.130 Mask 255.255.255.0
         inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  ... ...
```

4. Log in to Lenovo XClarity Administrator (see Logging in to Lenovo XClarity Administrator).

– VMware ESXi

1. Connect to the host through VMware vSphere Client.
2. Right-click the virtual machine, and click **Power → Power on**.
3. Click the **Console** tab. When the virtual machine is started, the IPv4 and IPv6 addresses are listed for each interface, as shown in the following example.

   The XClarity Administrator eth0 management port uses a DHCP IP address by default. At the end of the XClarity Administrator boot process, you can choose to set a static IP address for the eth0 management port by entering 1 when prompted, as shown in the example below. The prompt is available for 150 seconds, until the login prompt is displayed. To proceed to the login prompt without delay, enter x at the prompt.

Important:

- When changing the static IP address settings, you have a maximum of 60 seconds to enter the new settings. Ensure that you have the required IP information before continuing.
  - For IPv4 settings, you must have the IP address, subnet mask, and gateway IP address
  - For IPv6 settings, you must have the IP address and prefix length
- If you are not using a DHCP server, you can use a configuration file to specify the IP settings for the XClarity Administrator eth0 management port. that you want to use to access the XClarity Administrator. For more information, see the “What to do next” section below.
- If you change the IP address settings from the console, XClarity Administrator is restarted to apply the new settings.
- No action is required to log in. Ignore the console login message. The console interface is not for customer use.
- You might see the message `TCP: eth0: Driver has suspect GRO implementation, TCP performance may be compromised` on the console. The performance of the virtual machine is not impacted, and you can ignore this warning.

Attention: Changing the IP address of the XClarity Administrator management port after managing devices might cause the devices to be placed in offline state in XClarity Administrator. If you choose to change the IP address after XClarity Administrator is up and running, ensure that all devices are unmanaged before changing the IP address.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0     Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56
         inet addr: 192.0.2.10  Bcast 192.0.2.55  Mask 255.255.255.0
         inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link

eth1     Link encap:Ethernet  HWaddr 2001:db8:64:23:45:67
         inet addr: 192.0.2.20  Bcast 192.0.2.130 Mask 255.255.255.0
         inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

4. Log in to Lenovo XClarity Administrator (see Logging in to Lenovo XClarity Administrator).

What to do next

When Lenovo XClarity Administrator restarts, it recollects inventory for each managed device. Wait approximately 30-45 minutes, depending upon the number of managed devices, before attempting firmware updates, configuration pattern deployments, or operating-system deployments.

Chapter 3. Monitoring devices and activities

You can monitor your devices and activities though the dashboard, alerts and audit logs, and jobs logs.

Viewing a summary of your environment

The Dashboard displays the status of all managed devices, an overview of all provisioning-related tasks, an information about Lenovo XClarity Administrator resources and activities.

Learn more:  XClarity Administrator: Monitoring

Procedure

Step 1. From the XClarity Administrator menu bar, click **Dashboard**.

© Copyright Lenovo 2015, 2021



Step 2. Expand the hardware status, provisioning status, or the administrator activity section to obtain more information about each of these areas.

Viewing a summary of your hardware status

The Hardware Status area displays the status of all managed devices.

Procedure

To obtain more information about all of the devices of that type, click the number listed under the device type.

To view more information about only those devices of that type and status, click the icon or number beside each status icon.

- **Servers**. Displays the total number of servers (compute nodes, rack servers, and tower servers) that XClarity Administrator manages, and the number of servers with normal, warning, and critical status. For more information, see Viewing the status of a managed server.
- **Storage**. Displays the total number of storage devices that XClarity Administrator manages, and the number of storage devices with normal, warning, and critical status. For more information, see Viewing the status of storage devices.
- **Switches**. Displays the total number of RackSwitch and Flex System switches that XClarity Administrator manages, and the number of switches with normal, warning, and critical status. For more information, see Viewing the status of switches
- **Chassis**. Displays the total number of Flex chassis that XClarity Administrator manages, and the number of Flex chassis with normal, warning, and critical status. For more information, see Viewing the status of a managed chassis.
- **Racks**. Displays the number of racks that are created in XClarity Administrator, and the number of racks with devices that have the normal, warning, and critical as their highest status. For more information, see Viewing the status of devices in a rack.
- **Resource groups**. Displays the number of resource groups that XClarity Administrator manages and the number of resource groups with devices that have the normal, warning, and critical as their highest status. For more information, see Viewing the status of devices in a resource group.

To customize the hardware resources that are displayed on the dashboard, click the **Customize** icon ( ). You can choose the device types that you want to show or hide. You can also choose whether to aggregate servers into a single summary, display separate summaries for each type of server (rack and tower, Flex System, ThinkServer, and NeXtScale servers), or omit specific types of servers.



Viewing a summary of your provisioning status

The Provisioning Status area provides a summary of all tasks that are associated with provisioning devices.

Procedure

- **Configuration Patterns**. Displays details about the number of servers that have profiles, including the following statistics.

  Note: When the management server is not license compliant, all values are 0 (see Installing the full-function enablement license in the XClarity Administrator online documentation).

- The number of servers that are compliant with their server profile. You can click the number to display the Configuration Patterns: Server Profiles page with a list of compliant servers.
- The number of servers that are not compliant with their server profile. You can click the number to display the Configuration Patterns: Server Profiles page with a list of non-compliant servers.
- The number of devices for which compliance status is unknown. You can click the number to display the Configuration Patterns: Server Profiles page with a list of servers with unknown compliance.

  Note: Compliance status is unknown, typically after a partial profile deployment, when Lenovo XClarity Administrator did not collect the configuration information from the sever. Refresh the server inventory or revisit the server-profile details page to force collecting configuration information from server.
- The number of servers that are assigned a server profile. You can click the number to display the Configuration Patterns: Server Profiles page with a list of servers with profiles.
- The number of servers that are not assigned a server profile. You can click the number to display the Configuration Patterns: Server Patterns page with a list of server patterns that can be deployed to servers without profiles.
- The number of server patterns that are currently being deployed.

To view trending data for configuration patterns, click **View Trending Data** (see Monitoring trends in provisioning status).

For more information about configuration patterns and server profiles, see Configuring servers using configuration patterns.

- **Operating System Images**. Displays details about operating-system deployments, including the following statistics.

  Note: When the management server is not license compliant, all values are 0 (see Installing the full-function enablement license in the XClarity Administrator online documentation).

  - The number of OS images in the repository. You can click the number to display the Deploy Operating Systems: Manage OS Images page with a list of operating systems.
  - The number of current OS deployments that are in progress. You can click the number to display the Deploy Operating Systems: Deploy OS Images page with a list devices for which an operating system is being installed.
- **Firmware Updates**. Displays details about firmware updates, including the following statistics.
  - The number of devices that are compliant. You can click the number to display the Firmware Updates: Apply / Activate page with a list of compliance devices.
  - The number of devices that are not compliant. You can click the number to display the Firmware Updates: Apply / Activate page with a list of non-compliance devices.
  - The number of devices that do not have an assigned firmware-compliance policy. You can click the number to display the Firmware Updates: Apply / Activate page with a list of devices without a compliance policy.

    From this page, you can assign each device a firmware-compliance policy by selecting a policy from the **Assigned Compliance Policy** column.
  - The number of devices for which updates are not supported. You can click the number to display the Firmware Updates: Apply / Activate page with a list of devices for which updates are not supported.
  - The number of updates that are in progress.
  - The number of devices with pending firmware. You can click the number to display the Firmware Updates: Apply / Activate page with a list of devices for which updates are pending activation.

  To view trending data for firmware updates, click **View Trending Data** (see Monitoring trends in provisioning status).

For more information about firmware updates and compliance policies, see Updating firmware on managed devices.

Viewing a summary of Lenovo XClarity Administrator activity

The XClarity Administrator Activity area displays information about active jobs, active sessions, and system resources in XClarity Administrator.

Procedure

- **Jobs**. Displays the number of active jobs that are currently in progress. For more information about jobs, see Monitoring jobs.
- **Active Sessions**. Displays the user ID and IP address for each active XClarity Administrator session. For more information about users, see Managing user accounts.
- **Resource Usage**. Displays the processor usage, memory usage, and disk capacity on the host system and remote files shares. For more information about system resources, see Monitoring system resources.

Monitoring system resources

You can determine the processor usage, memory usage, and disk capacity on the host system from the Dashboard page.

Before you begin

The following *minimum requirements* must be met for the virtual machine. Depending on the size of your environment and your use of Configuration Patterns, additional resources might be required for optimal performance.

- Two virtual microprocessors
- 8 GB of memory
- 192 GB of storage for use by the XClarity Administrator virtual appliance.
- Display with a minimum resolution of 1024 pixels in width (XGA)

The following table lists the minimum recommended virtual-machine configurations for a given number of devices. Keep in mind that if you run the minimum configuration, you might experience longer than expected completion times for management tasks. For provisioning tasks such as operating system deployment, firmware updates, and server configuration, you might need to increase the VM resources temporarily.

Number of Managed Devices	Virtual CPU/Memory Configuration
0 - 100 devices	2 vCPUs, 8 GB RAM
100 - 200 devices	4 vCPUs, 10 GB RAM
200 - 400 devices	6 vCPUs, 12 GB RAM
400 - 600 devices	8 vCPUs, 16 GB RAM
600 - 800 devices	10 vCPUs, 20 GB RAM
800 – 1,000 devices	12 vCPUs, 24 GB RAM

Notes:

- A single XClarity Administrator instance can support a maximum of 1,000 devices.
- For the latest recommendations and additional performance considerations, see the XClarity Administrator: Performance Guide (White paper).

- Depending on the size of your managed environment and the pattern of use in your installation, you might need to add resources to maintain acceptable performance. If you frequently see processor usage in the system resources dashboard displaying high or very high values, consider adding 1-2 virtual processor cores. If your memory usage persists above 80% at idle, consider adding 1-2 GB of RAM. If your system is responsive at a configuration as defined in the table, consider running the VM for a longer period to assess system performance.
- For information about how to free up disk space by deleting XClarity Administrator resources that are no longer needed, see Managing disk space.

Procedure

From the Lenovo XClarity Administrator menu bar, click **Dashboard**.



The host-system resource usage is listed in the XClarity Administrator Activity section.

Processor

The usage measurement indicates the number of XClarity Administrator processes that are simultaneously accessing the processors on the host.

Tip: The usage measure might occasionally spike to High or Very High. If the usage remains at these level for more than 30 minutes, check the jobs log to see if long running jobs are in progress (see Monitoring jobs).

The total-capacity measurement indicates the number of processors that are available on the host.

Memory

The usage measurement indicates the amount of memory that is currently in use by XClarity Administrator.

The total-capacity measurement indicates the total amount of available memory on the host.

User Data

The usage measurement indicates the amount of disk space that is currently in use by XClarity Administrator on the host system.

The total-capacity measurement indicates the total amount of space (used and unused) that is allocated for user data, such as operating systems and firmware updates.

For more information about managing disk space, see Managing disk space.

Attention: If the allocated resources are insufficient to handle the current number of managed devices with good performance, consider increasing the resource allocation. For information about recommended

hardware requirements based on the number of managed devices in your environment, see Supported host systems in the XClarity Administrator online documentation.

Monitoring trends in provisioning status

Lenovo XClarity Administrator regularly collects provisioning status, including compliance and active jobs for firmware updates and configuration patterns, for all managed devices so that you can monitor trends over a period of time.

About this task

You must have **lxc_admin** or **lxc-supervisor** authority to view trend data.

The following data is collected:

- **Firmware updates**
  - **Devices compliant**. Number of devices that are compliant with their assigned firmware-compliance policy
  - **Devices non-compliant**. Number of devices that are not compliant with their assigned firmware-compliance policy
  - **Devices without policies**. Number of devices that do not have an assigned firmware-compliance policy
  - **Devices not supported for updates**. Number of devices for which firmware updates are not supported
  - **Updates in progress**. Number of devices for which firmware updates are in progress
- **Configuration patterns**
  - **Servers with profiles**. Number of devices that have an assigned server profile
  - **Servers without profiles**. Number of devices that do not have an assigned server profile
  - **Servers compliant**. Number of devices that are compliant with their assigned server profile
  - **Servers non-compliant**. Number of devices that are not compliant with their assigned server profile
  - **Server patterns in progress**. Number of devices for which configuration-pattern updates are in progress

Procedure

Complete the following steps to view trends in provisioning status.

Step 1. From the XClarity Administrator menu bar, click **Dashboard** to display the Dashboard page.

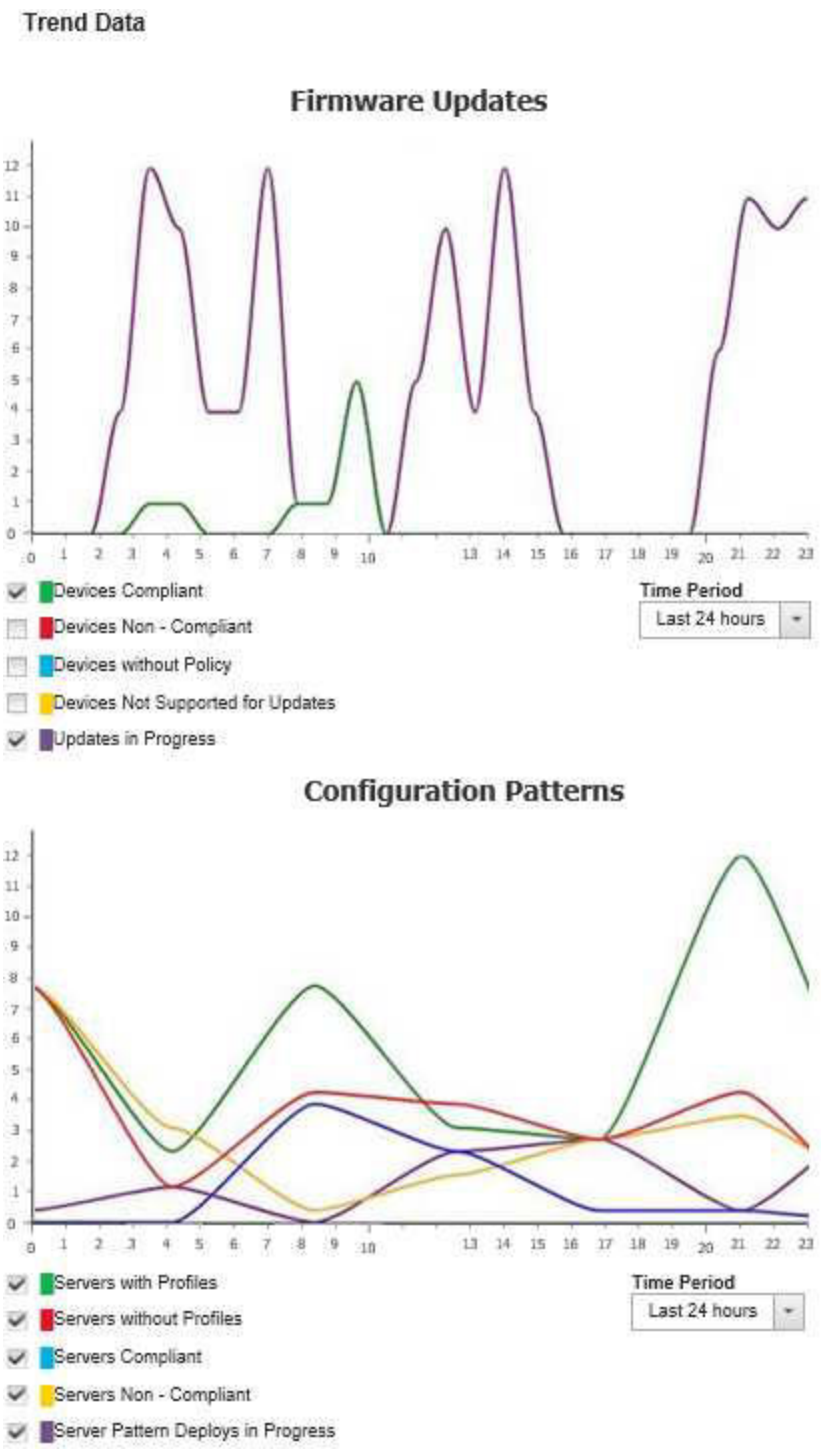
Step 2. Click the **Trending Data** link to display the Threshold Settings dialog.

Step 3. Clear or select the data that you want to view.

Step 4. Select the time period that you want to view.

- **24 hours**. Displays data for the last 24 hours. Each data point is an average over a 1-hour period.
- **1 month**. Displays data for the last 30 days. Each data point is an average over a 24-hour period.

The trend data is shown as a graph over the selected time period.



Placing devices in maintenance mode

When a device is in maintenance mode, Lenovo XClarity Administrator excludes all events and alerts for that device from all pages on which events and alerts are displayed. Excluded alerts are still logged but are hidden from view.

About this task

Only events and alerts that were generated for a device while the device is in maintenance mode are excluded. Events and alerts were generated before the device was placed in maintenance mode are displayed.

Placing a managed device in maintenance and then back in service might cause inventory for that device to be out of date. If you see abnormalities, manually refresh the inventory from the device page by selecting the device and clicking **All Actions → Inventory → Refresh Inventory**.

Procedure

Complete one of the following steps to place devices in maintenance mode.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.

Step 2. Click **Endpoint Actions** in the left navigation to display the Endpoint Actions page.

Step 3. Select one or more devices to place in maintenance mode.

Step 4. Click **Actions → Maintenance** to display the Maintenance mode dialog.

Step 5. Select the date and time for taking the device out of maintenance mode and placing back in service.

Select **Indefinitely** if you do not want the device placed back in service.

Step 6. Click **Confirm**. The maintenance column in the table changes to Yes for that device.

What to do next

When you are done with maintenance on the device, you can put the device back in service by selecting the device and clicking **Actions → Maintenance**, and then clicking **Turn off maintenance** in the dialog. If you do not manually place the device back in service mode, it is placed in service mode automatically after the specified end date and time expires.

Working with alerts

Alerts are hardware or management conditions that require investigation and user action. Lenovo XClarity Administrator polls the managed devices asynchronously and displays alerts that are received from those devices.

Learn more: XClarity Administrator: Monitoring

About this task

Typically, when an alert is received, a corresponding event is stored in the event log. It is possible to have an alert without a corresponding event in the event log (even if the log wraps). For example, events that occur before you manage a chassis are not displayed in the event log. However, the alerts for the chassis are displayed in the alert log because Lenovo XClarity Administrator polls the CMM after the chassis has been managed.

Viewing active alerts

You can view a list of all active hardware and management alerts.

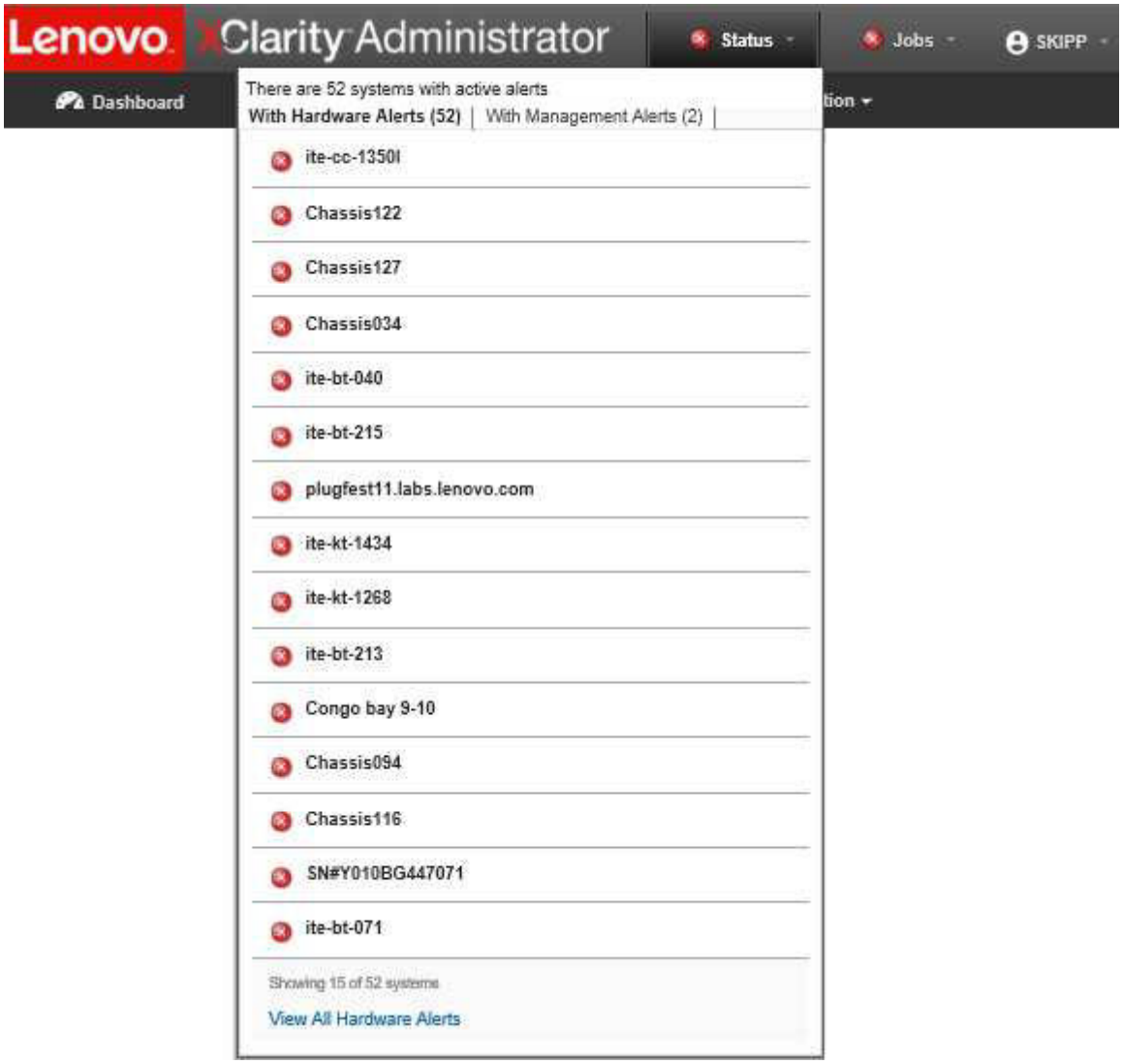
About this task

Note: Alerts for Lenovo Storage devices are presented only in English, even when the locale for Lenovo XClarity Administrator is set to another language. Use an external translation system to translate the messages manually, if needed.

Procedure

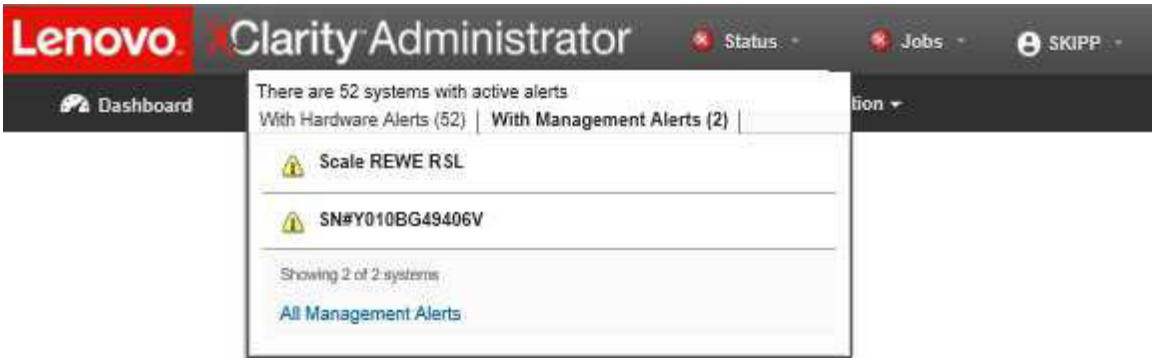
Complete one of these procedures to view the active alerts.

- To view only alerts for managed devices (known as *hardware alerts*):
  1. From the Lenovo XClarity Administrator title bar, click the **Status** pull-down to display a summary of hardware and management alerts.
  2. Click the **With Hardware Alerts** tab to see a summary of alerts for each managed device.



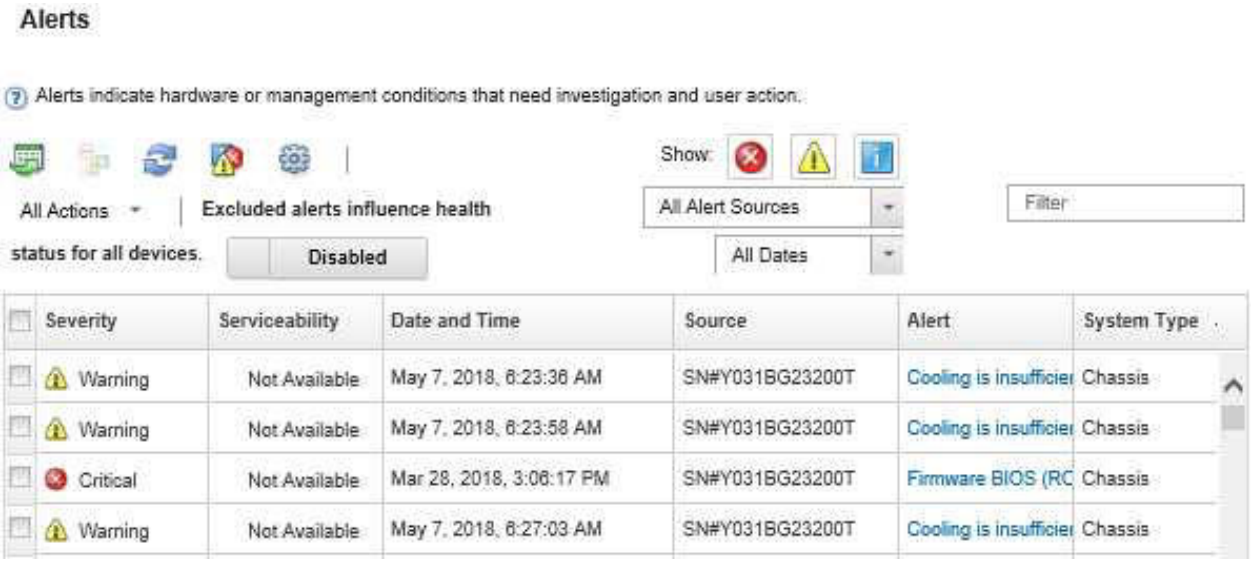
  3. Hover the cursor over a device that is listed under that tab to display a list of alerts for that device.
  4. Click the **All Hardware Alerts** link to display the Alerts page with a filtered list of all hardware alerts.
- To view only alerts from Lenovo XClarity Administrator (known as *management alerts*):
  1. From the Lenovo XClarity Administrator title bar, click the **Status** pull-down to display a summary of hardware and management alerts.

2. Click the **With Management Alerts** tab to see a summary of all CMM and Lenovo XClarity Administrator alerts.



3. Hover the cursor over a device that is listed under that tab to display a list of alerts for that device.
4. Click the **All Management Alerts** link to display the Alerts page with a filtered list of all CMM and Lenovo XClarity Administrator alerts.

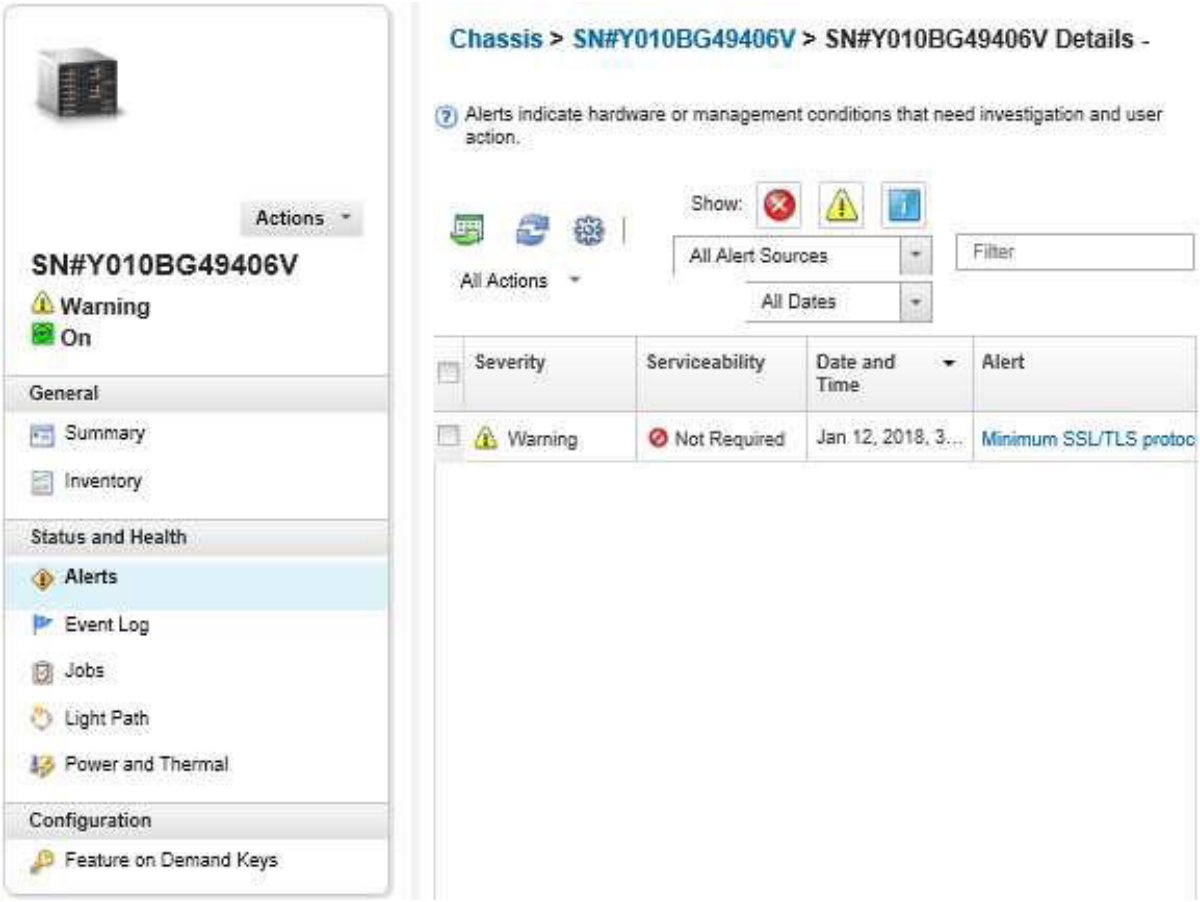
- To view all alerts in Lenovo XClarity Administrator, click **Monitoring → Alerts** from the Lenovo XClarity Administrator menu bar. The Alerts page is displayed with a list of all active alerts.



- To view alerts for a specific device:
  1. From the Lenovo XClarity Administrator menu bar, click **Hardware**, and then click a device type. A page is displayed with a tabular view of all managed devices of that type. For example, click **Hardware → Servers** to display the Servers page.
  2. Click a specific device to display the Summary page for the device.
  3. Under Status and Health, click **Alerts** to display a list of all alerts associated with that device.

     Notes: The Serviceability column might show “Not Available” if:

     – The alert on the device occurred before Lenovo XClarity Administrator started managing it
     – The event log has wrapped, and the event associated with that alert is no longer in the event log.



Results

From the Alerts page, you can perform the following actions:

- Refresh the list of alerts by clicking the **Refresh** icon ( ).

  Tip: If new alerts are detected, the alerts log refreshes automatically every 30 seconds.
- View information about a specific alert (including an explanation and user action) and about the device that is the source of the alert (such as the Universally Unique Identifier) by clicking the link in the **Alert** column. A dialog with information about the alert properties and details is displayed.

  Note: If the explanation and recovery actions for an alert are not displayed under the **Details** tab, go to Lenovo Flex System online documentation, and search for the alert ID (for example, `FQXHMSE0004G`). The website always provides the most up-to-date information.
- By default, excluded alerts do not influence the health status of managed devices. You can allow excluded alerts to influence the health status of managed devices from the Alerts page by clicking the toggle to enable **Excluded alerts influence health status for all devices**.
- You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level (see Setting threshold preferences for generating alerts and events).
- Export the alerts log by clicking the **Export as CSV** icon ( ).

  Note: The timestamps in the exported log use the local time that is specified by the web browser.
- Exclude specific alerts from all pages on which alerts are displayed (see Excluding alerts).

- Narrow the list of alerts that are displayed on the current page:
  - Show or hide alerts of a specific severity by clicking the following icons:
    - **Critical alerts** icon ( )
    - **Warning alerts** icon ( )
    - **Informational alerts** icon ( )
  - Show only alerts from specific sources. You can choose one of the following options from the drop-down list:
    - All Alert Sources
    - Hardware Events
    - Management Events
    - Service Center Events
    - Customer Serviceable Events
    - Non-serviceable Events
  - Show only alerts with a specific date and time. You can choose one of the following options from the drop-down list:
    - All Dates
    - Previous two hours
    - Previous 24 hours
    - Past Week
    - Past Month
  - List only alerts that contain specific text by entering the text in the **Filter** field.
  - Sort the alerts by column by clicking a column heading.

Excluding alerts

If there are specific alerts that are of no interest to you, you can exclude the alerts from all pages on which alerts are displayed. Excluded alerts are still in the log but are hidden from all pages on which alerts are displayed, including log views and device status.

About this task

Excluded alerts are hidden for all users, not just the user that set the configuration.

You can place devices in maintenance mode, so that all events and alerts for those devices device are excluded (see Placing devices in maintenance mode).

Restriction: Only users with administrative authority can exclude or restore alerts.

Important: If you exclude status alerts, device status on the device summary and detailed pages does not change.

ProcedureComplete the following steps to exclude alerts from the alerts log.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts**. The Alerts page is displayed.

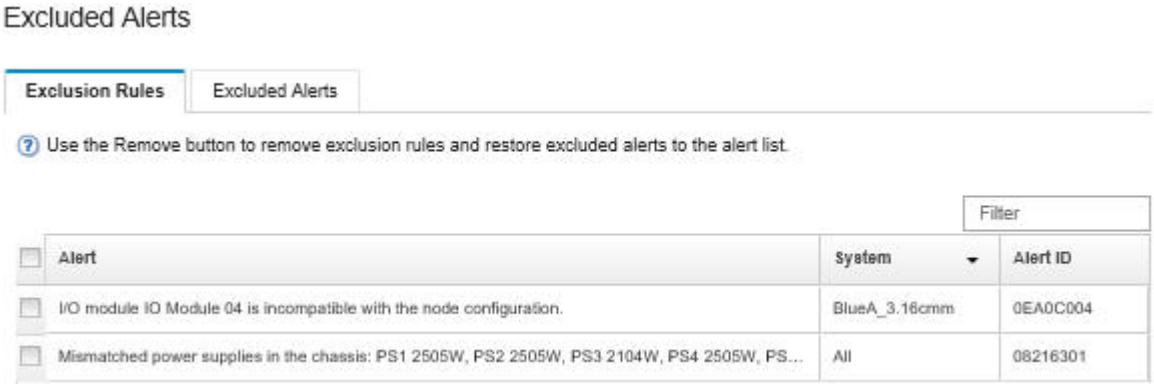
Step 2. Select the alerts to be excluded, and click the **Exclude alerts** icon ( ). The Exclude Alerts dialog is displayed.

Step 3. Select one of the following options:
- **Exclude selected alerts from all systems**. Excludes the selected alerts from all managed devices.
- **Exclude alerts only from systems in the scope of the instance selected**. Excludes the selected alerts from managed devices to which the selected alerts apply.

Step 4. Click **Save**.

What to do next

When you exclude alerts, Lenovo XClarity Administrator creates exclusion rules based on information that you provide. You can view a list of exclusion rules and excluded alerts from the Alerts page by clicking the **Show Excluded/Acknowledged Alerts** icon ( ). In the Excluded/Acknowledged Alerts dialog, click the **Exclusion Rules** tab to view the list of exclusion rules or click the **Excluded Alerts** tab to view the list of excluded alerts.



By default, excluded alerts do not influence the health status of managed devices. You can allow excluded alerts to influence the health status of managed devices from the Alerts page by clicking the toggle to enable **Show Excluded/Acknowledged Alerts**.

You can restore alerts that have been excluded in the alerts log by removing the appropriate exclusion rule.

To remove an exclusion rule, click the **Show Excluded Alerts** icon ( ) to display the Excluded Alerts dialog, select the exclusion rules or excluded alert to restore, and click **Remove**.

Resolving an alert

Lenovo XClarity Administrator provides information about the appropriate actions to perform to resolve an alert.

ProcedureComplete the following steps to resolve an alert.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts** to display the Alerts page.

Step 2. Locate the alert in the alerts log.

Step 3. Click the link in the **Alert** column to view information about the alert (including an explanation and recovery actions) and properties for the device that is the source of the alert (such as the Universally Unique Identifier).

Step 4. Complete the recovery actions that are listed under the **Details** tab to resolve the alert. The following example illustrates recovery actions for an event.

Change the security policy setting on the referenced managed chassis to match the current security policy on the management server.

To change the security policy on the chassis, open a command-line interface session on the Chassis Management Module (CMM) and run one of the following commands:

- To change the security policy level to `Secure`:
  ```
  security -p secure -T mm[p]
  ```

- To change the security policy level to `Legacy`:
  `security -p legacy -T mm[p]`

Note: If the explanation and recovery actions for an alert are not displayed under the **Details** tab, go to Lenovo Flex System online documentation, and search for the alert ID (for example, `FQXHMSE0004G`). The website always provides the most up-to-date information.

If you follow the recommended actions and the problem persists, contact Lenovo Support.

Acknowledging alerts

When an active alert is acknowledged, the alert is listed on pages on which alerts are displayed but does not affect the severity status for the applicable device.

Procedure

Complete the following steps to acknowledge an alert.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts**. The Alerts page is displayed.

Step 2. Select the alerts to be acknowledged.

Step 3. Click the **Acknowledge alerts** icon ( ).

What to do next

- You can view a list of acknowledged alerts from the Alerts page by clicking the **Show Excluded/ Acknowledged Alerts** icon ( ) to display the Excluded/Acknowledged Alerts dialog, and then clicking the **Acknowledged alerts** tab.
- You can remove the acknowledge for an active alert by clicking the **Show Excluded/Acknowledged Alerts** icon ( ) to display the Excluded/Acknowledged Alerts dialog, clicking the **Acknowledged alerts** tab, select the alerts, and then click the **Remove acknowledgement** icon ( ).

Working with events

From Lenovo XClarity Administrator, you have access to an event log and an audit log.

Learn more: XClarity Administrator: Monitoring

About this task

The *event log* provides a historical list of all hardware and management events.

The *audit log* provides a historical record of user actions, such as logging in to Lenovo XClarity Administrator, creating a new user, and changing a user password. You can use the audit log to track and document authentication and controls in IT systems.

Monitoring events in the event log

The *event log* provides a historical list of all hardware and management events.

About this task

The event log contains informational and non-informational events. The number of each of these events varies until the maximum of 50,000 events is reached in the event log. At that point, there is a maximum of

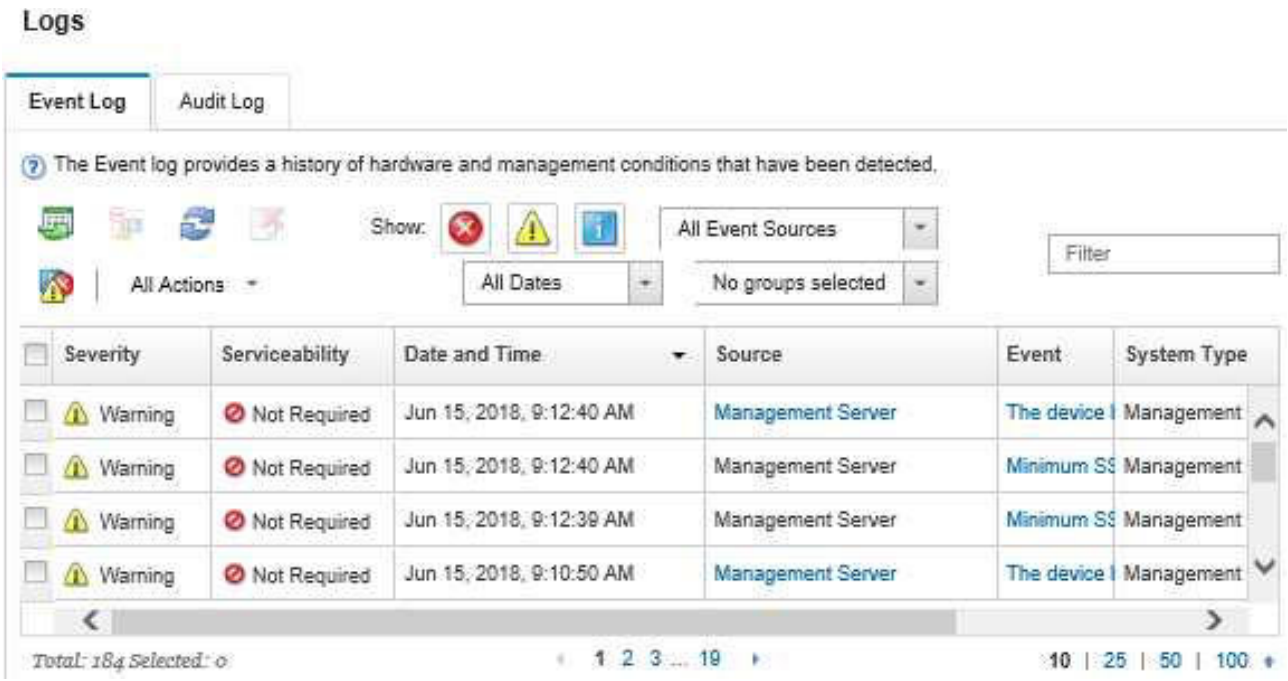
25,000 informational and 25,000 non-information events. For example, there are 0 events in the event log initially. Assume events are received so that 20,000 informational events and 30,000 non-informational events are received. When the next event is received, the oldest informational event is discarded even if a non-informational event is older. Eventually, the log balances out so that there are 25,000 of each type of event.

Lenovo XClarity Administrator sends an event when the event log reaches 80% of the minimum size and another event when the sum of the event and audit logs reaches 100% of the maximum size.

Tip: You can export the event log to ensure that you have a complete record of all hardware and management events. To export the event log, click the **Export as CSV** icon ( ).

Procedure

To view the event log, click **Monitoring → Event Logs** from the Lenovo XClarity Administrator menu bar, and click the **Event Log** tab. The Event Log page is displayed.



The **Serviceability** column identifies whether the device requires service. This column can contain one of the following values:

- **Not required**. The event is informational and does not require service.
- **User**. Take appropriate recovery action to resolve the issue.

  To view information about a specific event, click the link in the **Event** column. A dialog is displayed with information about the properties for the device that sent the event, details about the event, and recovery actions.
- **Support**. If Call Home is enabled on Lenovo XClarity Administrator, the event is typically submitted to Lenovo Support Center unless an open service ticket for the same event ID already exists for the device.

  If Call Home is not enabled, it is recommended that you manually open a service ticket to resolve the issue (see Opening a service ticket in the Lenovo XClarity Administrator online documentation).

Results

From the Event Log page, you can perform the following actions:

- View the source of the event by clicking the link in the **Source** column.
- Refresh the list of events by clicking the **Refresh** icon ( ).

  Tip: The event log refreshes automatically every 30 seconds if new events are detected.
- Clear all events in the event log by selecting **All Actions → Clear event log**.
- View details about a specific event by clicking the link in the **Event** column and clicking the **Details** tab.
- Export the event log by clicking the **Export as CSV** icon ( ).

  Note: The timestamps in the exported log use the local time that is specified by the web browser.
- Exclude specific events from all pages on which events are displayed (see Excluding events).
- Narrow the list of hardware and management events that are displayed on the current page:
  - Show or hide events of a specific severity by clicking the following icons from the drop-down list:
    - **Critical events** icon ( )
    - **Warning events** icon ( )
    - **Informational events** icon ( )
  - Show only events from specific sources. You can choose one of the following options from the drop-down list:
    - All Alert Sources
    - Hardware Events
    - Management Events
    - Serviceable Events
    - Customer Serviceable Events
    - Non-serviceable Events
  - Show only events with a specific date and time. You can choose one of the following options:
    - All Dates
    - Previous 2 hours
    - Previous 24 hours
    - Past Week
    - Past Month
    - Custom

    If you select **Custom**, you can filter hardware and management events that were raised between a custom start date and the current date.
  - List only events that contain specific text by entering the text in the **Filter** field.
  - Sort the events by column by clicking on a column heading.

Monitoring events in the audit log

The *audit log* provides a historical record of user actions, such as logging in to Lenovo XClarity Administrator, creating a new user, and changing a user password. You can use the audit log to track and document authentication and controls in IT systems.

About this task

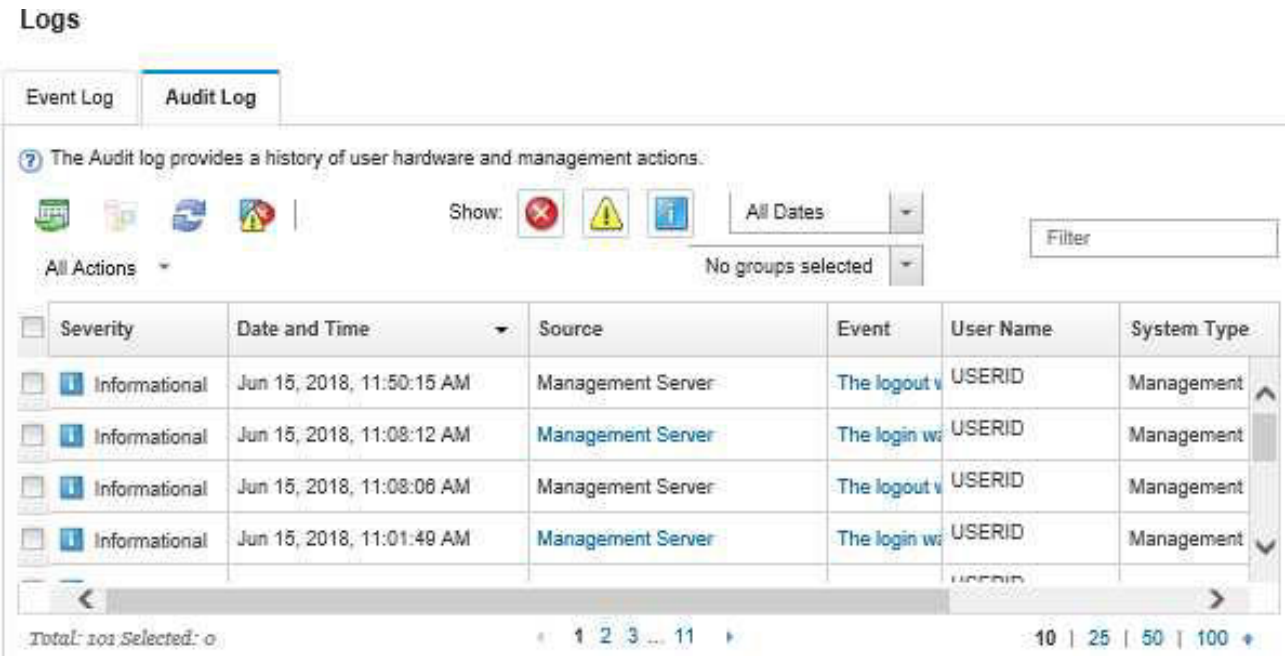
The audit log can contain a maximum of 50,000 events. When the maximum size is reached, the oldest event in the log is discarded and the new event is added to the log.

XClarity Administrator sends an event when the audit log reaches 80% of the maximum size and another event when the sum of the event and audit logs reaches 100% of the maximum size.

Tip: You can export the audit log to ensure that you have a complete record of all audit events. To export the audit log, click the **Export as CSV** icon ( ).

Procedure

To view the audit log, click **Monitoring → Event Logs** from the XClarity Administrator menu bar, and click the **Audit Log** tab. The Audit Log page is displayed.



To view information about a specific audit event, click the link in the **Event** column. A dialog is displayed with information about the properties for the device that sent the event, details about the event, and recovery actions.

Results

From this page, you can perform the following actions:

- View the source of the audit event by clicking the link in the **Source** column.
- Refresh the list of audit events by clicking the **Refresh** icon ( ).

  Tip: The event log refreshes automatically every 30 seconds if new events are detected.
- View details about a specific audit event by clicking the link in the **Event** column and then clicking the **Details** tab.
- Export the audit log by clicking the **Export as CSV** icon ( ).

  Note: The timestamps in the exported log use the local time that is specified by the web browser.
- Exclude specific audit events from all pages on which events are displayed (see Excluding events).
- Narrow the list of audit events that are displayed on the current page:
  - Show or hide events of a specific severity by clicking the following icons:

  - **Critical events** icon ()
  - **Warning events** icon ()
  - **Informational events** icon ()
- Show only events with a specific date and time. You can choose one of the following options from the drop-down list:
  - All Dates
  - Previous 2 hours
  - Previous 24 hours
  - Past Week
  - Past Month
  - Custom

  If you select **Custom**, you can filter hardware and management events that were raised between a custom start date and the current date.
- List only events that contain specific text by entering the text in the **Filter** field.
- Sort the events by column by clicking on a column heading.

Resolving an event

Lenovo XClarity Administrator provides information about the appropriate actions to perform to resolve an event.

Procedure

Complete the following steps to resolve an event.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Event Logs** to display the Logs page.

Step 2. Click the **Event Log** tab.

Step 3. Locate the event in the events log.

Step 4. Click the link in the **Event** column to view information about that event (including an explanation and recovery actions) and about the device that is the source of the event.

Step 5. Click the **Details** tab.

Step 6. Complete the recovery actions under the **Details** tab to resolve the event.

Note: If the explanation and recovery action for an event are not displayed, go to Lenovo Flex System online documentation, and search for the event title. The website always provides the most up-to-date information.

If you follow the recommended actions and the problem persists, contact Lenovo Support.

Excluding events

If there are specific events that are of no interest to you, you can exclude the events from all pages on which events are displayed. Excluded events are still in the log but are hidden from all pages on which events are displayed.

About this task

Excluded events are hidden for all users, not just the user that set the configuration.

You can place devices in maintenance mode, so that all events and alerts for those devices are excluded (see Placing devices in maintenance mode).

Restriction: Only users with administrative authority can exclude or restore events.

Procedure

Complete the following steps to exclude events from the event logs.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Event Logs**, and click the **Event Log** tab. The Event Logs is displayed.

Step 2. Select the events to be excluded, and click the **Exclude events** icon ( ). The Exclude Events dialog is displayed.

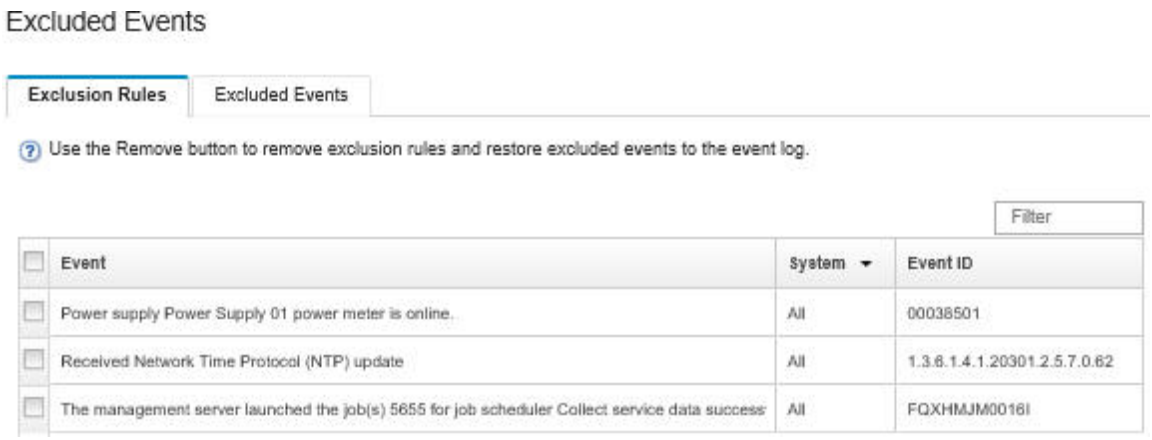
Step 3. Select one of the following options:
- **Exclude selected events from all systems**. Excludes the selected events from all managed devices.
- **Exclude events only from systems in the scope of the instance selected**. Excludes the selected events from managed devices to which the selected events apply.

Step 4. Click **Save**.

What to do next

When you exclude events, Lenovo XClarity Administrator creates exclusion rules based on information that you provide.

- View a list of exclusion rules and excluded events from the Logs page by clicking the **Show Excluded Events** icon ( ). In the Excluded Events dialog, click the **Exclusion Rules** tab to view the exclusion rules, or click the **Excluded Events** tab to view excluded events.



- Restore events that have been excluded in the event log by removing the appropriate exclusion rule. To remove an exclusion rule, click the **Show Excluded Events** icon ( ) to display the Excluded Events dialog, select the exclusion rules to restore, and click **Remove Exclusions**.
- Prevent serviceable events that are in the list of excluded events from automatically opening problem reports by clicking **Administration → Service and Support** from the Lenovo XClarity Administrator menu bar, clicking the **Service Forwarders** tab, and then selecting **No** next to the question **Do you want excluded events to open problem reports?**.

Forwarding events

You can configure Lenovo XClarity Administrator to forward events to mobile devices and to connected applications that you have in your environment for aggregating and monitoring hardware status and runtime issues for your hardware environment.

Learn more: XClarity Administrator: Monitoring

Forwarding events to syslog, remote SNMP manager, email, and other event services

You can configure Lenovo XClarity Administrator to forward events to connected applications that you have in your environment for aggregating and monitoring hardware status and runtime issues for your hardware environment. You can define the scope of events to be forwarded based on device, event class, event severity, and component.

About this task

Lenovo XClarity Administrator can forward events for one or more devices. For audit events, you can choose to forward all audit events or none. You cannot forward specific audit events. For hardware and management events, you can choose to forward events for one or more severities (critical, warning, and informational) and for one or more components (such as disk drives, processors, and adapters).

Lenovo XClarity Administrator uses event forwarders to forward events. An *event forwarder* includes information about the protocol to use, the recipient, the devices to monitor, and the events to forward. After you create and enable an event forwarder, Lenovo XClarity Administrator starts monitoring for incoming events based on the filter criteria. When a match is found, the associated protocol is used to forward the event.

The following protocols are supported:

- **Azure Log Analytics**. Lenovo XClarity Administrator forwards the monitored events to over the network to Microsoft Azure Log Analytics.
- **Email**. Lenovo XClarity Administrator forwards the monitored events to one or more email addresses using SMTP. The email contains information about the event, the host name of the source device, and links to the Lenovo XClarity Administrator web interface and Lenovo XClarity Mobile app.
- **FTP**. Forwards monitored events over the network to an FTP server.
- **REST**. Lenovo XClarity Administrator forwards the monitored events over the network to a REST Web Service.
- **SNMP**. Lenovo XClarity Administrator forwards the monitored events over the network to a remote SNMP manager. SNMPv1 and SNMPv3 traps are supported.

  For information about the management information base (MIB) file that describes the SNMP traps Lenovo XClarity Administrator generates, see lenovoMgrAlert.mib filelenovoMgrAlert.mib file in the Lenovo XClarity Administrator online documentation.
- **Syslog**. Lenovo XClarity Administrator forwards the monitored events over the network to a central log server where native tools can be used to monitor the syslog.

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Note: Events are not delivered if, for example, connectivity between Lenovo XClarity Administrator and the event forwarder is down or if the port is blocked.

Setting up event forwarding to Azure Log Analytics

You can configure Lenovo XClarity Administrator to forward specific events to Azure Log Analytics.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for Azure Log Analytics.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forders** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **Azure Log Analytics** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name and optional description for the event forwarder.
- Enter the primary key for the Azure Log Analytics interface.
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional**: If authentication is required, select one of the following authentication types:
  - **Basic**. Authenticates to the specified server using the specified user ID and password.
  - **None**. No authentication is used.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for Azure Log Analytics recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for Azure Log Analytics recipients are listed in the Output Format dialog.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
```

```
\"LXCA\":\"[[LXCA_IP]]\"}
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this event forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I,FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Select each component and severities for which you want events to be forward.

Step 13. Click **Next** to display the **Scheduler** tab.

Step 14. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

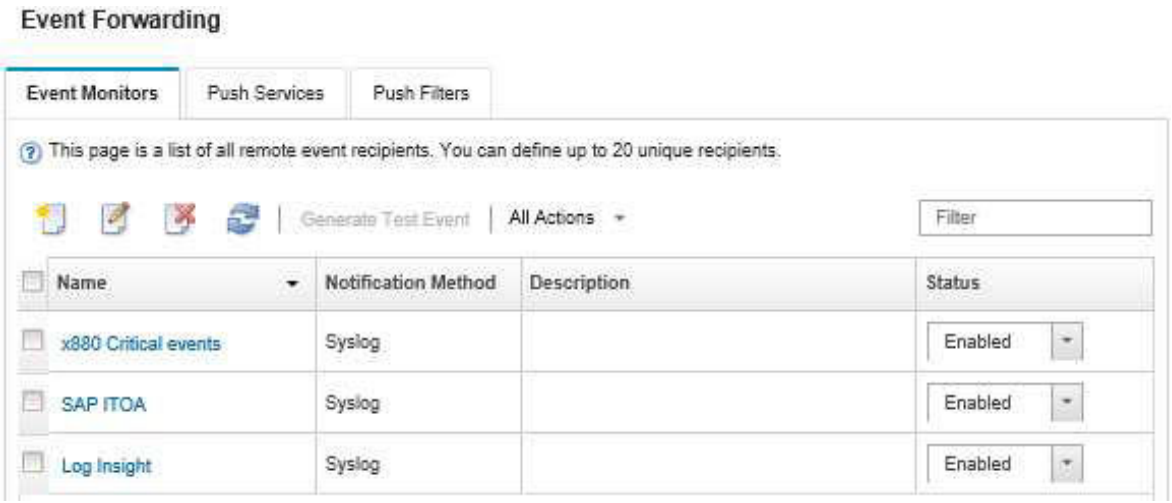
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.

3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:
- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 15. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 16. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate Azure Log Analytics server.

What to do next

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).

Setting up event forwarding to an email service using SMTP

You can configure Lenovo XClarity Administrator to forward specific events to an email service using SMTP.

Before you begin

To forward email to a web-based email service (such as Gmail, Hotmail, or Yahoo), your SMTP server must support forwarding web mail.

Before setting up an event forwarder to a Gmail web service, review information in Setting up event forwarding to a Gmail SMTP serviceSetting up event forwarding to syslog, remote SNMP manager, or email in the Lenovo XClarity Administrator online documentation.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for email using SMTP.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forders** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **Email** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name, destination host, and optional description for the event forwarder.
- Enter the port to use for forwarding events. The default is `25`.
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- Enter the email address for each recipient. Separate multiple email addresses by using a comma.

  To send the email to the support contact that is assigned for the device, select **Use Support Contact Email(s)** (see Defining the support contacts for a device in the XClarity Administrator online documentation).
- **Optional:** Enter the email address for the sender of the email (for example, `john@company.com`).

  If you do not specify an email address, the sender address is `LXCA.`<*source_identifier*>`@`<*smtp_host*> by default.

  If you specify only the sender domain, the format of the sender address is <*LXCA_host_name*>`@`<*sender_domain*> (for example, XClarity1@company.com).

  Notes:

  – If you set up your SMTP server to require a hostname to forward emails, and you do not set up a hostname for XClarity Administrator, it is possible that the SMTP server might reject forwarded events. If XClarity Administrator does not have a hostname, the event is forwarded with the IP address. If the IP address cannot be obtained, “localhost” is sent instead, which might cause the SMTP server to reject the event.

  - If you specify the sender domain, the source does not identify in the sender address. Instead, information about the source of the event is included in the body of the email, including system name, IP address, type/model, and serial number.
  - If the SMTP server accepts only emails that were sent by a registered user, the default sender address (LXCA.<*source_identifier*>@<*smtp_host*>) is rejected. In this case, you must specify at least a domain name in the **From address** field.
- **Optional:** To establish a secure connection to the SMTP server, select the following connection types:
  - **SSL**. Use the SSL protocol while communicating.
  - **STARTTLS**. Uses TLS to form a secure communication over an unsecure channel.

  If one of these connection types is selected, LXCA attempts to download and import the SMTP server's certificate to its truststore. You are asked to accept adding this certificate to the truststore.
- **Optional:** If authentication is required, select one of the following authentication types:
  - **Regular**. Authenticates to the specified SMTP server using the specified user ID and password.
  - **NTLM**. Uses the NT LAN Manager (NTLM) protocol to authentication to the specified SMTP server using the specified user ID, password, and domain name.
  - **OAUTH2**. Uses the Simple Authentication and Security Layer (SASL) protocol to authenticate to the specified SMTP server using the specified user name and security token. Typically, the user name is your email address.

    Attention: The security token expires after a short time. It is your responsibility to refresh the security token.
  - **None**. No authentication is used.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded in the email body and the format of the email subject. The information varies for each type of event forwarder.

The following example output format is the default format for email recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for the email recipients are listed in the Output Format dialog.

Email subject

```
[[DeviceName]]-[[EventMessage]]
```

Email body

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
```

```
Common Event ID : [[CommonEventID]]\n
EventSeverity   : [[EventSeverity]]\n
Event Class     : [[EventClass]]\n
Sequence ID     : [[EventSequenceID]]\n
Event Source ID : [[EventSourceUUID]]\n
Component ID    : [[EventComponentUUID]]\n
Serial Num      : [[EventSerialNumber]]\n
MTM             : [[EventMachineTypeModel]]\n
EventService    : [[EventService]]\n
Console link    : [[ConsoleLink]]\n
iOS link        : [[iOSLink]]\n
Android link    : [[AndroidLink]]\n
System Name     : [[DeviceFullPathName]]\n
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this event forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I,FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Select each component and severities for which you want events to be forward.

Step 13. Click **Next** to display the **Scheduler** tab.

Step 14. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

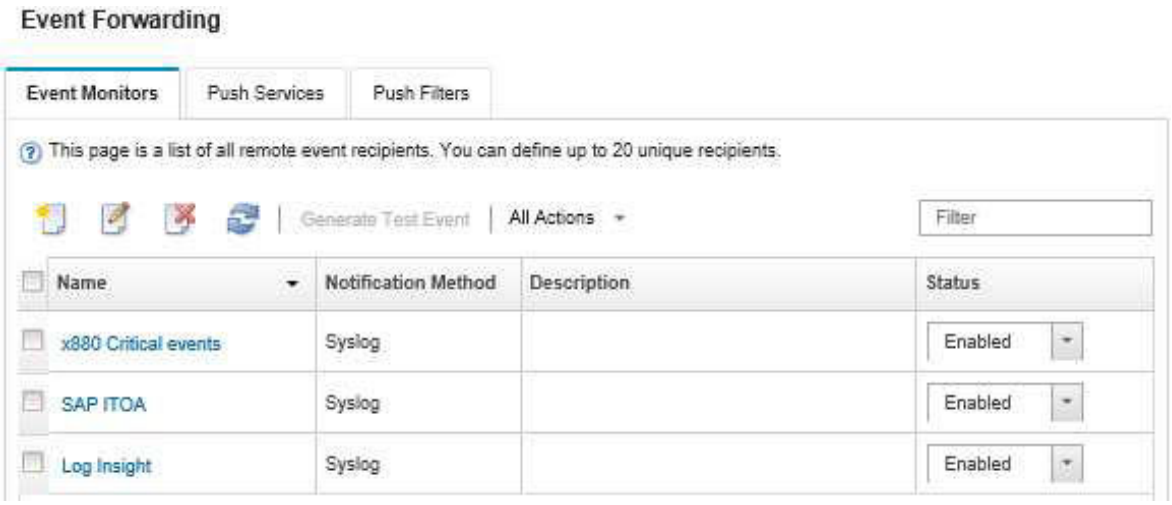
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 15. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 16. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate email service.

What to do next

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ().
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ().
- Suspend event forwarding (see Suspending event forwarding).

Setting up event forwarding to a Gmail SMTP service

You can setup Lenovo XClarity Administrator to forward monitored events to a web-based email service, such as Gmail.

Use the following configuration examples to help you set up your event forwarder to use the Gmail SMTP service.

Note: Gmail recommends using the OAUTH2 authentication method for the most secure communication. If you choose to use regular authentication, you will receive an email indicating that an application tried to use your account without using the latest security standards. The email includes instructions for configuring your email account to accept these types of applications.

For information about configuring a Gmail SMTP server, see https://support.google.com/a/answer/176600?hl=en.

Regular authentication using SSL on port 465

This example communicates with the Gmail SMTP server using the SSL protocol over port 465, and authenticates using a valid Gmail user account and password.

Parameter	Value
Host	smtp.gmail.com
Port	465
SSL	Select
STARTTLS	Clear
Authentication	Regular
User	Valid Gmail email address
Password	Gmail authentication password
From Address	(optional)

Regular authentication using TLS on port 587

This example communicates with the Gmail SMTP server using the TLS protocol over port 587, and authenticates using a valid Gmail user account and password.

Parameter	Value
Host	smtp.gmail.com
Port	587
SSL	Clear
STARTTLS	Select
Authentication	Regular

Parameter	Value
User	Valid Gmail email address
Password	Gmail authentication password
From Address	(optional)

OAUTH2 authentication using TLS on port 587

This example communicates with the Gmail SMTP server using the TLS protocol over port 587, and authenticates using a valid Gmail user account and security token.

Use the following example procedure to obtain the security token.

1. Create a project in the Google Developers Console, and retrieve the client ID and client secret. For more information, see the Google Sign-In for Websites webpage website.
   a. From a web browser, open the Google APIs webpage.
   b. Click **Select a project → Create a project** from the menu on that webpage. The New Project dialog is displayed.
   c. Type a name, select **Yes** to agree to the license agreement, and click **Create**.
   d. On the **Overview** tab, use the search field to search for "gmail."
   e. Click **GMAIL API** in the search results.
   f. Click on **Enable**.
   g. Click the **Credentials** tab
   h. Click **OAuth consent screen**.
   i. Type a name in the **Product name shown to users** field, and click **Save**.
   j. Click **Create credentials → OAuth client ID**.
   k. Select **Other**, and enter a name.
   l. Click **Create**. The OAuth client dialog is displayed with your client ID and client secret.
   m. Record the client ID and client secret for later use.
   n. Click **OK** to close the dialog.
2. Use the oauth2.py Python script to generate and authorize a security token by entering the client ID and client secret that was generated when you created the project.

   Note: Python 2.7 is required to complete this step. You can download and install Python 2.7 from the Python website).
   a. From a web browser, open the gmail-oauth2-tools webpage.
   b. Click **Raw**, and then save the content as a file name `oauth2.py` on your local system.
   c. Run the following command a terminal (Linux) or a command line (Windows):
   ```
   py oauth2.py --user=<your_email> --client_id=<client_id>
      --client_secret=<client_secret> --generate_oauth2_token
   ```
   For example
   ```
   py oauth2.py --user=jon@gmail.com
      --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
   ```
   This command returns a URL that you must use to authorize the token and retrieve a verification code from the Google website, for example:
   ```
   To authorize token, visit this url and follow the directions:
   ```

```
https://accounts.google.com/o/oauth2/auth?client_id=884243132302
-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&redirect_uri=
urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&response_type=code&scope=https%3A%2F%2Fmail.
google.com%2F

Enter verification code:
```

d. From a web browser, open the URL that was returned in the previous step.

e. Click **Allow** to agree to this service. A verification code to returned.

f. Enter the verification code in the **oauth2.py** command.

The command returns the security token and refreshes token, for example:

```
Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

Important: The security token expires after a period of time. You can use the oauth2.py Python script and the refresh token to generate a new security token. It is your responsibility to generate the new security token and update the event forwarder in Lenovo XClarity Administrator with the new token.

3. From the Lenovo XClarity Administrator web interface, set up event forwarder for email using the following attributes:

Parameter	Value
Host	smtp.gmail.com
Port	587
SSL	Clear
STARTTLS	Select
Authentication	OAUTH2
User	Valid Gmail email address
Token	Security token
From Address	(optional)

Setting up event forwarding to an FTP server

You can configure Lenovo XClarity Administrator to forward specific events to an FTP server.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for an FTP server.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forders** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **FTP** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name, destination host, and optional description for the event forwarders.
- Enter the port to use for forwarding events. The default is 21.
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional:** Specify the sequence of characters to be removed from the file content.
- Enter the file-name format to use for the file that contains the forwarded event. The default format is `event_[[EventSequenceID]].txt`.

  Note: Each file contains information for a single event.
- Enter the path on the remote FTP server where the file is to be uploaded.
- Choose the character encoding, either **UTF-8** or **Big5** . This is UTF-8 by default.
- Select the authentication type. This can be one of the following values.
  - **Anonymous**. (default) No authentication is used
  - **Basic**. Authenticates to the FTP server using the specified user ID and password.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarders.

The following example output format is the default format for FTP recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for FTP recipients are listed in the Output Format dialog.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
```

```
EventService    : [[EventService]]\n
Console link    : [[ConsoleLink]]\n
iOS link        : [[iOSLink]]\n
Android link    : [[AndroidLink]]\n
System Name     : [[DeviceFullPathName]]\n"
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this event forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I,FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Select each component and severities for which you want events to be forward.

Step 13. Click **Next** to display the **Scheduler** tab.

Step 14. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

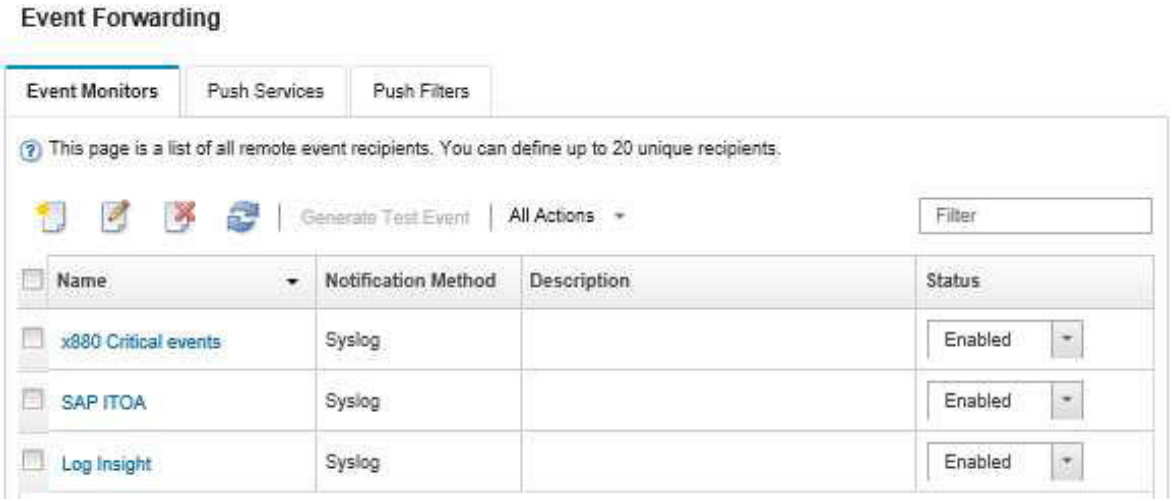
If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:
- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 15. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 16. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate FTP server.

What to do next

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).

- Suspend event forwarding (see Suspending event forwarding).

Setting up event forwarding to a REST Web Service

You can configure Lenovo XClarity Administrator to forward specific events to a REST Web Service.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for a REST Web Service.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forders** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **REST** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the resource path on which the forwarder is to post the events (for example, /rest/test).
- Select the protocol to use for forwarding events. This can be one of the following values.
  - **HTTP**
  - **HTTPS**
- Select the REST method. This can be one of the following values.
  - **PUT**
  - **POST**
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional:** If authentication is required, select one of the following authentication types:
  - **Basic**. Authenticates to the specified server using the specified user ID and password.
  - **None**. No authentication is used.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for REST Web Service recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for REST Web Service recipients are listed in the Output Format dialog.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
```

```
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this event forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Select each component and severities for which you want events to be forward.

Step 13. Click **Next** to display the **Scheduler** tab.

Step 14. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

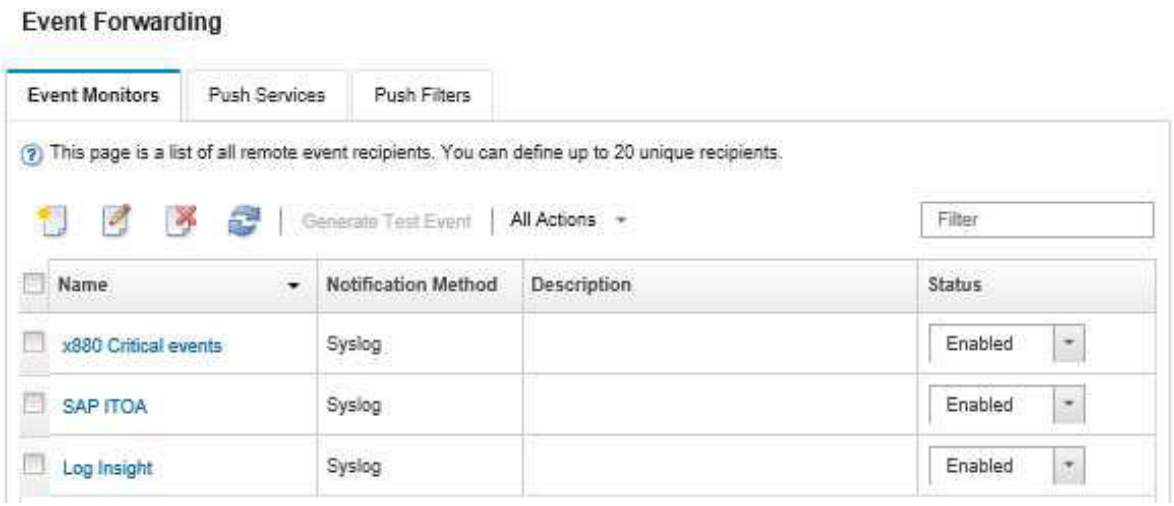
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 15. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 16. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate REST Web Service.

What to do next

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.

- Delete the event forwarder by clicking the **Delete** icon ().
- Suspend event forwarding (see Suspending event forwarding).

Setting up event forwarding to a remote SNMPv1 or SNMPv3 manager

You can configure Lenovo XClarity Administrator to forward specific events to a remote SNMPv1 or SNMPv3 manager.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for a remote SNMPv1 or SNMPv3 manager.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forders** tab.

Step 3. Click the **Create** icon (). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **SNMPv1** or **SNMPv3** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name and destination host for the event forwarder.
- Enter the port to use for forwarding events. The default is `162`.
- **Optional:** Enter additional information, including the description, contact name, and location.
- Select the SNMP version. This can be one of the following values.
  - **SNMPv1**. If this version is selected, specify the community password that is sent with every SNMP request to the device.
  - **SNMPv3**. This is the default version and is recommended for enhanced security. If SNMPv3 is selected, optionally specify the user ID, authentication type and password, and privacy type and password.

    If the SNMPv3 trap receiver requires the engine ID for the XClarity Administrator instance, you can find the engine ID by performing the following steps:

    1. Ensure that the connection parameters (username, authProtocol, authPassword, privProtocol, privPassword) match the ones set in XClarity Administrator.
    2. Using your preferred software (such as snmpwalk), perform an SNMP GET request on the XClarity Administrator server using one of the following OIDs:
       - EngineID: 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots : 1.3.6.1.6.3.10.2.1.2.0
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional**: If trap authentication is needed, enter the user ID and authentication password. The same user ID and password must be entered in the remote SNMP manager to which the traps are forwarded.

- Select the authentication protocol that is used by the remote SNMP manager to verify the trap sender. This can be one of the following values
  - **SHA**. Uses the SHA protocol to authentication to the specified SNMP server using the specified user ID, password, and domain name.
  - **None**. No authentication is used
- If trap encryption is needed, enter the privacy type (encryption protocol) and password. This can be one of the following values. The same protocol and password must be entered in the remote SNMP manager to which the traps are forwarded.
  - **AES**
  - **DES**
  - **None**

Step 5. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 6. Select **Enable this event forwarder** to activate event forwarding for this event forwarder.

Step 7. Click **Next** to display the **Devices** tab.

Step 8. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 9. Click **Next** to display the **Events** tab.

Step 10. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I,FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 11. Select each component and severities for which you want events to be forward.

Step 12. Click **Next** to display the **Scheduler** tab.

Step 13. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:
- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 14. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 15. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate remote SNMP manager.

What to do next

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.

- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).
- Download the MIB file that contains information about SNMP traps by clicking the **Create** icon ( ), and then clicking **Download MIB File** on the General tab of New Event Forwarding dialog

lenovoMgrAlert.mib file

This management information base (MIB) file describes the SNMP traps that Lenovo XClarity Administrator generates. You can compile this MIB file in any SNMP trap manager so that the SNMP traps that are sent from Lenovo XClarity Administrator can be rendered meaningfully.

For Lenovo XClarity Administrator v1.3 and later, you can download the MIB file from the web interface by clicking **Monitoring → Event Forwarding** from the menu bar, clicking the **Create** icon ( ), selecting **SNMP** for the event-forwarder type, and then clicking **Download MIB File** at the bottom of the dialog.

You can also use the following links to download the MIB file for your Lenovo XClarity Administrator version.
- lenovoMgrAlert_v320.mib
- lenovoMgrAlert_v310.mib
- lenovoMgrAlert_v300.mib
- lenovoMgrAlert_v280.mib
- lenovoMgrAlert_v270.mib
- lenovoMgrAlert_v260.mib
- lenovoMgrAlert_v250.mib
- lenovoMgrAlert_v240.mib
- lenovoMgrAlert_v230.mib
- lenovoMgrAlert_v210.mib
- lenovoMgrAlert_v210.mib
- lenovoMgrAlert_v200.mib

The following objects are included in all outgoing SNMP traps. Additional objects might be included in some SNMP traps. All objects are described in the MIB file.

Note: This list might differ for earlier releases of Lenovo XClarity Administrator.
- mgrTrapSystemName
- mgrTrapDateTime
- mgrTrapAppId
- mgrTrapTxtId
- mgrTrapSysContact
- mgrTrapSysLocation
- mgrTrapID
- mgrTrapSeverity
- mgrTrapEvtID
- mgrTrapMsgID
- mgrTrapMsgText
- mgrTrapEventClass
- mgrTrapUserid
- mgrTrapService
- mgrTrapUuid
- mgrTrapSN
- mgrTrapMtm
- mgrTrapSrcLoc
- mgrTrapSrcName

- mgrTrapSrcIP
- mgrTrapFailFRUs
- mgrTrapFailSNs

Setting up event forwarding to a syslog

You can configure Lenovo XClarity Administrator to forward specific events to a syslog.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for a syslog.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forders** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **Syslog** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name, destination host, and optional description for the event forwarder.
- Enter the port to use for forwarding events. The default is `514`.
- Select the protocol to use for forwarding events. This can be one of the following values.
  - **UDP**
  - **TCP**
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- Optionally select the format for the timestamp in the syslog. This can be one of the following values.
  - **Local time**. The default format, for example `Fri Mar 31 05:57:18 EDT 2017`.
  - **GMT time**. International standard (ISO8601) for dates and times, for example `2017-03-31T05:58:20-04:00`.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for sylog recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for sylog recipients are listed in the Output Format dialog.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this event forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I,FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Select each component and severities for which you want events to be forward.

Step 13. Click **Next** to display the **Scheduler** tab.

Step 14. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

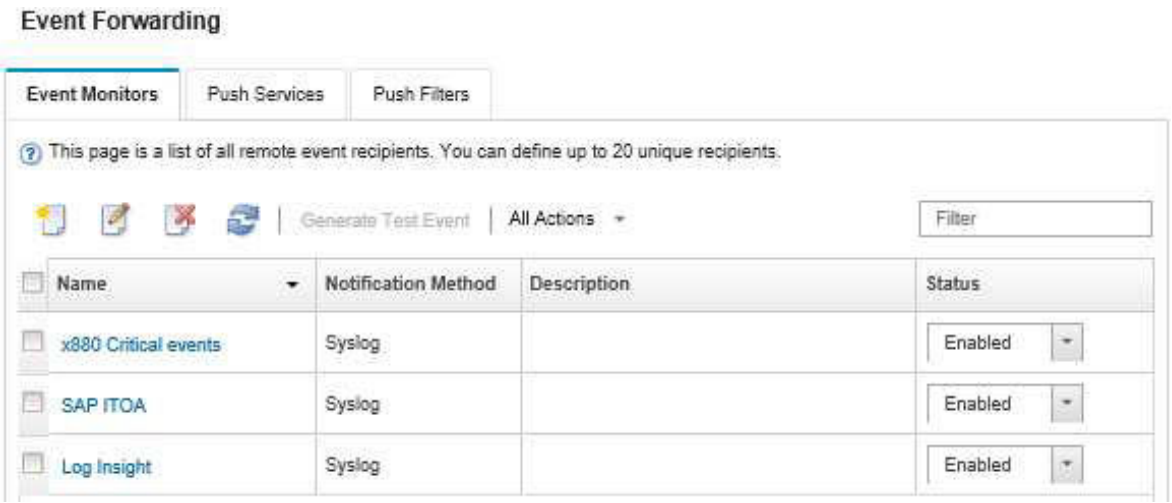
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.

4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:
- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 15. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 16. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate syslog.

What to do next

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).

Suspending event forwarding

You can suspend event forwarding by disabling the event forwarder. Suspending event forwarding stops the monitoring of incoming events. Events that are received while monitoring is suspended are not forwarded.

About this task

The disabled state is not persistent. If the management node is restarted, all event forwarders become enabled.

Procedure

Complete the following steps to disable the forwarding of events.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Forwarding Events**. The Event Forwarding page is displayed.

Step 2. Select **Disable** in the **Status** column for each event forwarder that you want to suspend.

Forwarding events to mobile devices

You can configure Lenovo XClarity Administrator to push event notifications to mobile devices

Before you begin

The following requirements must be met to forward events to mobile devices:

- Ensure that a valid DNS server is configured to allow Lenovo XClarity Administrator to connect to the Apple or Google push servers. This can be configured by clicking the **Administration → Network Access → Edit Network Access** and then clicking the **Internet Settings** tab (see Configuring network access).
- Ensure that all required ports for event management are open on the network and firewalls. For information about port requirements, see Port availability in the Lenovo XClarity Administrator online documentation.

About this task

When the Lenovo XClarity Mobile app is installed on a mobile device, you can enable each connected Lenovo XClarity Administrator instance to push event notifications to that mobile device. When push notifications are enabled for a specific instance, a subscription is created in Lenovo XClarity Administrator for that mobile device.

You can define the events that are pushed to the mobile device by assigning predefined or customized global event filters for each Lenovo XClarity Administrator instance. The predefined global event filters are enabled by default. Lenovo XClarity Administrator starts monitoring for incoming events based on the filter criteria. When a match is found, the event is forwarded to the mobile device.

For more information about Lenovo XClarity Mobile and supported mobile devices, see Using the Lenovo XClarity Mobile app.

Procedure

To set up push notifications to that mobile device, complete the following steps from the Lenovo XClarity Mobile app on your mobile device.

Step 1. Enable push notifications:

- You can enable push notifications when you create a connection to a Lenovo XClarity Administrator instance. Push notifications are enabled by default.
- You can enable push notifications on existing connections by enabling one or more event filters

Step 2. Assign global event filters to specify which events are to be forwarded to the mobile device:

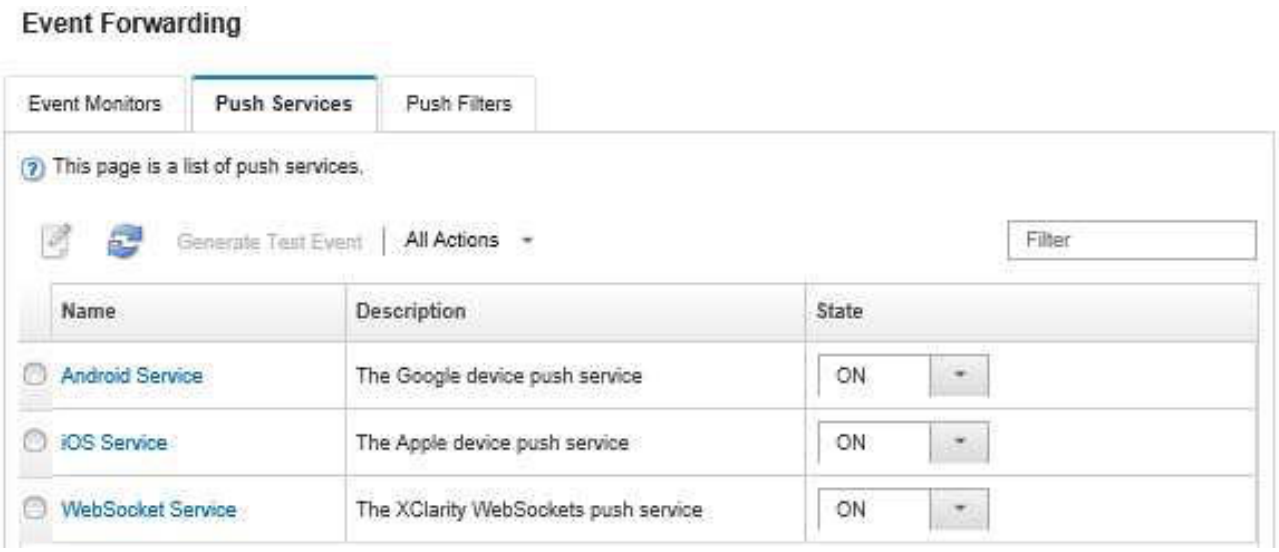
Note: You can add or remove global filters from the subscription only from the Lenovo XClarity Mobile app. You can create global filters only from the Lenovo XClarity Administrator web interface.

For information about creating customized global event filters, see Creating event filters for mobile devices and WebSockets.

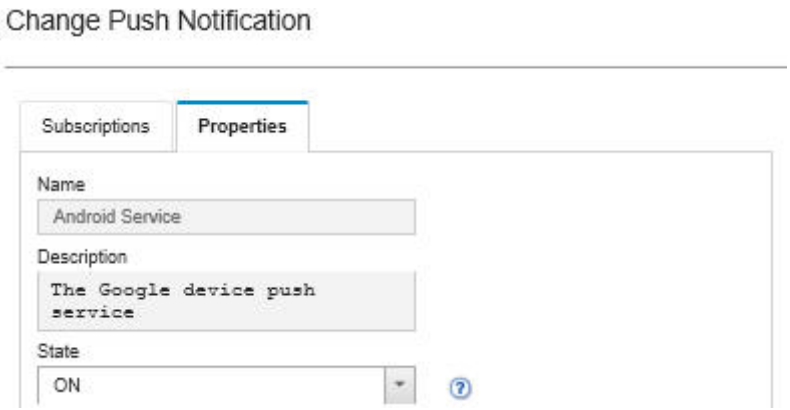
1. Tap **Settings → Push notifications**. A list of Lenovo XClarity Administrator connections is displayed.
2. Tap the Lenovo XClarity Administrator instance to display a list of push filters.
3. Enable the event filters for the events that you want pushed to the mobile device for the Lenovo XClarity Administrator instance.
4. Tap **Touch to generate test push notification** to verify that the event notifications are pushed correctly.

Results

You can manage subscriptions from the Event Forwarding page in the Lenovo XClarity Administrator web interface. Click **Monitoring → Event Forwarding** to display the Event Forwarding page.



- You can change the device notification service properties from the **Push Service** tab on the Event Forwarding page by clicking the link for the push notification service (Google or Apple) in the **Name** column to display the Change Push Notification dialog, and then click the **Properties** tab.

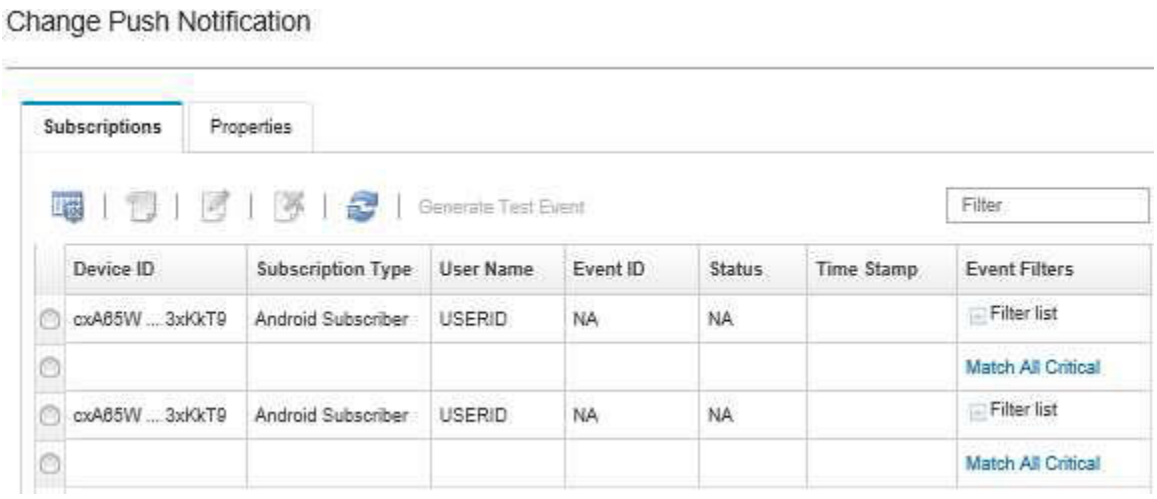


- You can enable and disable subscriptions:

  - Enable or disable all subscriptions for a specific device notification service from the **Push Service** tab on the Event Forwarding page by selecting the **ON** or **OFF** state in the table for the device notification service.
  - Enable or disable all subscriptions for a specific device from the Lenovo XClarity Mobile app by tapping **Settings → Push notification**, and then enabling or disabling Enabled push notification.
  - Enable or disable a specific subscription from the Lenovo XClarity Mobile app by tapping **Settings → Push notification**, tapping a Lenovo XClarity Administrator connection, and enabling at least one event filter or disabling all event filters.
- You can generate a test event for all subscriptions for a specific mobile service from the **Push Service** tab on the Event Forwarding page by selecting the mobile service and clicking **Generate Test Event**.
- You can view a list of current subscriptions. From the **Push Service** tab on the Event Forwarding page, click the link for the applicable device notification service (Android or iOS) in the **Name** column to display the Change Push Notification dialog, and then click the **Subscriptions** tab. The device ID identifies each subscription.

  Tips:

  - The device ID is the first and last 6 digits of the push registration ID. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**.
  - If you are logged in as a user with one of the following roles, all subscriptions are displayed; otherwise, subscriptions for only the logged-in user are displayed.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- You can view the list of event filters that are assigned to the subscription from the **Subscriptions** tab on the Change Push Notification dialog by expanding the **Filter list** in the **Event Filters** column for the subscription.



- You can create event filters for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription, and click the **Create** icon ( ).

  Note: These event filters apply to only a specific subscription and cannot be used by other subscriptions.

  You can also edit or remove an event filter by selecting the event filter and clicking the **Edit** icon ( ) or **Remove** icon ( ), respectively.

- You can determine the status of the last attempted push for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog. The **Time Stamp** column indicates the date and time of the last push. The **Status** indicates whether the push notification was successfully delivered to the push service. No status is available regarding whether the push notification was successfully delivered to the device from the service. If the delivery to the push service failed, the Status column provides additional information about the failure.
- You can generate a test event for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription and clicking **Generate Test Event**.
- You can remove a subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription, and clicking the **Remove** icon ( ).

Forwarding events to WebSocket services

You can configure Lenovo XClarity Administrator to push event notifications to WebSocket services.

About this task

The WebSocket subscriptions are not stored persistently in Lenovo XClarity Administrator. When Lenovo XClarity Administrator is rebooted, the WebSocket subscribers must subscribe again.

Procedure

To push event notification to a WebSocket service, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Push Services** tab.

Step 3. Click the link for the **WebSocket Service** in the **Name** column. The Change Push Notification dialog is displayed.

Step 4. Click the **Subscriptions** tab.

Step 5. Click the **Create** icon ( ).

Step 6. Enter the IP address of the destination host.

Step 7. Click **Create**.

Step 8. Select the new subscription, click **Generate Test Event**, and then verify that the events are forwarded correctly to the WebSocket service.

Results

From the **Subscriptions** tab on the Change Push Notification dialog, you can perform the following actions on a selected WebSocket subscription:

- Refresh the list of WebSocket services by clicking the **Refresh** icon ( ).
- Delete subscriptions by selecting the subscriptions and clicking the **Delete** icon ( ).
- Determine the status of the last attempted push for a specific subscription by viewing the content of the **Status** column. If the attempt failed, this column contains a message that describes the error.

From the **Properties** tab on the Change Push Notification dialog, you can perform the following actions:

- Change the WebSocket service properties, including the connection idle time, maximum buffer size, maximum number of subscribers, and the register time-out period.
- You can reset the WebSocket service to the default settings by clicking **Restore Defaults**.

- Suspend pushing event notifications to all subscriptions for the WebSocket service by setting the **State** to Off.

From the **Push Service** tab on the Event Forwarding page, you can generate a test event for all WebSocket subscriptions by selecting the WebSocket service and clicking **Generate Test Event**.

Creating event filters for mobile devices and WebSockets

You can create global events filters that can be used in one or more subscriptions for mobile devices and WebSockets. You can also create event filters that are unique to a subscription.

Before you begin

You must have supervisor authority to create event filters.

You can create up to 20 global event filters.

About this task

The following global event filters are predefined:

- **Match All Critical**. This filter matches all critical events that are generated by any managed device or by XClarity Administrator.
- **Match All Warning**. This filter matches all warning events that are generated by any managed device or by XClarity Administrator.

Procedure

To create a global event filter, complete the following steps.

- Create a global event filter that can be used by any subscription.
  1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.
  2. Click the **Push Filters** tab.
  3. Click the **Create** icon ( ). The **General** tab of New Push Filter dialog is displayed.
  4. Specify the name and option description for this event filter.
  5. Click **Next** to display the **Systems** tab.
  6. Select the devices that you want monitor.

     Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.
  7. Click **Next** to display the **Events** tab.
  8. Select the components and severities for which you want events to be forward.

     Tip:
     - To forward all hardware events, select **Match all events**.
     - To forward audit events, select **Include All Audit events**.
     - To forward warranty events, select **Include Warranty events**.
  9. Click **Create**.

- Create an event filter for a specific subscription:
  1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The New Event Forwarding page is displayed.
  2. Click the **Push Filters** tab.
  3. Select the link for the type of mobile device (Android or iOS) in the Name column of the table. The Change Push Notification dialog is displayed.
  4. Click the **Subscriptions** tab to display a list of active subscriptions.
  5. Select the subscription, and click the **Create** icon ( ). The **General** tab of New Event Filter dialog is displayed.
  6. Specify the name and option description for this event filter.
  7. Click **Next** to display the **Systems** tab.
  8. Select the devices that you want monitor.

     Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.
  9. Click **Next** to display the **Events** tab.
  10. Select the components and severities for which you want events to be forward.

      Tip:
      - To forward all hardware events, select **Match all events**.
      - To forward audit events, select **Include All Audit events**.
      - To forward warranty events, select **Include Warranty events**.
  11. Click **Create**.

What to do next

From the Push Filters tab on the Event Forwarding page, you can perform the following actions on a selected event filter:

- Refresh the list of event filters by clicking the **Refresh** icon ( ).
- View details about a specific event filter by clicking the link in the **Name** column.
- Change the event filter properties and filter criteria by clicking the **Edit** icon ( ).

Delete the event filter by clicking the **Delete** icon ( ).

Working with jobs

Jobs are longer running tasks that are performed against one or more devices. You can schedule certain jobs to run only one time (immediately or at later time), on a reoccurring basis, or when a specific event occurs.

Jobs run in the background. You can see the status of each job from the jobs log.

Monitoring jobs

You can view a log of all jobs that are started by Lenovo XClarity Administrator. The jobs log includes jobs that are running, completed, or have errors.

About this task

Jobs are longer running tasks that are performed against one or more devices. For example, if you deploy an operating system to multiple servers, each server deployment is listed as a separate job.

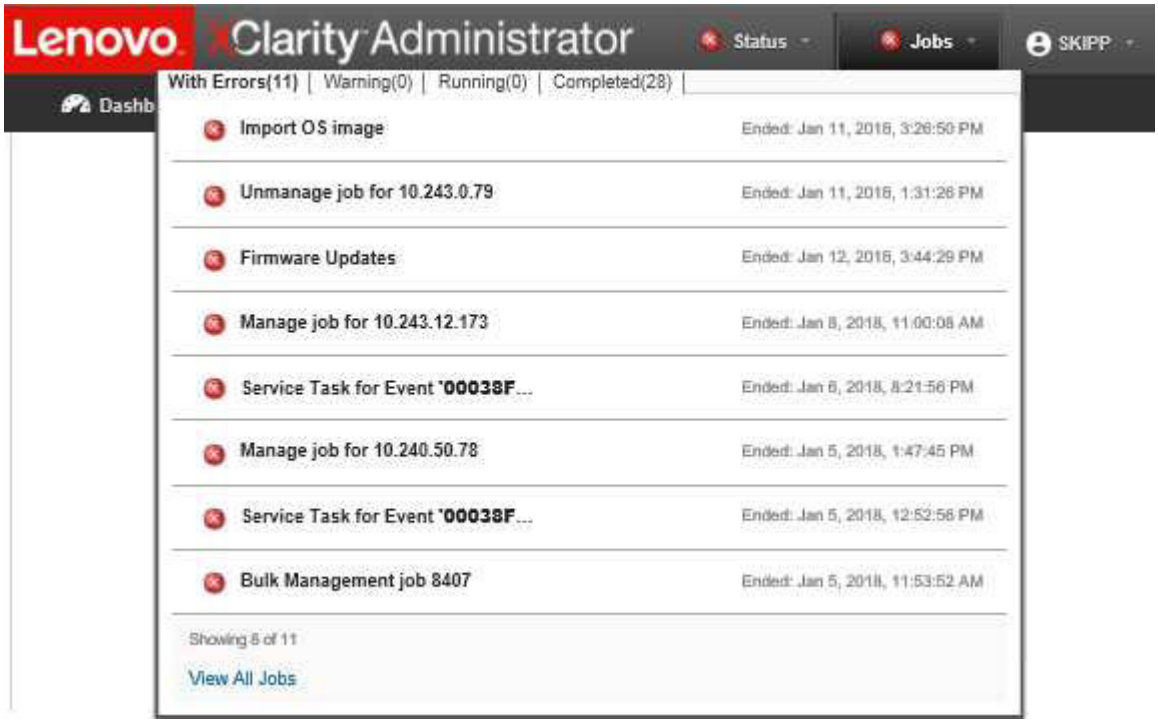
Jobs run in the background. You can see the status of each job from the jobs log.

The jobs log contains information about each job. The log can contain a maximum of 1000 jobs or 1 GB. When the maximum size is reached, the oldest jobs that completed successfully are deleted. If there are no jobs that completed successfully in the log, the oldest jobs that completed with warnings are deleted. If there are no jobs that completed successfully or with warnings in the log, the oldest jobs that completed with errors are deleted.

Procedure

Complete one of the following steps to display the jobs log.

- From the XClarity Administrator title bar, click **Jobs** to display a summary of jobs that are running, completed, and have errors.

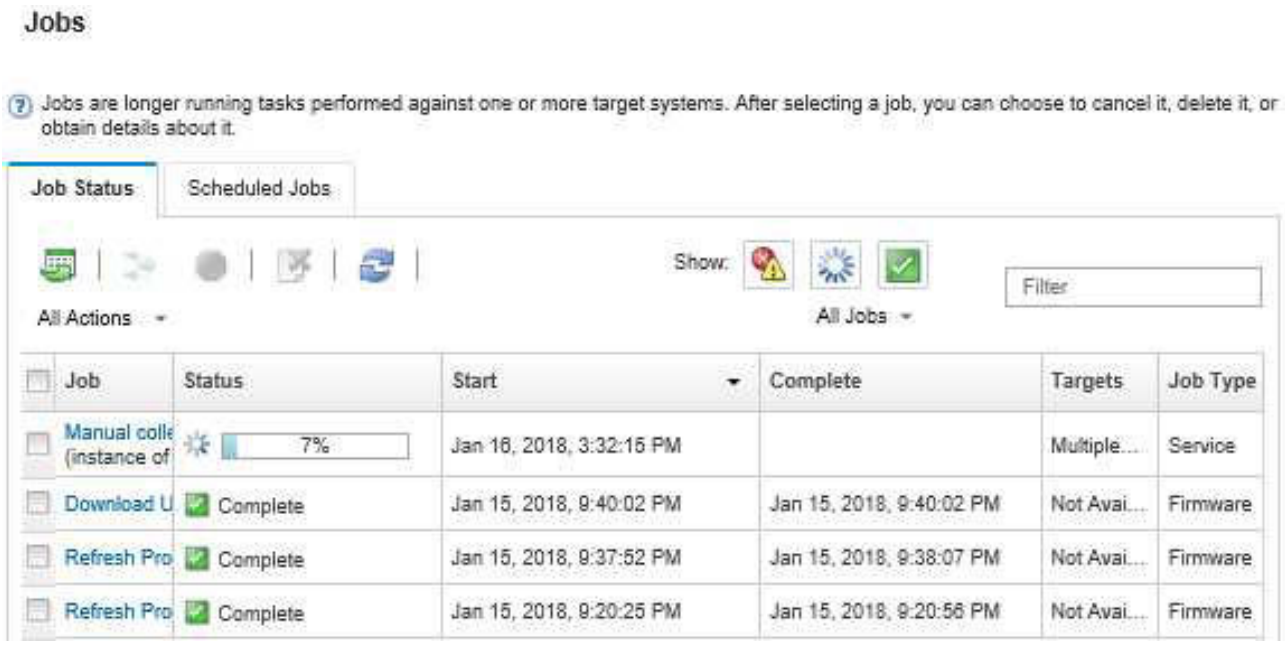


  From this pull down, you can click the following tabs:
  - **Errors**. Displays a list of all jobs that have errors associated with them.
  - **Warnings**. Displays a list of all jobs that have warnings associated with them.
  - **Running**. Displays a list of all jobs that are currently in progress.
  - **Completed**. Displays a list of all jobs that are completed.

  Hover over a job entry in the pull down to get more information about the job, including the status, progress, and user that created the job.
- From the XClarity Administrator title bar, click **Jobs**, and click the **View All Jobs** link to display the Jobs Status page.
- From the XClarity Administrator menu bar, click **Monitor → Jobs** and click the **Job Status** tab to display the Jobs Status page.

What to do next

The Jobs page is displayed with a list of all jobs for XClarity Administrator.



From this page, you can perform the following actions:

- Create job schedules by clicking the **Scheduled Jobs** tab (see Scheduling jobs).
- View more information about a specific job by clicking the job description in the **Jobs** column. A dialog is displayed with a list of subtasks (subjobs) and their targets, a summary of the subtasks including any necessary actions, and log details including the severity and timestamp for each message. You can choose to hide or show logs for child tasks.
- For scheduled jobs, view information about the job schedule by clicking the “this” link under the job description in the **Jobs** column.
- Change the number of jobs that are displayed per page. The default is 10 jobs. You can display 25, 50, or all jobs.
- Narrow the list of jobs that are displayed:
  - List only jobs from a specific source by clicking **Job Types** and choosing from the following options.
    - **All Job Types**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**
    - **Power**
    - **Remote Access**
    - **System ID**
    - **OS Images**
    - **OS Deployment**
    - **OS Profile Export**
    - **Custom**
    - **Inventory**
    - **Unknown**

  - List only scheduled jobs that are associated with a specific schedule type by clicking **Schedule Types** and choosing from the following options.
    - **All Schedule Types**
    - **One Time**
    - **Recurring**
    - **Triggered**
  - Hide or show jobs that have errors or warnings by clicking the **Hide error/warning jobs** icon ().
  - Hide or show jobs that are currently running by clicking the **Hide running jobs** icon ().
  - Hide or show jobs that are completed by clicking the **Hide completed jobs** icon ().
  - List only jobs that contain specific text by entering the text in the **Filter** field.
  - If filtering is applied to the page, remove the filter by clicking the **Show All Jobs** icon ().
  - Sort the jobs by column by clicking a column heading.
- Export the jobs list as a CSV file by clicking the **Export as CSV** icon ().

  Note: The timestamps in the exported log use the local time that is specified by the web browser.
- Cancel running jobs or subtasks by selecting one or more running jobs or subtasks and clicking the **Stop** icon ().

  Note: It might take several minutes to cancel the job.
- Delete completed jobs or subtasks from the jobs log by selecting one or more completed jobs or subtasks and clicking the **Delete** icon ().
- Export information about specific jobs by selecting the jobs and clicking the **Export as CSV** icon ().
- Refresh the jobs log by clicking the **Refresh** icon ().

Scheduling jobs

You can create schedules in Lenovo XClarity Administrator to run certain tasks at specific times.

About this task

You can schedule the following types of jobs:
- Simple tasks, such as powering off and rebooting
- Collecting service data for specific devices
- Refreshing the firmware-update and OS device-driver catalogs from the Lenovo website
- Refreshing the XClarity Administrator updates catalog from the Lenovo website
- Downloading firmware from the Lenovo website
- Updating firmware and OS device drivers on managed devices
- Backing up XClarity Administrator data and settings
- Backing up and restoring switch configuration data

You can schedule jobs to run:
- Only one time (immediately or at a later time)
- On a recurring basis
- When a specific event occurs

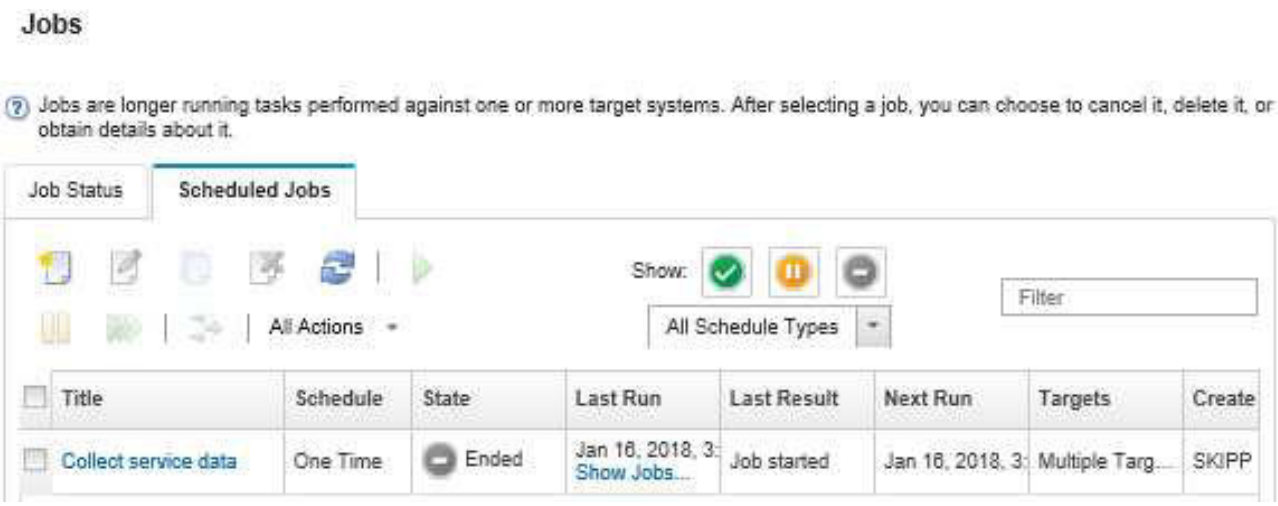
Procedure

To create and schedule a job, complete the following steps.

- For complex tasks, such as updating firmware and collecting service data, create the job from the current the task page or dialog.
  1. Click **Schedule** to create a schedule for running this task. The Schedule New Job dialog is displayed.
  2. Enter a name for the job.
  3. Specify when the job is to be run. The available options depend on the type of job. Some jobs cannot be recurring or triggered by an event
     - **One Time**. These jobs run only one time. Specify the date and time when you want this job to run.
     - **Recurring**. These jobs run more than one time. Specify the when and how often you want this job to run.
     - **Triggered by Event**. These jobs run when a specific event occurs.
       a. Specify the date and time when you want this job to run, and click **Next**.
       b. Select the event to trigger the job.
  4. Click **Create Job**.
- For simple tasks, such as powering on and rebooting, create the job schedule from the Jobs page.
  1. From the XClarity Administrator menu bar, click **Monitor → Jobs**, and click the **Scheduled Job** tab to display the Scheduled Jobs page.
  2. Click the **Create** icon ( ) to display the Schedule New Jobs dialog.
  3. Enter a name for the job.
  4. Specify when the job is to be run.
     - **One Time**. These jobs run only one time.
       a. Specify the date and time when you want this job to run, and click **Next**.
       b. Select managed devices on which the job is to run.
     - **Recurring**. These jobs run more than one time.
       a. Specify the when and how often you want this job to run.
       b. Select managed devices on which the job is to run**.**
     - **Triggered by Event**. These jobs run when a specific event occurs.
       a. Specify the date and time when you want this job to run, and click **Next**.
       b. Select managed devices on which the job is to run, and click **Next**.
       c. Select the event to trigger the job.
  5. Click **Create**.

What to do next

The Scheduled Jobs tab is displayed with a list of all job schedules in XClarity Administrator.



From this page, you can perform the following actions:

- View information about all active and completed jobs for a specific job schedule by clicking the link in the **Job** column.
  - Narrow the list of job schedules that are displayed by a specific schedule type by clicking **Schedule Types** and choosing from the following options:
    - **All Schedule Types**
    - **One Time**
    - **Recurring**
    - **Triggered**
  - Hide or show only job schedules that are in a specific state by clicking one of the following icons:
    - All scheduled jobs that are active by clicking the **Active** icon ( ).
    - All scheduled jobs that are not active by clicking the **Paused** icon ( ).
    - All scheduled jobs that already ran and are not scheduled to run again by clicking the **Ended** icon ( ).
  - List only scheduled jobs that contain specific text by entering the text in the **Filter** field.
  - Sort the scheduled jobs by column by clicking a column heading.
- View when the job ran last by looking at the **Last Run** column. View the status of the last run job by clicking the “Job Status” link in that column.
- View when the job is scheduled to run next by looking at the **Next Run** column. View a list of all future dates and times by clicking the “More” link in that column.
- Immediately run the job that is associated with the schedule by clicking the **Run** icon ( ).
- Disable or enable a job schedule by clicking the **Pause** icon ( ) or **Activate** icon ( ) respectively.
- Copy and then modify a job schedule by clicking the **Copy** icon ( ).
- Edit a job schedule by clicking the **Edit** icon ( ).
- Delete one or more selected job schedules by clicking the **Delete** icon ( ).
- Export information about specific job schedules by selecting the schedules and clicking the **Export as CSV** icon ( ).
- Refresh the list of job schedule by clicking the **All Actions → Refresh**.

Adding a resolution and comments to a job

You can add a resolution and comments to a completed job, regardless of the success or error state. You can do this for a parent job and for subtasks in the job.

Procedure

Complete one of the following steps to add a resolution and comments to a job.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitor → Jobs**, and click the **Job Status** tab to display the Jobs Status page.

Step 2. Click the link for the job in the **Job** column to display the job details.

Step 3. Click the **Notes** icon ( ) to display the Notes dialog.

From this dialog, you can see a history of all notes and resolutions that were added to the job. You can clear the history by clicking **Clear All Records**.

Step 4. Choose one of the following resolutions.
- **No Changes**
- **Investigating**
- **Resolved**
- **Aborted**

Step 5. Add a remark in the **Note** field.

Step 6. Click **Apply**.

On the Job Status page, the resolution is displayed in the **Status** column for that job.

Viewing relationships between jobs and events

A *flow diagram* is a graphical view that shows relationships between activities (including jobs and events) that are manually initiated by a user or automatically initiated by Lenovo XClarity Administrator. The flow diagram helps to identify problems by illustrating the sequence of actions that were initiated and events that were generated, when they generated, and what caused them to be generated.

Before you begin

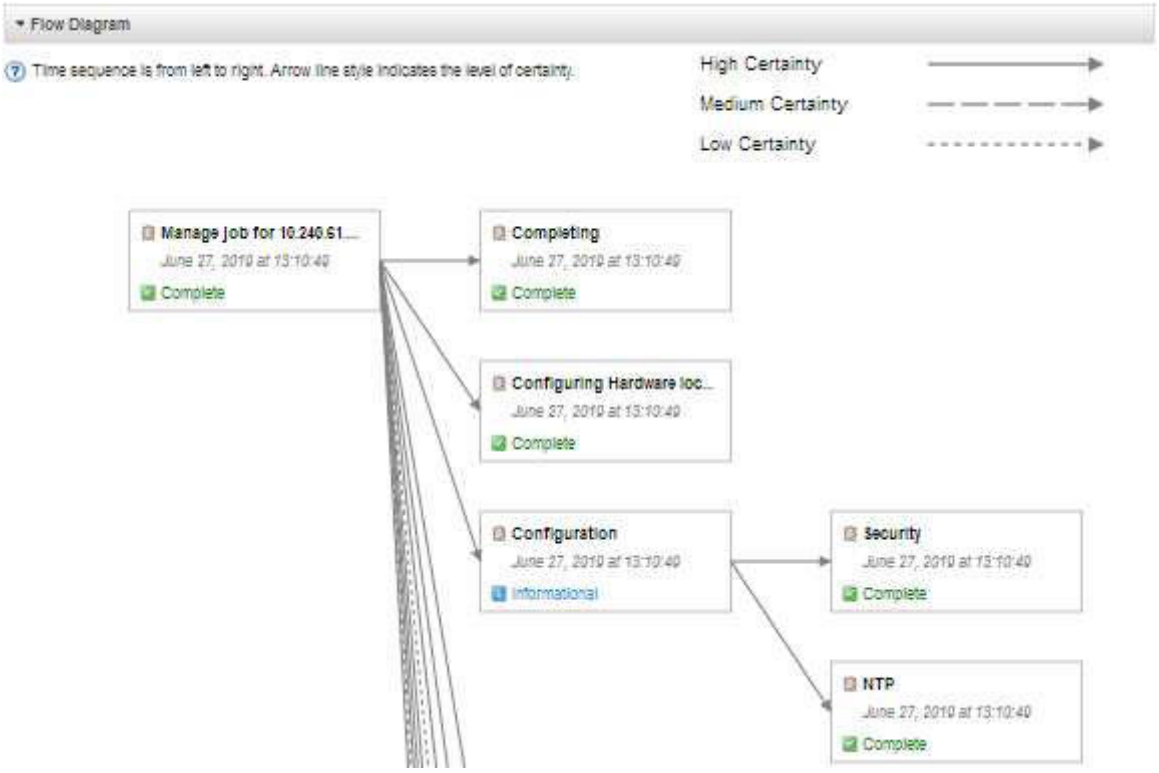
Activity flows are disabled by default. You must enable activity flows before flows can be generated for an activity. You can view flows only for activities that occur when Activity Flow is enabled.

Attention: Activity flows increase memory usage by XClarity Administrator. It is recommended that you do not enable activity flows if memory usage by XClarity Administrator is already high.

About this task

The following example illustrates a flow diagram. The sequence of events flow from left to right. Each node in the flow represents a single activity and includes the activity description, date, and status. You can hover the cursor over the node title to view additional information about the activity.

The style of the lines between the nodes indicates the certainty of relationship between nodes.
- Solid lines represent a high certainty.
- Long-dashed lines represent a medium certainty.
- Short-dashed lines represent a low certainty.



Procedure

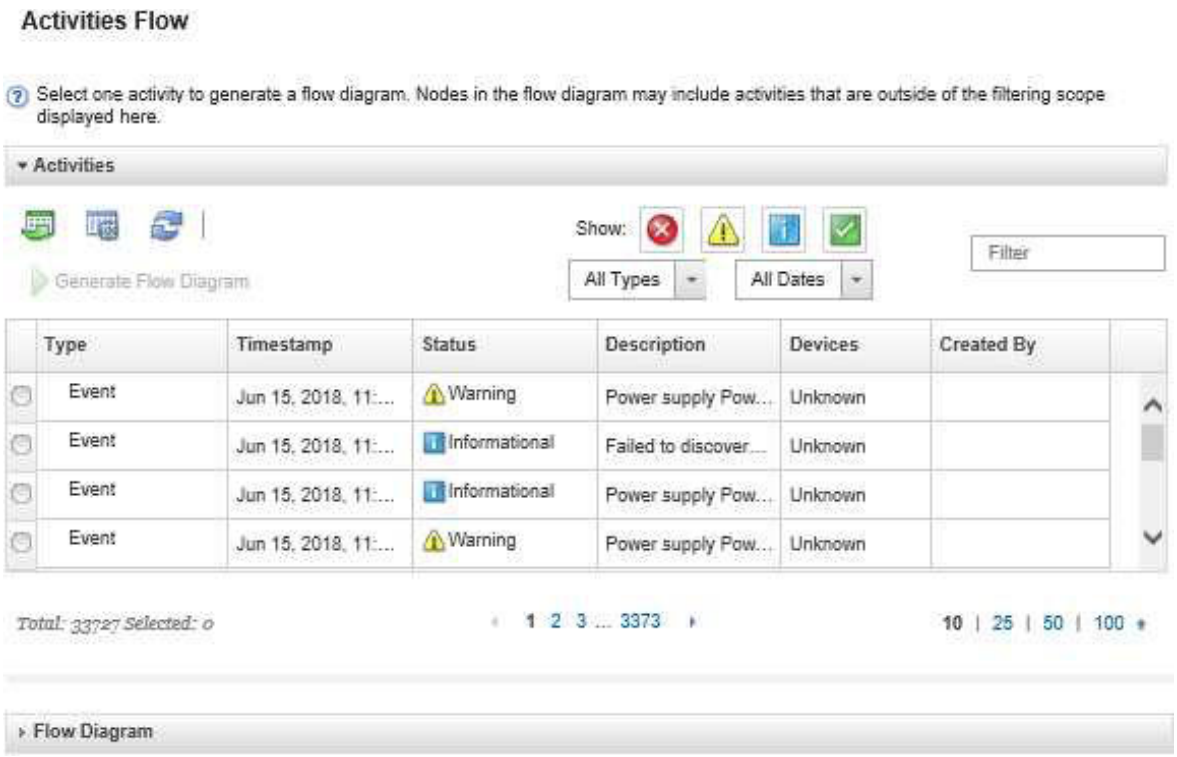
Complete the following steps to view the flow diagram for a specific activity.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Activities flow** to display the Activities flow page

Step 2. Enable activity flows by selecting **Enable Activities Flow**.

Step 3. In the **Activities** section, select the job or event.

You can sort the table columns to make it easier to find specific activities. In addition, you can select a status type, activities type, date, enter a custom filter, or enter text (such as a name or IP address) in the **Filter** field, and to list only those activities that meet the selected criteria



Step 4. Click **Generate Flow Diagram** to display the flow diagram in the **Flow Diagram** section

What to do next

From this page you can perform the following actions:

- View additional information about each activity in the flow diagram by hovering the cursor over the activity.
- Export related flow for the selected activities to a CSV file clicking the **Actions → Export to CSV**.

Chapter 4. Management considerations

There are several alternatives to choose from when managing devices. Depending on the devices being managed, you might need multiple management solutions running at the same time.

For a list of hardware that Lenovo XClarity Administrator can manage, see Supported hardware in the XClarity Administrator online documentation.

Consider the following factors that are related to the management of devices by XClarity Administrator:

- a device can be managed by only one instance of Lenovo XClarity Administrator.
- You cannot use the following management software to manage devices that XClarity Administrator currently manages:
  - Flex System Manager
  - IBM Fabric Manager
  - IBM Systems Director

  However, you can use other management software (such as IBM device Manager or Microsoft Systems Center Operations Manager) in tandem with XClarity Administrator to *monitor* managed devices (see Using another management software in tandem with Lenovo XClarity Administrator).
- You can discover and manage Flex Power Systems compute nodes and Flex System v7000 Storage Node. Using XClarity Administrator, you can view properties and status. Additionally for storage devices, you can also power on and off a storage device, virtually reseat the storage controllers, and launch the management module. However, you must use other management alternatives to take any management-related actions on the devices, such as updating or configuring the device.
  - Use the Flex Power Systems Hardware Management Console to manage Flex Power Systems compute nodes. You can use the Power Systems Hardware Management Console to manage these devices even if you are also managing that chassis in which the devices are installed using XClarity Administrator.
  - Use either the management controller web interface or the command-line interface (CLI) that is provided with the Flex System v7000 Storage Node to manage that device.
  - LAN-over-USB is used when updating firmware. XClarity Administrator automatically enables the LAN-over-USB interface.
  - Intelligent Platform Management Interface (IPMI) is used to perform management operations on System x M4 and ThinkServer servers. Disabling IMPI prevents XClarity Administrator from managing these servers.

Comparison between Flex System Manager and Lenovo XClarity Administrator

Lenovo XClarity Administrator is an optimized hardware manager for Flex System servers. It is also designed to integrate with industry leaders in virtualization management, such as VMware vSphere and Microsoft System Center.

The following table compares the features and functions that are available with the Flex System Manager and with the XClarity Administrator.

© Copyright Lenovo 2015, 2021

Table 3. Functional comparison between Flex System Manager and XClarity Administrator

Feature	Flex System Manager	Lenovo XClarity Administrator	More information
Provide a graphical representation of all supported managed devices.	√	√	
Support failover of the management server		√	XClarity Administrator is a virtual appliance. Therefore, it can leverage VMware High Availability and Hyper-V clustering for failover.
Manage rack and tower servers		√	XClarity Administrator manages Converged, NeXtScale, and System x servers. XClarity Administrator manages the hardware only. It does not require the installation of agents on the rack or tower servers.
Manage Flex System servers	√	√	Both Flex System Manager and XClarity Administrator manage Flex System servers. Flex System Manager requires the use of agents installed in the servers to discover, inventory, and manage the server and installed operating system. XClarity Administrator manages the hardware only. It does not require the installation of agents on the servers.
Manage Flex Power Systems servers	√		If you are managing a chassis that contains both Flex System servers and Flex Power Systems servers: • Use XClarity Administrator to manage the Flex System servers. • Use the Flex Power Systems Hardware Management Console (HMC) to manage the Flex Power Systems servers.For information about managing a Flex Power Systems server from the HMC, see the Flex System p270 Compute Node Planning and Implementation Guide.
Managing RackSwitch switches		√	XClarity Administrator manages RackSwitch switches. XClarity Administrator manages the hardware only. It does not require the installation of agents.
Manage storage devices, such as the Flex System v7000 Storage Node or external devices	√		If a Flex System v7000 Storage Node is installed in a managed chassis, it is displayed in the graphical chassis view, and you can view properties and status for the storage device. However, management of the storage device must be done through the management controller web interface or command-line interface for the storage device.

Table 3. Functional comparison between Flex System Manager and XClarity Administrator (continued)

Feature	Flex System Manager	Lenovo XClarity Administrator	More information
Manage virtual addressing for servers	√	√	On Flex System Manager, you can define virtual address ranges and allocate those virtual addresses to managed servers using IBM Fabric Manager (IFM). You can choose to configure IFM to distribute an address to a server through the CMM (called *push mode*), or to distribute the address directly in response to server request (called *pull mode*). XClarity Administrator uses a different approach to define virtual address through Configuration Patterns. Managed servers pull the virtual-address information from XClarity Administrator.
Update firmware for managed devices	√	√	Flex System Manager updates firmware and device drivers. XClarity Administrator updates the firmware. Devices drivers are updated through your normal operating-system update processes.
Centrally manage configurations for managed chassis and servers.	√	√	Both management applications support the use of configuration patterns to manage configurations for managed chassis and servers.
Deploy operating systems to managed servers	√	√	Both management applications support the deployment of operating systems to managed servers.
Manage virtualized resources	√	√	XClarity Administrator can be used with Lenovo XClarity Integrator options (previously known as Upward Integration Modules or UIMs) to integrate with virtualization managers. For more information about Lenovo XClarity Integrator options, see Lenovo XClarity Integrator online documentation.
Script management functions		√	XClarity Administrator includes both REST APIs and Microsoft PowerShell cmdlets to provide scripting capabilities for management functions. For more information about support for REST APIs and Microsoft PowerShell, see Scripting XClarity Administrator management functions in the XClarity Administrator online documentation.

Migrating from Flex System Manager

If you are planning to manage a chassis with Lenovo XClarity Administrator and that chassis is managed by a Flex System Manager, review these considerations to transition the chassis to XClarity Administrator management successfully.

Depending on your configuration, transitioning from management by Flex System Manager to management by XClarity Administrator might be disruptive to your running workloads. Therefore, consider doing the transition during a maintenance window to minimize downtime with running workloads.

To ensure that XClarity Administrator can manage a chassis that was previously managed by Flex System Manager, complete the following steps:

1. Optional: Prepare the chassis to be removed from management by Flex System Manager.If you are using IBM Fabric Manager (IFM) to virtualize addresses, modify IFM to use push mode to distribute

virtual addresses through the CMM. If you are using IFM in pull mode and Flex System Manager is powered off, the virtual addresses will no longer be available after the next restart of the compute node.

Note: IFM supports the concept of a standby node. In the event of a hardware failure, IFM assigns the virtual address of the failed compute node to the standby node so that it can automatically take over the workload from the failed node. XClarity Administrator does not support the concept of a standby node. Therefore, if you have implemented the standby node, you must devise a different strategy for continuous availability when there is a failed compute node.

Remember that if virtual addresses are changed, you must adjust infrastructure services as well. For example:

- If the World Wide Port Name (WWPN) is changed for a compute node, adjust SAN zoning and LUN mapping.
- If the MAC address for a port is changed, adjust the MAC-to-IP address binding in the DHCP server or clustering software.
- IFM can configure a virtual boot-target WWN. If you do not migrate correctly, you might lose the ability to start our operating system.

2. Remove the chassis from management by the Flex System Manager.
3. Manage the chassis from XClarity Administrator. For information about managing a chassis, see Managing chassis in the XClarity Administrator online documentation.
4. Remove any agents that were installed on devices that are managed by the Flex System Manager. The XClarity Administrator implements an agentless management approach. Therefore, you do not need to install agents on managed compute nodes. Although the installed agents have no effect on XClarity Administrator management functions, you can choose to remove those agents and reclaim the space on the compute node.

Using another management software in tandem with Lenovo XClarity Administrator

You can use other management software (such as IBM device Manager or Microsoft Systems Center Operations Manager) in tandem with Lenovo XClarity Administrator to *monitor* devices that XClarity Administrator manages.

Attention: Extra care must be taken when using multiple management tools to manage your devices to prevent unforeseen conflicts. For example, submitting power-state changes using another tool might conflict with configuration or update jobs that are running in XClarity Administrator.

Flex System devices

If you intend to use another management software to monitor your managed devices, and if that management software uses SNMPv3 or IPMI communication, you must prepare your environment by performing the following steps for each managed CMM:

1. Log in to the management controller web interface for the chassis using the `RECOVERY_ID` user name and password.
2. If the security policy is set to **Secure**, change the user authentication method.
   a. Click **Mgt Module Management → User Accounts**.
   b. Click the **Accounts** tab.
   c. Click **Global login settings**.
   d. Click the **General** tab.
   e. Select **External first, then local authentication** for the user authentication method.
   f. Click **OK**.
3. Create a new local user with the correct SNMP or IPMI settings from the management controller web interface.

4. If the security policy is set to **Secure**, log out and then log in to the management controller web interface using the new user name and password. When prompted, change the password for the new user.

You can now use the new user as an active SNMP or IPMI user.

Note: If you unmanage and then manage the chassis again, this new user account becomes locked and disabled. In this case, repeat these steps to create a new user account.

ThinkSystem, ThinkServer and System x devices

If you intend to use another management software to monitor your managed devices, create a new local user with the correct SNMP or IPMI settings from the IMM interface. Ensure that you grant SNMP or IPMI privileges, depending on the your needs.

Chapter 5. Managing resource groups

You can use resource group in Lenovo XClarity Administrator to create logical set of managed devices that you can view collectively and act on.

Learn more: XClarity Administrator: Resource groups

About this task

There are three types of resource groups:

- **Static**. Customized group of specific devices.
- **Dynamic**. Rule-based group of devices (for example, all servers of a specific type). This group contains a dynamic list of devices based on a set of inventory properties.

Actions cannot be performed on a resource group; however, you can select all devices in the group, and perform actions collectively on all selected devices.

Viewing the status of devices in a resource group

You can view the status of all managed devices in a resource group.

About this task

The following status icons are used to indicate the overall health of all devices the resource group. The overall health of the group indicates the device with the highest severity in the group.

- **Critical** icon ( )
- **Warning** icon ( )
- **Normal** icon ( )

Procedure

Complete the following steps to view the status of devices in a resource group.

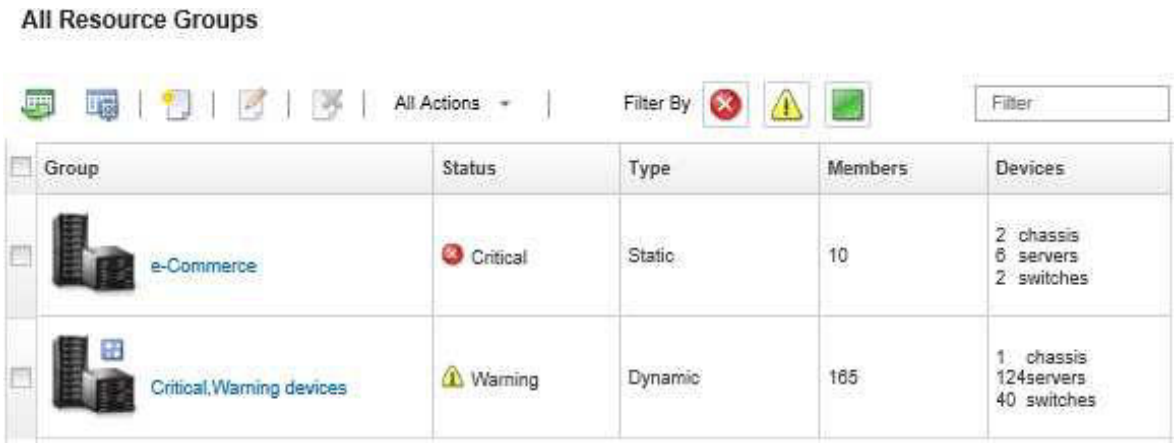
Step 1. From the Lenovo XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of all managed devices and other resources, including resource groups.

© Copyright Lenovo 2015, 2021



Step 2. From the XClarity Administrator menu bar, click **Hardware → Resource Groups**. The All Resource Groups page is displayed.

The All Resource Groups page lists each resource group, including the name of the group, the number of managed devices that are in the group, and the status of the device with the highest severity in the group.



From this page, you can perform the following actions:

- Create a new resource group (see Creating a dynamic resource group and Creating a static resource group)
- Edit group membership by selecting a group and clicking the **Edit** icon ( ).
- Edit group properties by selecting the group and clicking **All Actions → Edit properties**.
- Remove a resource group by selecting a group and clicking the **Delete** icon ( ).

Note: Removing a group only removes the group definition. It does not affect the devices in the group.

- Export detailed information about all devices in one or more resource groups to a CSV file clicking the **Export** icon ( ).

Step 3. From the All Resource Groups page, click the name in the **Groups** column to display the list of devices in that group.



From this page, you can perform the following actions:

- Add or remove devices in a static resource group by clicking the **Edit** icon ( ).
- Display detailed information about a specific device in the resource group by clicking the device name in the **Device Name** column.
- Export detailed information about all devices in one or more resource groups to a CSV file clicking the **Export** icon ( ).

Viewing the members of a resource group

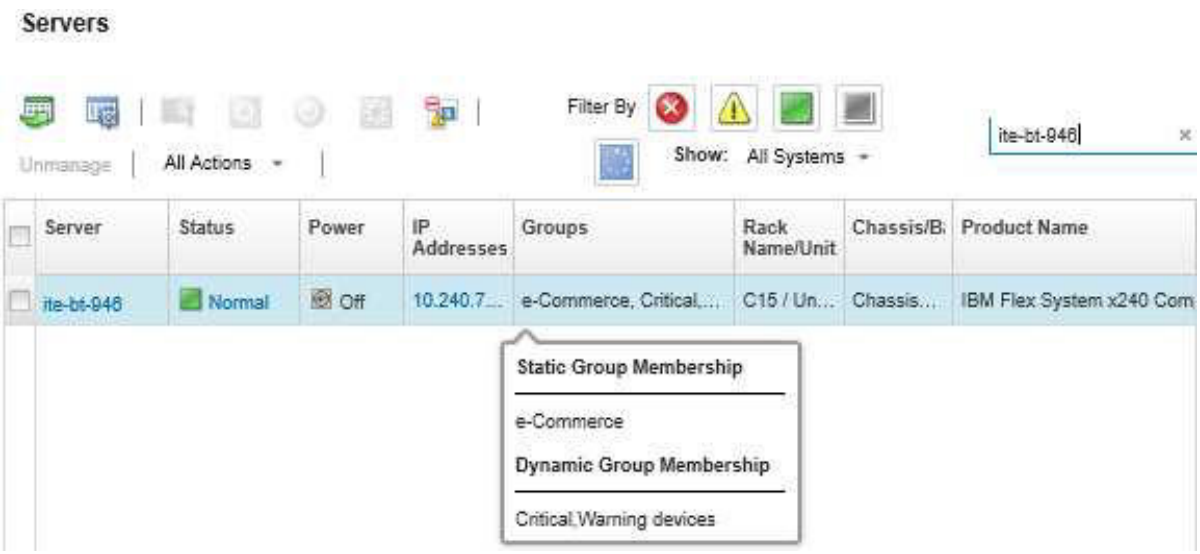
You can view detailed information about the resource groups including group members.

Procedure

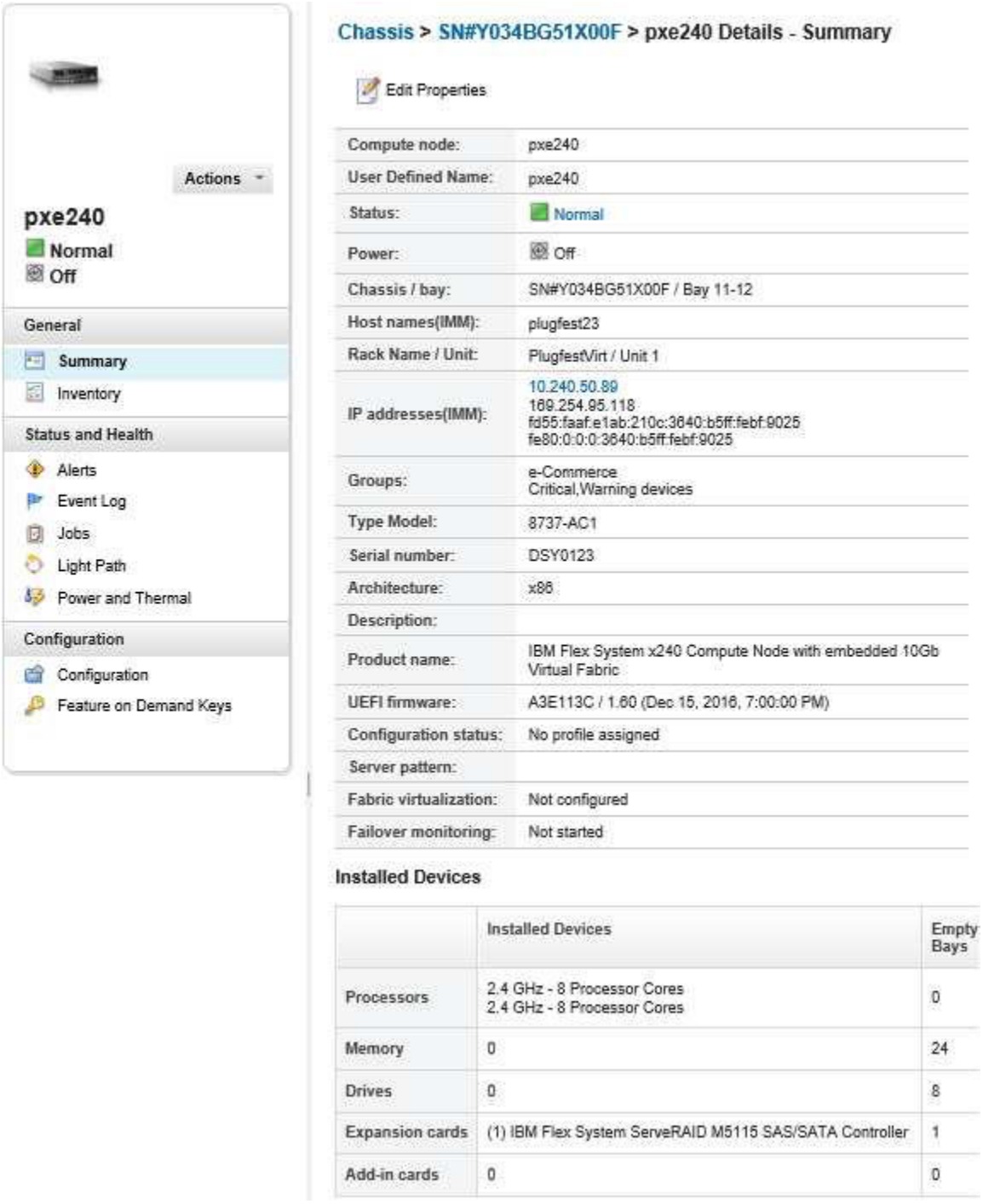
Complete the following steps to view group membership.

- To view all groups of which a device is a member.
  1. From the Lenovo XClarity Administrator menu bar, click **Hardware** and then click the device type to the display the all-devices page.

     Hover over the group lists in the **Groups** column to list the groups of which the device is a member.

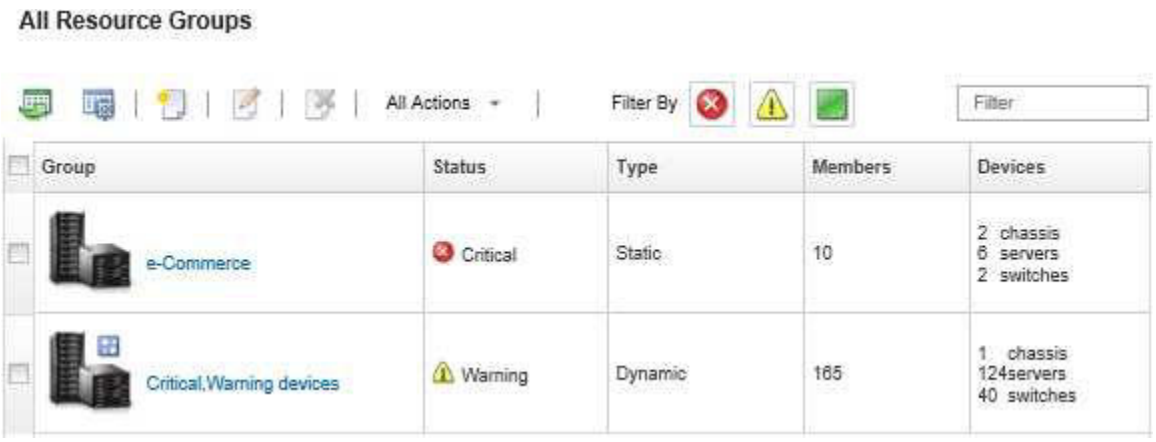


2. Click the link for the device name in the first column. The summary page for that device is displayed, including a list of resource groups of which the device is a member.



- To view the members of a group.
  1. From the XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of the all managed devices and other resources, including racks.
  2. From the XClarity Administrator menu bar, click **Hardware → Groups**. The Resource Groups page is displayed.

     This page lists the total number of members and the number of member of each device type in the group.



3. From the All Resource Groups page, click the name in the **Groups** column to display the resource group details.

   This page lists each device that is a member of the resource group.



Creating a dynamic resource group

You can create a resource group for a dynamic set of managed devices based on a set of criteria.

About this task

You can create a dynamic resource group using one or more of the following criteria for each device type.

Criteria	Chassis	Dense chassis	Servers	Flex System switch	RackS-witch switch	Storage device
Add-in card name			√ (except ThinkServ-er)			
Contact	√		√		√	√
Description	√	√	√		√	√
Fully-qualified domain name	√		√			
Hostname	√		√	√	√	

Criteria	Chassis	Dense chassis	Servers	Flex System switch	RackS-witch switch	Storage device
IPv4 address*	√		√	√	√	√
IPv6 address	√		√	√	√	
Location	√	√	√		√	√
Machine type	√		√	√	√	√
Model	√		√	√	√	√
Overall health state	√		√	√	√	√
Processor cores			√			
Product name	√		√	√	√	√
Rack	√	√	√		√	√
Room	√	√	√		√	√
User-defined name	√	√ (v2.1.0 and later)	√	√	√	√

Note: For IPv4 addresses, you can specify a single address or a range of addresses, separated by dash or using an asterisk as wildcard (for example, `192.0.2.5 - 192.0.2.46` or `192.0.2.*`).

Procedure

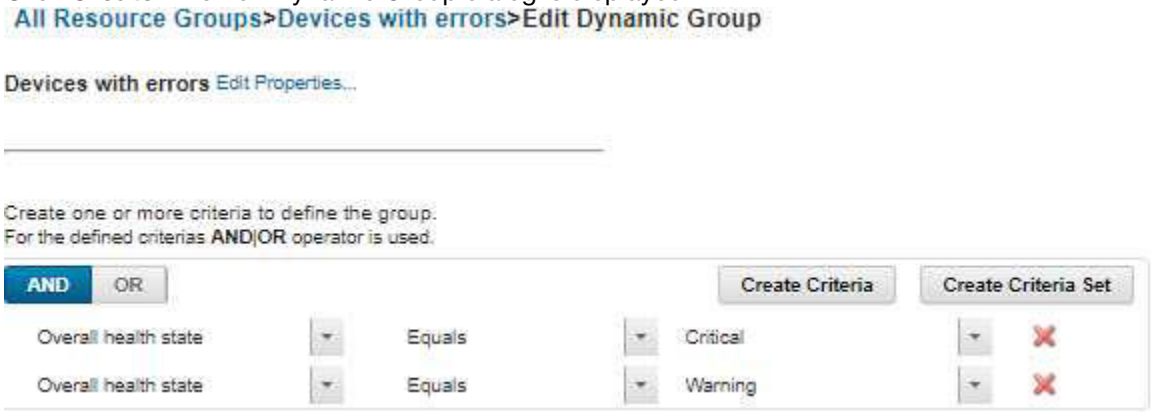
To create and populate a dynamic resource group, complete the following steps

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Resource Groups**. The All Resource Groups page is displayed.

Step 2. Click the **Create** icon ( ) to create an empty group. The Create Empty Group dialog is displayed.

Step 3. Select **Dynamic Group** to group of devices based on a set of criteria.

Step 4. Click **Create**. The Edit Dynamic Group dialog is displayed.



Step 5. Add criteria for this dynamic group.

- Select the operator to use for the group set. This can be one of the following values:
  - **AND**. Members must satisfy all specified values.
  - **OR**. Members must satisfy one or more of the specified values.
- Click **Create Criteria** to add and a new criteria rule to the set.
- Click **Create Criteria Set** to add a subset of criteria rules.

Note: New criteria and criteria sets are always added to the bottom of the list.

Step 6. Click **Apply** to save the group criteria and create the group, or click **Preview** to see what devices are included in the group using the current criteria without creating the group.

What to do next

- You can see which resource groups a device belongs from the **Groups** column on the all-devices pages and the device summary pages.
- You can modify the criteria for the dynamic group by selecting the resource group and clicking the **Edit** icon ( ).
- You can modify resource-group properties by clicking **All Actions → Edit properties**.

Creating a static resource group

You can create a resource group that contains a customized set of managed devices.

Procedure

To create and populate a static resource group, complete the following steps.

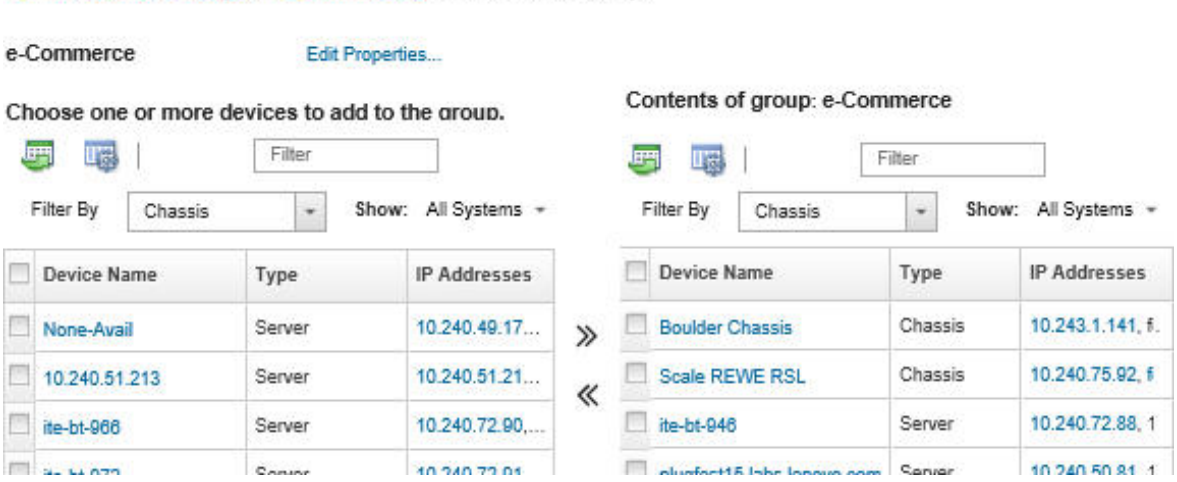
Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Resource Groups**. The Resource Groups page is displayed.

Step 2. Click the **Create** icon ( ) to create an empty group. The Create Empty Group dialog is displayed.

Step 3. Specify the group name and optional description.

Step 4. Select **Static Group** to create a group of explicitly defined devices.

Step 5. Click **Create**. The Edit Static Group page is displayed.



Step 6. Select the devices that you want to add to the group from the **All available devices not in group** list, and click the **Add** icon (») to move the selected devices to the **Contents of group** list.

Notes:

- You can sort the lists to make it easier to find specific devices by clicking on the column headers. In addition, you can select a device type from the **Filter By** drop-down list, select a chassis from the drop-down list, or enter text (such as a name or IP address) in the **Filter** field to list only those devices that meet the selected criteria
- If you choose to move a chassis to the group, the devices in the chassis are not automatically added to the group. To add all chassis components to the group, select **Chassis →** *<chassis_*

name> in the **Show** drop-down menu to list all components in the specified chassis, select the checkbox next to the Device Name column heading to select all devices, and then click the **Add** icon (») to move the selected devices to the **Contents of group** list.

What to do next

- You can see which resource groups a device belongs from the **Groups** column on the all-devices pages and the device summary pages.
- You can add or remove a device from a static resource group from the all-devices pages and the device details pages by clicking **All Actions → Groups → Add to Group** or **All Actions → Groups → Remove from Group**.

  Note: You can add and remove devices only from static resource groups. You cannot remove them from dynamic groups.
- You can modify resource-group properties by clicking **All Actions → Edit properties**.

Removing a resource group

You can remove a resource group from Lenovo XClarity Administrator.

About this task

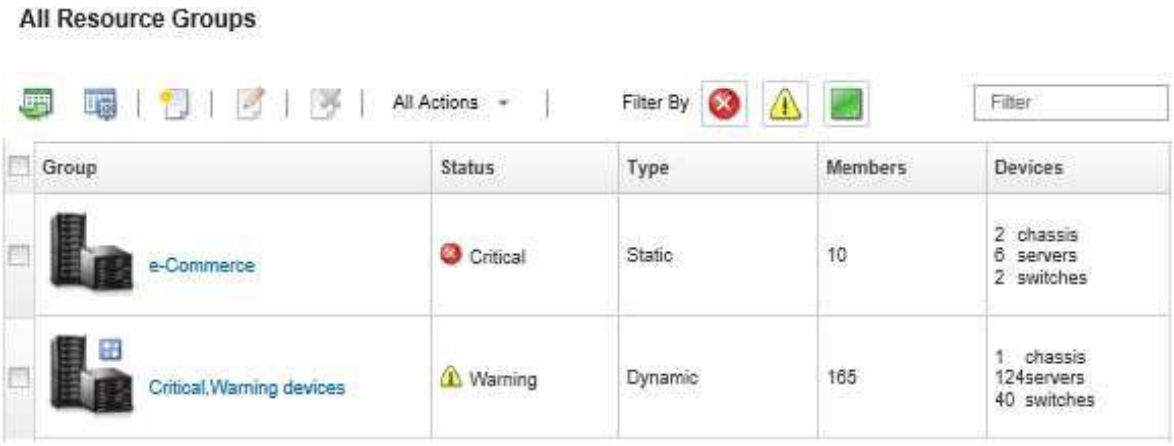
Deleting a group only deletes the group definition. It does not affect the devices in that group.

Procedure

Complete the following steps to remove a resource group.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Resource Groups**. The All Resource Groups page is displayed.

The All Resource Groups page lists each resource group, including the name of the group, the number of managed devices that are in the group, and the status of the device with the highest severity in the group.



Step 2. Select the resource group to be removed.

Step 3. Click the **Delete** icon (✖).

Step 4. Click **Delete**.

Modifying resource-group properties

You can modify the properties for a specific resource group.

Procedure

Complete the following steps to modify the resource-group properties

Step 1. From the XClarity Administrator menu bar, click **Hardware → Resource Groups** to display the All Resource Groups page

Step 2. Select the resource group to be updated.

Step 3. Click **All Actions → Edit Properties** to display the Edit Group Properties dialog.



Step 4. Change the following information, as needed.
- Group name
- Description

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface

Chapter 6. Managing racks

You can use racks in Lenovo XClarity Administrator to group your managed devices to reflect the physical rack setup in your datacenter.

Before you begin

After moving a node from one chassis to another, wait 5 to 10 minutes before attempting to edit the racks in XClarity Administrator that contains the chassis.

When you move a device out of a rack, the rack name and lowest rack unit values are cleared in device inventory. The room and location values are not cleared.

About this task

This procedure describes how to create and populate a single rack with managed devices and fillers interactively.

If you must add many devices to racks, or edit many racks, consider using a spreadsheet to perform a bulk import or implementing a PowerShell script to automate the task. For more information about using the bulk-import, see Managing chassis and Managing servers. For information about PowerShell scripts, see PowerShell (LXCAPSTool) toolkit in the XClarity Administrator online documentation.

XClarity Administrator recognizes rack properties that are defined in a manageable device. When you manage that device, XClarity Administrator sets the system properties for that device and updates the rack view. If the rack does not exist in XClarity Administrator, a new rack is created and the device is added to the new rack.

Notes:

- System x3500 M5 servers, NeXtScale nx360 M5 servers, ThinkServer SD350 servers, and tower servers are not supported in rack view.
- System x3850 X5 scalable-complex systems, you must add each node (server) to the rack individually.
- Demo hardware is not persistent in rack views when XClarity Administrator is restarted.

Procedure

To create and populate racks, complete the following steps.

- Create and populate a single rack with managed devices.
  1. From the XClarity Administrator menu bar, click **Hardware → Racks**. The All Racks page is displayed.

     The All Racks page shows each rack as a thumbnail image with the name of the rack, the number of managed devices that are in the rack, and the status of the device with the highest severity.

     Notes: You can filter the racks by severity by clicking the following icons in the toolbar. You can also enter a rack name in the **Filter** field to further filter the racks that are displayed.
     - **Critical alerts** icon ()
     - **Warning alerts** icon ()
     - **Normal alerts** icon ()

© Copyright Lenovo 2015, 2021

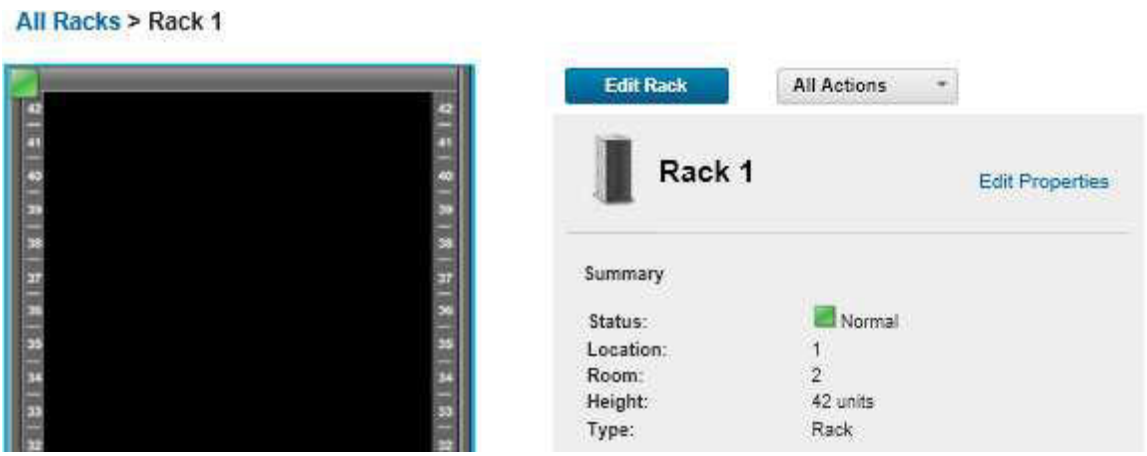


2. Click the **Create** icon ( ) to create an empty rack. The Create Empty Rack dialog is displayed.
3. Fill in the dialog with the rack name, height, location, and room.

   Notes:

   – The rack name can include only the upper and lower case letters, numbers, and the following special characters: period (.), dash (-), and underscore (_).

   – The location can be a maximum of 23 characters.
4. Click **Create**. A thumbnail image for the new rack is added to the All Racks page.
5. Double-click the thumbnail image for the rack. The rack-view page is displayed with an empty rack image and properties for that rack.



6. Click **Edit Rack** to display the Edit Rack page.



7. Add all appropriate managed devices and fillers to the graphical view:

   Note: Only managed devices that are in an Online state can be added to the rack.

   - Click the **Chassis** tab to view a list of managed chassis that have not been added to a rack. Drag and drop a managed chassis to the desired location in the rack to add the chassis to the rack.
   - Click the **Server Enclosures** tab to view a list of managed rack-servers and multi-node server enclosures that have not been added to a rack. Drag and drop a rack server or server enclosures into the rack at the desired location to add the rack server to the rack.
   - Click the **RackSwitch** tab to view a list of managed RackSwitch switches that have not been added to a rack. Drag and drop a RackSwitch switch into the rack at the desired location to add the switch to the rack.
   - Click the **Storage** tab to view a list of various storage devices. Drag and drop the appropriate storage device into the rack at the desired location to add the storage device to the rack.
   - Click the **Fillers** tab to view a list of various fillers. Drag and drop the appropriate filler into the rack at the desired location to add the filler to the rack.

     A *filler* is any device that is in the rack that is not managed by XClarity Administrator. The following fillers are available:
     - Generic fillers
     - Generic rack switches
     - Lenovo Storage or Nimble storage controllers and enclosures
     - Partner storage controllers and enclosures (such as IBM, NetApp, and EMC)

   - The location, room, rack, and lowest rack unit properties are updated for the device when you add or remove devices from a rack.
   - You can sort the list of devices on each tab by using the **View by** drop-down list. In addition, you can enter text (such as a name or IP address) in the **Filter** field to further filter the devices that are displayed.
   - You can remove managed devices and fillers from the rack by dragging and dropping the objects outside the rack.

8. Click **Save** to save the rack configuration.

   The configuration process might take several minutes to complete. During configuration, the rack and location information is pushed to the CMM or baseboard management controller for the managed devices.

9. Customize the fillers that you added to the rack by clicking the filler and then clicking **Edit Properties**. In the Edit Properties dialog, you can specify a name, lowest rack unit (LRU), and a URL to use to launch the management user interface for that device.

   Tip: After the rack configuration is saved, you can launch the management user interface for a filler by clicking the filler in the rack and then clicking the **Launch URL** link.

- Create and populate racks using a bulk-import file.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Click **Bulk Import**. The Bulk Import wizard is displayed.

  3. Click the **in Excel** or **in CSV** link on the Import Data File page to download the template bulk-import file in Excel or CSV format.

     Important: The template file might change from one release to the next. Ensure that you always use the latest template.

  4. Fill in the data worksheet in the template file, and save the file in CSV format.

     Tip: The Excel template includes a **Data** worksheet and a **Readme** worksheet. Use the **Data** worksheet to fill in your device data. The **Readme** worksheet provides information about how to fill in each field on the **Data** worksheet (including which fields are required) and sample data.

     Important:

     – Devices are managed in the order that is listed in the bulk-import file.
     – XClarity Administrator uses rack-assignment information that is defined in the device configuration when the device is managed. If you change the rack assignment in XClarity Administrator, XClarity Administrator updates the device configuration. If you update the device configuration after the device is managed, the changes are reflected in XClarity Administrator.
     – It is recommended but not required to explicitly create a rack in the spreadsheet before assigning the rack to a device. If a rack is not explicitly defined and the rack does not already exist in XClarity Administrator, the rack-assignment information that is specified for a device is used to create the rack with a default height of 52U.

       If you want to use another height for the rack, you must explicitly define the rack in the spreadsheet before assigning it to a device.

     To define your racks in the bulk-import file, complete the following required columns.
     – (Columns A) Specify “rack” for the device type.
     – (Columns V) Specify the rack name.
     – (Column X) Specify rack height. The following rack heights are supported: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U, and 52U.

The following figure shows an example bulk-import file with racks defined.

A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

Note: You can use the same bulk-import file to manage devices and add those devices to a rack (see Managing systems in the Lenovo XClarity Administrator online documentation).

5. From the Bulk Import wizard, enter the name of the CSV file to upload file for processing. You can click **Browse** to help you find the file.
6. Click **Upload** to upload and validate the file.
7. Click **Next** to display the Input Summary page with a list of rack and other devices to be managed, and review the summary of racks and other devices that you want to manage.
8. Click **Next** to display the Device Credentials page. Click on each tab, and optionally specify global settings and credentials to use for all devices of a specific type. The devices that will use the global settings and credentials are listed on right side of each tab.
9. Click **Manage**. The Monitoring Results page is displayed with information about the management status of each device in the bulk-import file.

   A job is created for the management process. If you close the Bulk-Import wizard, the management process continues running in the background. You can monitor the status of the management process from the jobs log. For information about the jobs log, see “Monitoring jobs” on page 154.

What to do next

You can change the rack numbering order preference (see Setting inventory preferences).

Viewing the status of devices in a rack

For each rack, you can view the status of all managed devices in the rack.

Procedure

Complete the one or more of the following action to view the status of all devices in a rack.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of the all managed devices and other resources, including racks.



Step 2. From the XClarity Administrator menu bar, click **Hardware → Racks**. The Racks page is displayed.

The Racks page shows each rack as a thumbnail image with the name of the rack, the number of managed devices that are in the rack, and the status of the device with the highest severity.

Notes: You can sort the list by rack name, number of devices in the rack, or by severity to make it easier to find specific racks. Sorting is ordered from left to right, top to bottom. In addition, you can filter the racks by severity by clicking on the following icons in the toolbar or enter a rack name in the **Filter** field to further filter the racks that are displayed.

- **Critical alerts** icon ( )
- **Warning alerts** icon ( )
- **Normal alerts** icon ( )



Step 3. From the All Racks page, click the rack name or double-click a rack thumbnail to display the graphical view and properties for that rack.

The *rack view* is a graphical view of the front rack that shows each device in the rack, including chassis, rack servers, top-of-rack switches, and fillers. A status icon on each device indicates the current status of that device.

From this page, you can perform the following actions:

- Add or remove devices in the rack by clicking **Edit Rack**.

  Note: When you change the components in the rack, there might be a short delay before the information appears in the XClarity Administrator interface.
- Modify device and filter properties (including the name, location, and URL to launch the management web interface) by clicking the device or filler, and then clicking the **Edit Properties** in the device summary pane.
- View the management controller web interface for a device or filler by clicking the device or filler, and then clicking the **Launch URL** link in the device summary pane.



Step 4. Display a summary or detailed status for a device or component:

a. Click a device or component in the rack to display the status summary and properties and status for the device or component.

b. Double-click a device to display the device details page.

Procedure

You can change the rack numbering order preference (see Setting inventory preferences).

Removing a rack

You can remove a rack from Lenovo XClarity Administrator.

Procedure

Complete the following steps to remove a rack.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Racks**. The All Racks page is displayed.

The All Racks page shows each rack as a thumbnail image with the name of the rack, the number of managed devices that are in the rack, and the status of the device with the highest severity.

Notes: You can sort the list by rack name, number of devices in the rack, or by severity to make it easier to find specific racks. Sorting is ordered from left to right, top to bottom. In addition, you can filter the racks by severity by clicking on the following icons in the toolbar or enter a rack name in the **Filter** field to further filter the racks that are displayed.

- **Critical alerts** icon ( )
- **Warning alerts** icon ( )
- **Normal alerts** icon ( )



Step 2. Select the thumbnail for the rack to be removed.

Step 3. Click the **Remove** icon ( ).

Step 4. Click **Remove**.

Results

The thumbnail for the rack is removed from the All Racks page, and all devices that were in the rack are now available for inclusion in other rack on the Edit Racks page.

Chapter 7. Managing chassis

Lenovo XClarity Administrator can manage several types of systems, including the Flex System chassis.

Learn more: XClarity Administrator: Discovery

Before you begin

Note: Chassis components (such as CMMs, Flex compute nodes, and Flex switches) are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed chassis components separate from the chassis.

Before managing chassis, ensure that the following conditions are met:

- Review the management considerations before managing a device. For information, see Management considerations in the XClarity Administrator online documentation.
- Certain ports must be available to communicate with the CMM for the chassis being managed. Ensure that these ports are available before you attempt to manage a chassis. For more information about ports, see Port availability in the XClarity Administrator online documentation.
- Ensure that the minimum required firmware is installed on each chassis that you want to manage using XClarity Administrator. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.
- Ensure that the **Number of simultaneous active sessions for LDAP users** setting in the CMM is set to 0 (zero) for the chassis. You can verify this setting from the CMM web interface by clicking **Mgmt Module Management → User Accounts**, click **Global Login Settings**, and then click the **General** tab.
- Ensure that there are at least three TCP command-mode sessions set for out-of-band communication with the CMM. For information about setting the number of sessions, see tcpcmdmode command in the CMM online documentation.
- To discover a chassis that is on a *different* subnet from XClarity Administrator, ensure that one of the following conditions are met:
  - Ensure that you enable multicast SLP forwarding on the top-of-rack switches, as well as the routers in your environment. See the documentation that was provided with your specific switch or router to determine whether multicast SLP forwarding is enabled and to find procedures to enable it if it is disabled.
  - If SLP is disabled on the endpoint or on the network, you can use DNS discovery method instead by manually adding a service record (SRV record) to your domain name server (DNS), for XClarity Administrator for example.

    ```
    _lxca._tcp.labs.lenovo.com      service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```

    Then, enable DNS discovery on the CMM from the management web interface, by clicking **Mgt Module Management → Network Protocol**, clicking the **DNS** tab, and selecting **Use DNS to discover Lenovo XClarity Administrator**.

    Notes:

    - The CMM must be running a firmware level dated May 2017 to support automatic discovery using DNS.
    - If there are multiple XClarity Administrator instances in your environment, the chassis is discovered only by the instance that is the first to respond to the discovery request. The chassis is not discovered by all instances.

© Copyright Lenovo 2015, 2021

Consider implementing either IPv4 *or* IPv6 addresses for all CMMs and Flex switches that are managed by XClarity Administrator. If you implement IPv4 for some CMMs and Flex switches and IPv6 for others, some events might not be received in the audit log (or as audit traps).

Attention: If you intend to manage CMMs that are running a firmware level of Flex stack release 1.3.2.1 2PET12K through 2PET12Q, that have been running more than three weeks, and that are in a dual-CMM configuration, you must virtually reseat the CMMs before updating firmware using XClarity Administrator.

Important: If you intend to use other management software in addition to Lenovo XClarity Administrator to monitor your chassis, and if that management software uses SNMPv3 communication, you must first create a local CMM user ID that is configured with the appropriate SNMPv3 information and then log in to the CMM using that user ID and change the password. For more information, see Using management software other than the XClarity Administrator in the XClarity Administrator online documentation.

About this task

XClarity Administrator can automatically discover chassis in your environment by probing for manageable systems that are on the same IP subnet as XClarity Administrator. To discover chassis that are in other subnets, specify an IP address or range of IP addresses, or import information from a spreadsheet.

After the chassis are managed by XClarity Administrator, XClarity Administrator polls each managed chassis periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed chassis and perform management action (such as configuring system information, network setting, and failover). For chassis that are in protected mode, management actions are disabled.

Chassis are managed using *XClarity Administrator managed authentication*.

By default, devices are managed using XClarity Administrator managed authentication to log in to the devices. When managing rack servers and Lenovo chassis, you can choose to use local authentication or managed authentication to log in to the devices.

- When *local authentication* is used for rack servers, Lenovo chassis, and Lenovo rack switches, XClarity Administrator uses a stored credential to authenticate to the device. The *stored credential* can be an active user account on the device or a user account in an Active Directory server.

  You must create a stored credential in XClarity Administrator that matches an active user account on the device or a user account in an Active Directory server before managing the device using local authentication (see Managing stored credentials in the XClarity Administrator online documentation).

  Notes:

  – RackSwitch devices support only stored credentials for authentication. XClarity Administrator user credentials are not supported.
- Using *managed authentication* allows you to manage and monitor multiple devices using credentials in the XClarity Administrator authentication server instead of local credentials. When managed authentication is used for a device (other than ThinkServer servers, System x M4 servers, and switches), XClarity Administrator configures the device and its installed components to use the XClarity Administrator authentication server for centralized management.

  – When managed authentication is enabled, you can manage devices using either manually-entered or stored credentials (see Managing user accounts and in the XClarity Administrator online documentation).

    The stored credential is used only until XClarity Administrator configures the LDAP settings on the device. After that, any change to the stored credential has no impact the management or monitoring of that device.

    Note: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.

- If a local or external LDAP server is used as the XClarity Administrator authentication server, user accounts that are defined in the authentication server are used to log in to XClarity Administrator, CMMs and baseboard management controllers in the XClarity Administrator domain. Local CMM and management controller user accounts are disabled.
- If an SAML 2.0 identity provider is used as the XClarity Administrator authentication server, SAML accounts are not accessible to managed devices. However, when using an SAML identity provider and an LDAP server together, if the identity provider uses accounts that exist in the LDAP server, LDAP user accounts can be used to log into the managed devices while the more advanced authentication methods that are provided by SAML 2.0 (such as multifactor authentication and single sign-on) can be used to log into XClarity Administrator.
- When managed authentication is enabled for ThinkSystem SR635 and SR655 servers:
  - Baseboard management-controller firmware supports up to five LDAP user roles. XClarity Administrator adds these LDAP user roles to the servers during management: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin**, and **lxc-os-admin**.

    Users must be assigned to at least one of the specified LDAP user roles to communicate with ThinkSystem SR635 and SR655 servers.
  - Management-controller firmware does not support LDAP users with the same username as local user of the sever.
- For ThinkServer and System x M4 servers, the XClarity Administrator authentication server is not used. Instead, an IPMI account is created on the device with the prefix “LXCA_” followed by a random string. (The existing local IPMI user accounts are not disabled.) When you unmanage a ThinkServer server, the “LXCA_” user account is disabled, and the prefix “LXCA_” is replaced with the prefix “DISABLED_”. To determine whether a ThinkServer server is managed by another instance, XClarity Administrator checks for IPMI accounts with the prefix “LXCA_”. If you choose to force management of a managed ThinkServer server, all the IPMI accounts on the device with the “LXCA_” prefix are disabled and renamed. Consider manually clearing IPMI accounts that are no longer used.

  In XClarity Administrator v2.4 and later, if you use manually-entered credentials, XClarity Administrator automatically creates a stored credential and uses that stored credential to manage the device.

  Notes: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.
  - Each time you manage a device using manually-entered credentials, a new stored credential is created for that device, even if another stored credential was created for that device during a previous management process.
  - When you unmanage a device, XClarity Administrator does not delete stored credentials there were automatically created for that device during the management process.

A device can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device on the initial XClarity Administrator, and then manage it with the new XClarity Administrator. If an error occurs during the unmanagement process, you can select the **Force management** option during management on the new XClarity Administrator.

Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a device is already managed by another manager until after it attempts to manage the device.

During the management process, XClarity Administrator performs the following actions:

- Logs in to the chassis using the provided credentials.

- Collects inventory for all components in each chassis, such as the CMM, compute nodes, storage devices, and Flex switches.

  Note: Some inventory data is collected after the management process completes. The chassis is in the Pending status until all inventory data is collected. You cannot perform certain tasks on a managed device (such as deploying a server pattern) until all inventory data is collected for that device and the chassis is no longer in the Pending state.
- Configures the settings for the NTP server so that all managed devices use the NTP server from XClarity Administrator.
- Assigns the last-edited firmware-compliance policy to the chassis.
- For Lenovo Flex devices, optionally configures the devices firewall rules so that incoming requests are accepted from only XClarity Administrator.
- Exchanges security certificates with the CMM, copying the CMM security certificate into the XClarity Administrator trust store and sending the XClarity Administrator CA security certificate to the CMM. The CMM loads the certificate into the CMM trust store and distributes it to the compute-node service processors for inclusion in their trust stores.
- Configures managed authentication. The settings for the CMM LDAP client are changed to use XClarity Administrator as the authentication server, and the Global Login Settings in the CMM are changed to **External Authentication Server Only**. For more information about managed authentication, see Managing the authentication server.
- Creates the recovery user account (`RECOVERY_ID`). For more information about the `RECOVERY_ID` account, see Managing the authentication server.

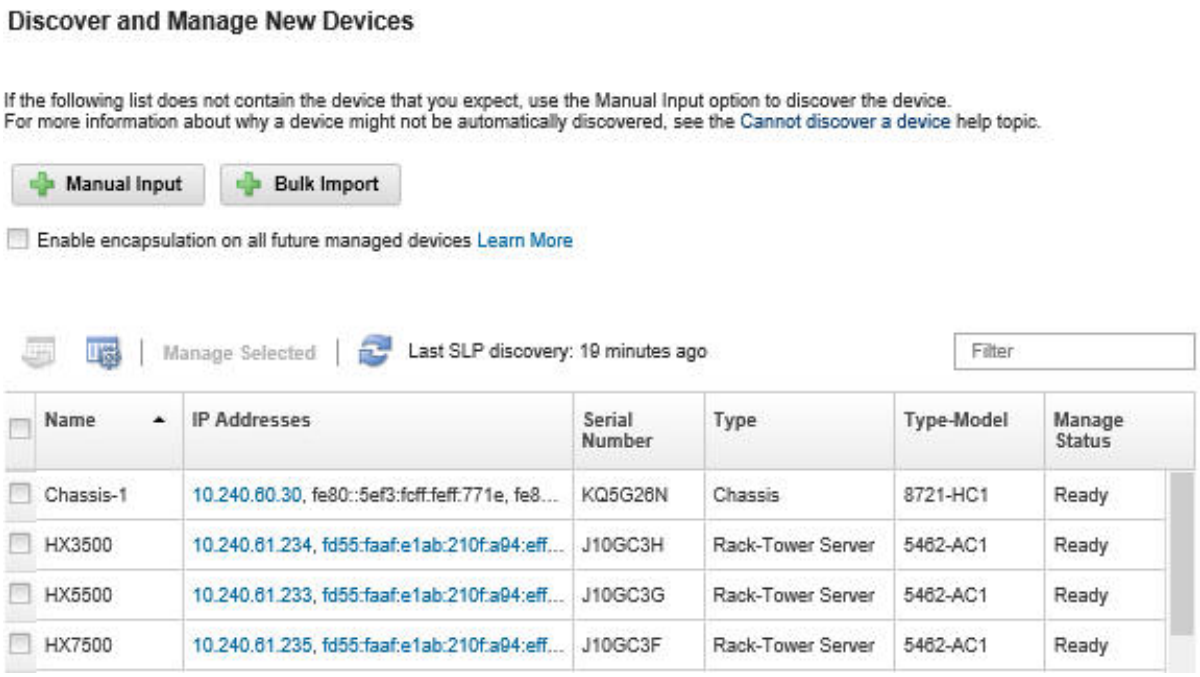
Attention: When managing a chassis, the XClarity Administrator changes the maximum number of simultaneous Secure TCP Command Mode connections to 15 and sets the maximum number of simultaneous Legacy TCP Command Mode connections to 0. This overrides settings that you might have already set on the CMM.

Note: XClarity Administrator does not modify the security settings or cryptographic settings (cryptographic mode and the mode used for secure communications) during the management process. You can modify the cryptographic settings after the chassis is managed (see Configuring cryptography settings).

Procedure

Complete one of the following procedures to discover and manage your chassis using XClarity Administrator.

- Discover and manage a large number of chassis and other devices using a bulk-import file (see Managing systems in the Lenovo XClarity Administrator online documentation).
- Discover and manage chassis that are on the same IP subnet as XClarity Administrator.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage New Devices page is displayed.



You can sort the table columns to make it easier to find the chassis that you want to manage. In addition, you can enter text (such as a system name or IP address) in the **Filter** field to further filter the chassis that are displayed. You can change the columns that are displayed and the default sort order by clicking the **Customize Columns** icon ( ).

2. Click the **Refresh** icon ( ) to discover all manageable devices in the XClarity Administrator domain. Discovery might take several minutes.
3. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

   Encapsulation can be enabled or disabled on specific devices after they are managed.

   Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
4. Select one or more chassis that you want to manage.
5. Click **Manage Selected**.
6. Choose to use XClarity Administrator managed authentication or local authentication for this device. Managed authentication is selected by default. To use local authentication, clear **Managed Authentication**.

   Note: Managed and local authentication are not supported for ThinkServer and System x M4 servers.
7. Choose the type of credentials to use for the device and specify the appropriate credentials:
   - **Use manually entered credentials**
     - Specify the local user ID and password with **lxc-supervisor** authority for authenticating to the CMM.
     - (Optional) Specify a new password for the CMM user account if the password is currently expired on the device.
   - **Use stored credentials**

Select the stored credential with **lxc-supervisor** authority to use for this managed device. You can add stored credentials by clicking **Manage Stored Credentials**.

Note: If you choose to use local authentication, you must select a stored credential to manage the device.

Tip: It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

For more information about normal and stored credentials, see Managing user accounts and Managing stored credentials.

8. Specify the recovery password if managed authentication is selected.

   A recovery account (`RECOVERY_ID`) is created on the CMM, and all local user accounts are disabled. If there is a problem with XClarity Administrator, and it stops working for some reason, you *cannot* log in to the CMM using normal user accounts. However, you can log in using the `RECOVERY_ID` account.

   Note:

   – The recovery password is required if you choose to use managed authentication and is not allowed if you if you choose to use local authentication.
   – You can choose to use a local recovery account or stored recovery credentials. In either case, the user name is always `RECOVERY_ID`.
   – Ensure that the password follows the security and password policies for the device. Security and password policies might vary.
   – Ensure that you record the recovery password for future use.

   For more information about the recovery ID, see Managing the authentication server.

9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   – You can select from a list of role groups that are assigned to the current user.
   – If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.

    When the process is complete, the dialog displays the number of devices in the chassis and the chassis status.

    Note: Some inventory data is collected after the management process completes. The chassis is in the Pending status until all inventory data is collected. You cannot perform certain tasks on a managed device (such as deploying a server pattern) until all inventory data is collected for that device and the chassis is no longer in the Pending state.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

- If the managing XClarity Administrator failed and cannot be recovered.

  Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.
- If the managing XClarity Administrator was taken down before the devices were unmanaged.
- If the devices were not unmanaged successfully.

Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

12. If this is a new chassis, click **Continue to Chassis Configuration** to validate and change management network settings for the entire chassis (including compute nodes and Flex switches) and to configure the compute node information, local storage, I/O adapters, boot targets, and firmware settings by creating and deploying server patterns. For more information, see Modifying the management-IP settings for a chassis and Configuring servers using configuration patterns.

- Discover and manage chassis that are not on the same IP subnet as XClarity Administrator by manually specifying IP addresses.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

     Encapsulation can be enabled or disabled on specific devices after they are managed.

     Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
  3. Select **Manual Input**.
  4. Specify the network addresses of the chassis that you want to manage:
     - Click **Single System**, and enter a single IP address domain name, or fully-qualified domain name (FQDN).

       Note: To specify an FQDN, ensure that a valid domain name is specified on Network Access page (see Configuring network access).
     - Click **Multiple Systems**, and enter a range of IP addresses. To add another range, click the **Add** icon (). To remove a range, click the **Remove** icon ().
  5. Click **OK**.
  6. Choose to use XClarity Administrator managed authentication or local authentication for this device. Managed authentication is selected by default. To use local authentication, clear **Managed Authentication**.

     Note: Managed and local authentication are not supported for ThinkServer and System x M4 servers.
  7. Choose the type of credentials to use for the device and specify the appropriate credentials:
     - **Use manually entered credentials**

- Specify the local user ID and password with **lxc-supervisor** authority for authenticating to the CMM.
- (Optional) Specify a new password for the CMM user account if the password is currently expired on the device.

– **Use stored credentials**

Select the stored credential with **lxc-supervisor** authority to use for this managed device. You can add stored credentials by clicking **Manage Stored Credentials**.

Note: If you choose to use local authentication, you must select a stored credential to manage the device.

Tip: It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

For more information about normal and stored credentials, see Managing user accounts and Managing stored credentials.

8. Specify the recovery password if managed authentication is selected.

   A recovery account (`RECOVERY_ID`) is created on the CMM, and all local user accounts are disabled. If there is a problem with XClarity Administrator, and it stops working for some reason, you *cannot* log in to the CMM using normal user accounts. However, you can log in using the `RECOVERY_ID` account.

   Note:

   - The recovery password is required if you choose to use managed authentication and is not allowed if you if you choose to use local authentication.
   - You can choose to use a local recovery account or stored recovery credentials. In either case, the user name is always `RECOVERY_ID`.
   - Ensure that the password follows the security and password policies for the device. Security and password policies might vary.
   - Ensure that you record the recovery password for future use.

   For more information about the recovery ID, see Managing the authentication server.

9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   - You can select from a list of role groups that are assigned to the current user.
   - If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. Monitor the progress to ensure that the process completes successfully.

    When the process is complete, the dialog is displayed the number of devices in the chassis and the chassis status.

    Note: Some inventory data is collected after the management process completes. The chassis is in the Pending status until all inventory data is collected. You cannot perform certain tasks on a managed device (such as deploying a server pattern) until all inventory data is collected for that device and the chassis is no longer in the Pending state.

11. When the process is complete, click **OK**.

The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

- If the managing XClarity Administrator failed and cannot be recovered.

  Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.
- If the managing XClarity Administrator was taken down before the devices were unmanaged.
- If the devices were not unmanaged successfully.

Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

12. If this is a new chassis, click **Continue to Chassis Configuration** to validate and change management network settings for the entire chassis (including compute nodes and Flex switches) and to configure the compute node information, local storage, I/O adapters, boot targets, and firmware settings by creating and deploying server patterns. For more information, see Modifying the management-IP settings for a chassis and Configuring servers using configuration patterns.

What to do next

- Discover and manage additional devices.
- Deploy operating-system images to the servers that do not already have an operating system installed. For more information, see Installing operating systems on bare-metal servers.
- Update firmware on devices that are not in compliance with current policies (Updating firmware on managed devices).
- Add the newly managed devices to the appropriate rack to reflect the physical environment (see Managing racks).
- Monitor hardware status and details (see Viewing the status of a managed server).
- Monitor events and alerts (see Working with events and Working with alerts).

Viewing the status of a managed chassis

You can view a summary and detailed status for the managed chassis and their installed components from Lenovo XClarity Administrator.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

The following status icons are used to indicate the overall health of the device. If the certificates do not match, “(Untrusted)” is appended to the status of each applicable device, for example Warning (Untrusted). If there is a connectivity issue or a connection to the device is not trusted, “(Connectivity)” is appended to the status of each applicable device, for example Warning (Connectivity).

- () Critical
- () Warning
- () Pending
- () Informational
- () Normal
- () Offline
- () Unknown

Procedure

Complete the following steps to view the status for a managed chassis.

- View detailed information about the chassis by clicking the **Details** link or by clicking **Actions → Views → Details**.
- Launch the CMM web interface for the chassis by clicking the **IP address** link (see Launching the CMM web interface for a chassis).
- Modify information (such as support contact, location, and description) by clicking **Actions → Inventory → Edit Properties**.
- Modify the management IP settings for the entire chassis, including compute nodes and Flex switches, by clicking **Actions → Inventory → Edit Management IP addresses**.
- Export detailed information about one or more chassis to a single CSV file by selecting the chassis and clicking **Actions → Inventory → Export Inventory**.

  Note: You can export inventory data for a maximum of 60 devices at one time.

  Tip: When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Resolve issues that might arise between the Lenovo XClarity Administrator security certificate and the security certificate of the CMM in the chassis by selecting a chassis and clicking **Actions → Security → Resolve Untrusted Certificates**.

Viewing the details of a managed chassis

You can view the detailed information about the managed chassis from Lenovo XClarity Administrator, including the firmware levels, IP addresses, and universally unique identifier (UUID).

Learn more:

-  XClarity Administrator: Inventory
-  XClarity Administrator: Monitoring

About this task

The system-level air temperature is measured by a physical sensor at the front of the server. This temperature represents inlet air temperature for the server. Note that the air temperature that is reported by XClarity Administrator and the CMM might differ if the temperature is captured at different points in time.

Procedure

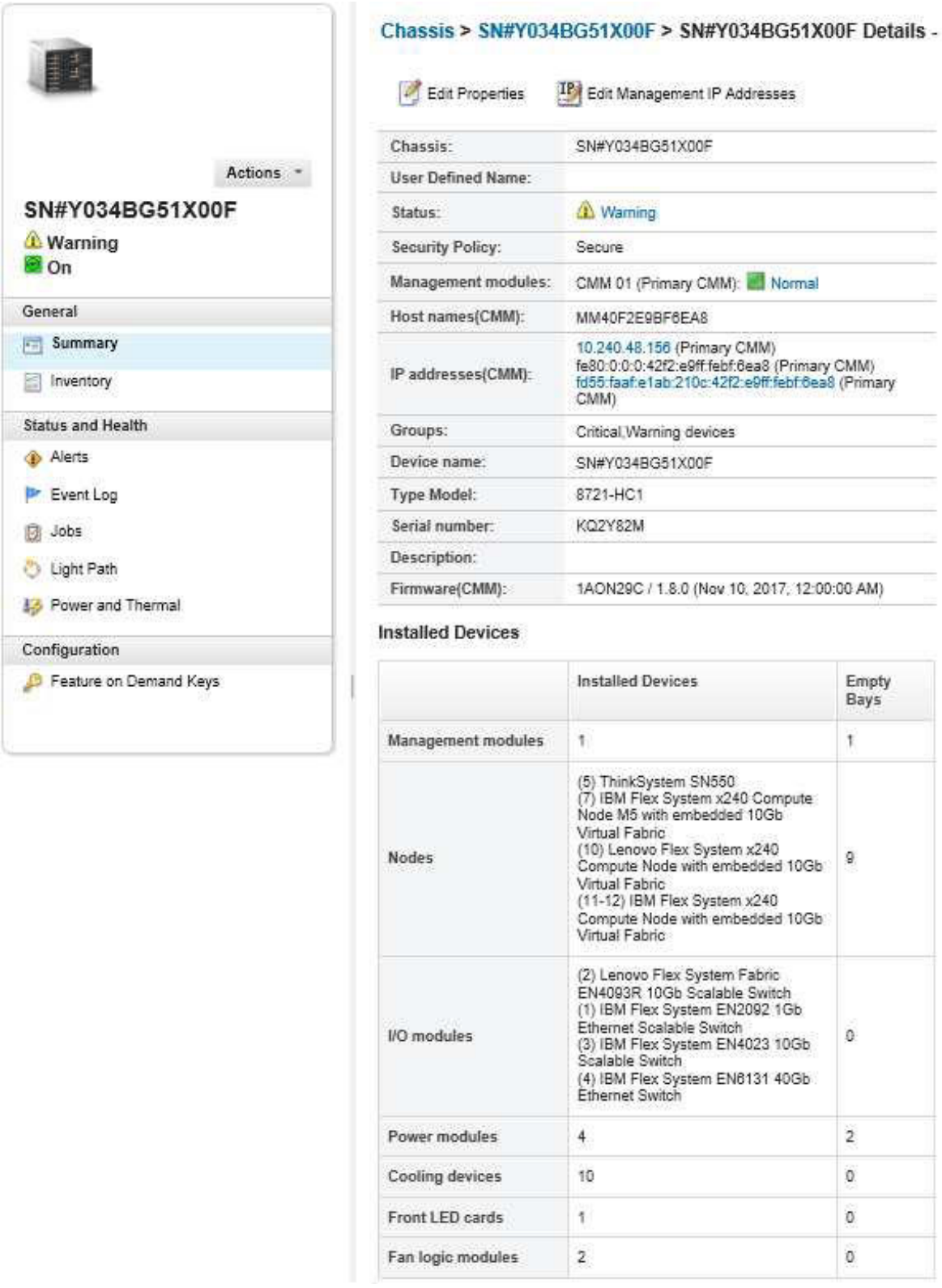
Complete the following steps to view the details for a managed chassis.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Chassis**. The Chassis page is displayed with a tabular view of all managed chassis.

You can sort the table columns to make it easier to find the chassis that you want to manage. In addition, you can enter text (such as a chassis name or IP address) in the **Filter** field to further filter the chassis that are displayed.



Step 2. Click the chassis name in the **Chassis** column. The status summary page for that chassis is displayed, showing the chassis properties and components that are installed in the chassis.



Step 3. Complete one or more of the following actions:

- Click **Summary** to view a summary of the chassis, including system information and installed components (see Viewing the status of a managed chassis).
- Click **Inventory Details** to view details about the chassis components, including:

  - Firmware levels for all components in the chassis.
  - Details of the CMM, such as the hostname, IPv4 address, IPv6 address, and MAC addresses.
  - Asset details of the chassis and CMM installed in the chassis, including name, universally unique identifier (UUID), and location.
- Click **Alerts** to display the list of current alerts for this chassis (see Working with alerts).
- Click **Event Log** to display the list of events for this chassis (see Monitoring events in the event log).
- Click **Jobs** to display a list of jobs associated with the chassis (see Monitoring jobs).
- Click **Light Path** to display the current status of the chassis LEDs, including Location, Fault, and Information. This is the equivalent of looking at the front panel of the chassis.
- Click **Power and Thermal** to display details about power and air flow.

  Tip: Use the refresh button on your web browser to collect the latest power and thermal data. Collecting data might take several minutes.
- Click **Feature on Demand Keys** to access information that is needed to order a Feature on Demand key and other agentless information (see Viewing Features on Demand keys).

What to do next

In addition to displaying summary and detailed information about a chassis, you can perform the following actions:

- View a chassis in graphical rack or chassis view by clicking **Actions → Views → Show in Rack View** or **Actions → Views → Show in Chassis View**.
- Launch the CMM web interface by clicking the **IP address** link (see Launching the CMM web interface for a chassis).
- Modify information (such as support contact, location and description) by clicking **Edit Properties** (see Modifying the system properties for a chassis).
- Modify the management IP settings for the entire chassis, including compute nodes and Flex switches, by clicking **All Actions → Inventory → Edit Management IP addresses** (see Modifying the management-IP settings for a chassis).
- Export detailed information about the chassis to a CSV file clicking the **Actions → Inventory → Export Inventory**.

  Notes:

  - For more information about inventory data in the CSV file, see the GET /chassis/<*UUID_list*> in the XClarity Administrator online documentation.
  - When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Unmanage a chassis (see Unmanaging a chassis).
- Enable or disable firewall rule changes on a chassis that limit incoming requests only from XClarity Administrator by selecting the chassis and clicking **Actions → Security → Enable Encapsulation** or **Actions → Security → Disable Encapsulation**.

  The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

  The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.

- Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the CMM in the chassis by selecting a chassis and clicking **Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).

Backing up and restoring CMM-configuration data

Lenovo XClarity Administrator does not include built-in backup functions for CMM-configuration data. Instead, use the backup functions that are available for your managed CMM.

Use the management web interface or the command-line interface (CLI) to back up and restore the CMM.

- Back up CMM configuration data
  - From the management web interface, click **Mgt Module Management → Configuration → Backup Configuration**. For more information, see Saving a CMM configuration through the web interface in the Flex Systems online documentation.
  - From the CLI, use the **write** command. For more information, see CMM write command in the Flex Systems online documentation
- Restore CMM configuration data
  - From the management web interface, click **Mgt Module Management → Configuration → Restore Configuration from File**. For more information, see Restoring a CMM configuration through the web interface in the Flex Systems online documentation.
  - From the CLI, use the **read** command. For more information, see CMM read command in the Flex Systems online documentation.

Note: Tip: You can find additional information about backing up and restoring chassis components in the PureFlex and Flex System Backup and Restore Best Practices Guide.

Launching the CMM web interface for a chassis

You can launch the CMM web interface for a specific chassis from Lenovo XClarity Administrator.

Procedure

Complete the following steps to launch a CMM web interface.

Note: Launching this CMM web interface from XClarity Administrator using the Safari web browser is not supported.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Chassis** to display the Chassis page.

You can sort the table columns to make it easier to find the chassis that you want to manage. In addition, you can enter text (such as a chassis name or IP address) in the **Filter** field to further filter the chassis that are displayed.



Step 2. Click the link for the chassis in the **Chassis** column. The status summary page for that chassis is displayed.

Step 3. Click **All Actions → Launch → Management Web Interface**. The CMM web interface is started.

Tip: You can also click the IP address to launch the CMM.

Step 4. Log on to the CMM web interface using your XClarity Administrator user credentials.

Modifying the system properties for a chassis

You can modify the system properties for a specific chassis.

Procedure

Complete the following steps to modify the system properties.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Chassis** to display the Chassis page.

Step 2. Select the chassis to be updated.

Step 3. Click **All Actions → Inventory → Edit Properties** to display the Edit dialog.

Step 4. Change the following information, as needed.
- Server name
- Support contact
- Description

Note: The location, room, rack, and lowest rack unit properties are updated by XClarity Administrator when you add or remove devices from a rack in the web interface (see Managing racks).

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface.

Modifying the management-IP settings for a chassis

You can modify the management-IP settings for the entire chassis, including compute nodes, storage devices, and Flex switches.

Procedure

Complete the following steps to modify the management-IP settings.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Chassis** to display the Chassis page.

Step 2. Select the chassis.

Step 3. Click **All Actions → Inventory → Edit Management IP Addresses** to display the Chassis and Components IP Settings page.

Step 4. Change the following global settings, as needed.

- Choose to enable or disable IPv4 addresses.

  If you enable IPv4 addresses, specify the following settings. IPv4 global settings are applied to a component when its IPv4 address is updated.
  - (Optional) Choose to obtain IP addresses using statically assigned IP addresses.
  - Specify the subnet mask and gateway address.
- Specify the following settings for IPv6 addresses. IPv6 global settings are applied to a component when its IPv6 address is updated.
  - (Optional) Choose to obtain IP addresses using statically assigned IP addresses.

    If static IP addresses are used, you can also choose to use stateless IP address auto configuration and stateful IP address configuration.
  - Specify the prefix length and gateway address.
- Choose to enable or disable DNS servers.

  If you enable DNS servers:
  - Choose the DNS server search preference.
  - Enter the IP addresses to use for the DNS search order.
  - Enter the domain name.

Step 5. Change the following CMM IP settings.

- Enter the hostname and IP address for the CMM.
- Click **Auto-Generate IP addresses** to create IP addresses for the compute nodes, storage devices, and Flex switches using the CMM IP address as the starting point.

Step 6. Enter the hostname and IP addresses for each compute node in the chassis

Step 7. Enter the hostname and IP addresses for each storage device in the chassis.

Step 8. Enter the IP addresses for each Flex switch in the chassis.

Step 9. Click **Save**. A dialog box displays with a summary of the network settings.

Step 10. Click **Apply**.

All existing components in the chassis are updated to the specified global settings. When the update is complete, the dialog displays the settings that were changed.

Note: When you change this information, there might be a short delay before the information appears in the Lenovo XClarity Administrator interface.

Step 11. Click **Close**.

Configuring CMM failover

When you install a second CMM in a chassis, the second CMM is automatically configured as a standby CMM by default. If the primary CMM fails, the IP address for the standby CMM changes to the same IP address that was used for the primary CMM, and standby CMM takes over the management of the chassis. However, you can perform more advanced failover configuration from the management controller web interface for the chassis.

About this task

For example, you can choose to:

- Disable the network interface for the standby CMM to prevent failover.
- Enable the network interface for the standby CMM, and allow IP addresses to swap between the two CMMs during failover.
- Enable the network interface for the standby CMM, and prevent the IP addresses from swapping between the two CMMs during failover.

For more information about CMM advanced failover capabilities, see the advfailover command in the CMM online documentation.

Procedure

To enable swappable IP address for the primary and standby CMMs, complete the following steps.

Step 1. From the management controller web interface for the chassis, click **Mgt Module Management → Network → Ethernet** to display the Ethernet Configuration page.

Step 2. Select either **IPv4** and **IPv6** for your system.

Step 3. Under **Configure IP address**, select the option to use a static IP address. Repeat for the other protocol.

Step 4. Click **Mgt Module Management → Properties → Advanced Failover**, and enable the advance failover option.

Step 5. Select **Swap Management Module IP address**.

Step 6. Perform test scenarios to verify that the failover works correctly and that Lenovo XClarity Administrator can connect to primary and backup CMMs.

Restarting a CMM

You can restart a Chassis Management Module (CMM) from Lenovo XClarity Administrator.

Procedure

Complete the following procedure to restart a chassis.

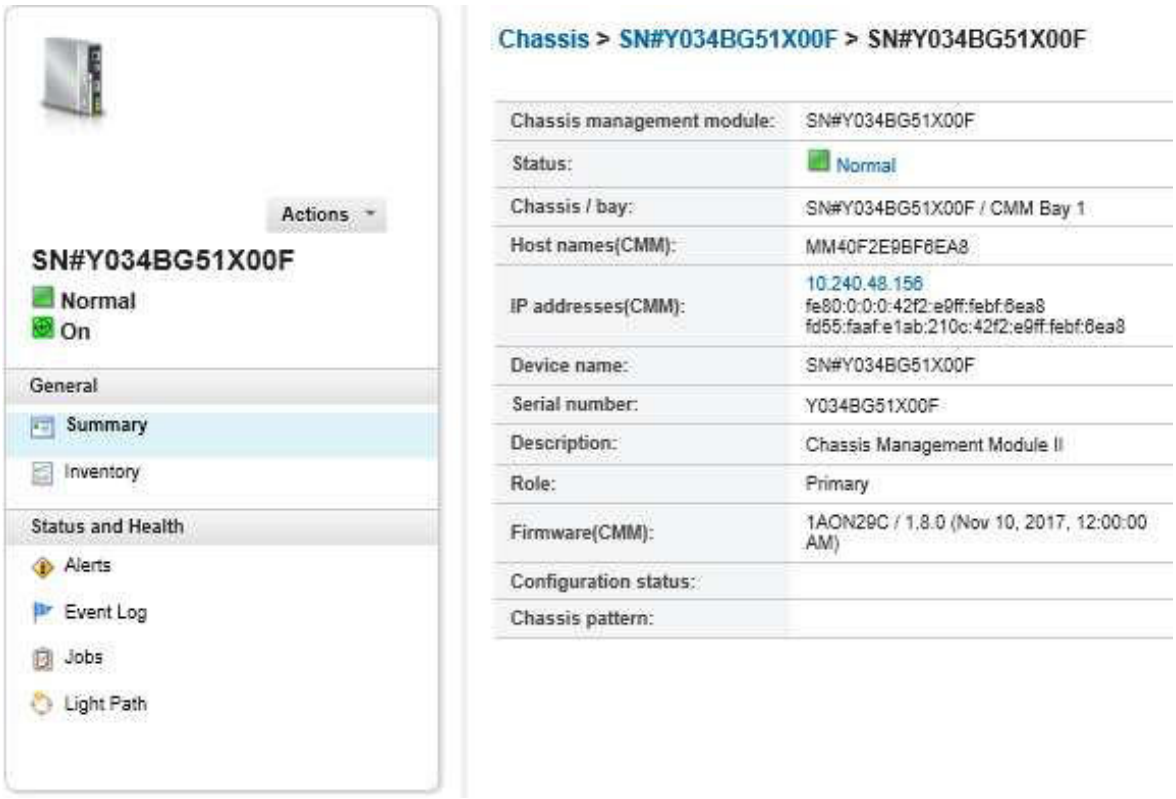
Note: When the CMM is restarted, all existing network connections to the CMM are lost temporarily.

Step 1. From the XClarity Administrator menu, click **Hardware → Chassis**. The Chassis page is displayed with a tabular view of all managed chassis.

Step 2. Click the chassis name in the **Chassis** column to display the graphical chassis view.

Step 3. Click the CMM graphic to display the in the CMM Summary page.

Tip: You can also click **Table View**, and then click the CMM name in the **Name** column to display the CMM Summary page.



Step 4. Click **Actions → Power Actions → Restart**.

Step 5. Click **Restart Immediately**.

This operation might take a few minutes to complete, and you might need to refresh the page to see the results.

Virtually reseating a CMM

You can simulate removing and reinserting a Chassis Management Module (CMM) in a chassis,

About this task

During the virtual reseat, all existing network connections to the CMM are lost, and the power state of the CMM changes.

Attention: Before performing a virtual reseat, ensure that you have saved all user data on the CMM.

Procedure

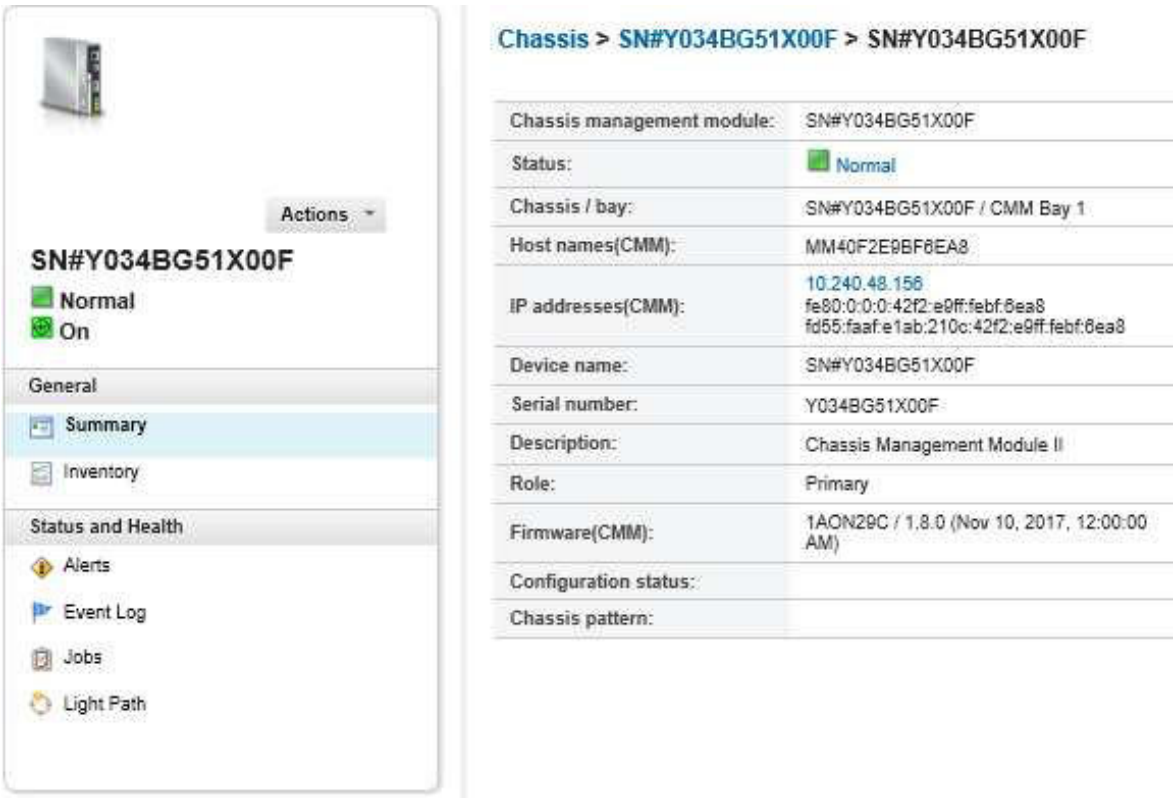
Perform the following steps to virtually reseat a CMM.

Step 1. From the Lenovo XClarity Administrator menu, click **Hardware → Chassis**. The Chassis page is displayed with a tabular view of all managed chassis.

Step 2. Click the chassis name in the **Chassis** column to display the graphical chassis view.

Step 3. Click the CMM graphic to display the in the CMM Summary page.

Tip: You can also click **Table View**, and then click the CMM name in the **Name** column to display the CMM Summary page.



Step 4. Click **Actions → Service → Virtual Reseat**.

Step 5. Click **Virtual Reseat**.

Resolving expired or invalid stored credentials for a chassis

When a stored credential becomes expired or inoperable on a device, the status for that device is shown as “Offline.”

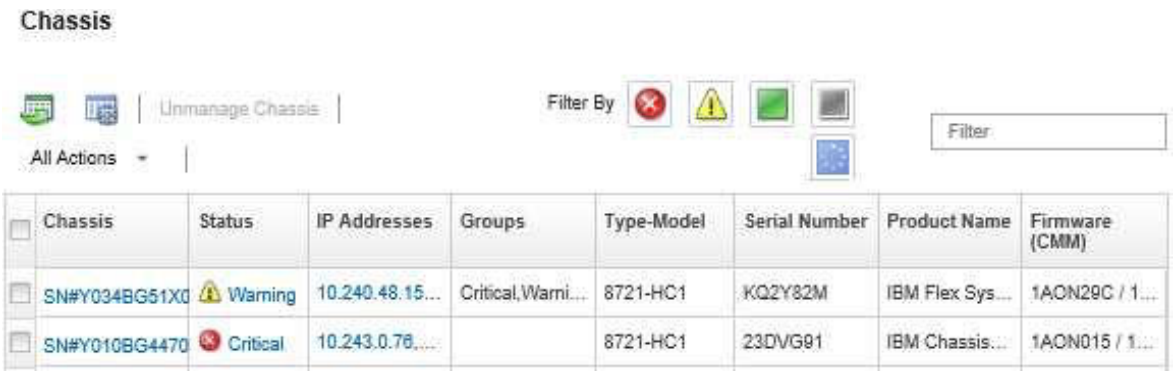
Procedure

To resolve an expired or invalid stored credential for a chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Chassis**. The Chassis page is displayed with a tabular view of all managed chassis.

Step 2. Click the **Power** column header to group all offline chassis at the top of the table.

You can sort the table columns to make it easier to find the chassis that you want to manage. In addition, you can enter text (such as a chassis name or IP address) in the **Filter** field to further filter the chassis that are displayed.



Step 3. Select the chassis to be resolved.

Step 4. Click **All Actions → Security → Edit Stored Credentials**.

Step 5. Change the password for the stored credential or select another stored credential to use for the managed device.

Note: If you managed more than one device using the same stored credentials and you change the password for the stored credentials, that password change affects all devices that are currently using the stored credentials.

Recovering management with a CMM after a management server failure

If a chassis is being managed by Lenovo XClarity Administrator, and XClarity Administrator fails, you can restore the management functions and the local user accounts for a CMM until the management node is restored or replaced.

Procedure

Complete one of the following procedures to restore management on a CMM.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, manage the device again using the RECOVERY_ID account and password and the **Force management** option (see Managing chassis).
- Reset the CMM to factory defaults by pressing the pinhole button on the CMM using a paperclip for at least 10 seconds. For more information about resetting the CMM, including important notices, see CMM Reset in the Flex Systems online documentation.
- Reset the CMM configuration using the following steps:
  1. Through an SSH session, open a management command-line interface for the chassis, and log in with the `RECOVERY_ID` account.

     Note: The password for the `RECOVERY_ID` account was set when you selected the chassis for management on the Management Domain page. For more information about central account management, see Managing chassis.

     If this is the first time that you have used the `RECOVERY_ID` account to log in to the CMM, you must change the password.
  2. If you are prompted, type the new password for the `RECOVERY_ID` account.
  3. Restore the CMM configuration by performing one of the following steps:
     - If you are running CMM firmware release June 2015 or later, run the following command:
       `read -f unmanage -T mm[p]`
       For more information, see the read command in the CMM online documentation.

– If you are running CMM firmware release earlier than June 2015, run the following commands in the order shown:
  a. **env -T mm[p]**
  b. **sslcfg -client disabled -tc1 remove**
  c. **accseccfg -am local**
  d. **ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""**
  e. **ntp -en disabled -i 0.0.0.0 -v3en disabled**
  f. **cimsub -clear all**
  g. **fsmcm -off**

     The **fsmcm** command disables XClarity Administrator user-account management and allows you to use local CMM user accounts to authenticate to the CMM and any management processor that is installed in the chassis.

     After you run the **fsmcm -off** command, the `RECOVERY_ID` account is removed from the CMM user registry. When you run the **fsmcm -off** command, the CMM CLI session terminates. You can now authenticate to the CMM and other chassis components by using local CMM credentials, and use local CMM credentials to access the CMM web interface or CLI for the chassis until user management by XClarity Administrator is restored.

     For more information, see the fsmcm command in the CMM online documentation.

After XClarity Administrator is restored or replaced, you can manage the chassis again (see Managing chassis). All information about the chassis (such as network settings) is retained.

Unmanaging a chassis

You can remove a chassis from management by Lenovo XClarity Administrator. This process is called *unmanaging*. After the chassis is unmanaged, you can log in to the CMM for the chassis by using the local CMM user accounts.

Before you begin

You can enable XClarity Administrator to automatically unmanage devices (including Flex System chassis, Flex System and rack switches, Flex System servers, System x servers, ThinkAgile, and ThinkSystem servers) that are offline for a specific amount of time. This is disabled by default. To enable the automatic unmanagment of offline devices, click **Hardware → Discover and Manage New Devices** from the XClarity Administrator menu, and then click **Edit** next to **Unmanage offline devices is Disabled**. Then, select **Enable unmanage offline devices** and set the time interval. By default, devices are unmanaged after being offline for 24 hours.

Before you unmanage a chassis, ensure that there are no active jobs running against any devices that are installed in the chassis.

When Call Home is enabled in XClarity Administrator, Call Home is disabled on all managed chassis and servers to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time (see Re-enabling call home on all managed devices in the XClarity Administrator online documentation).

About this task

When you unmanage a chassis, XClarity Administrator performs the following actions:

- Clears the configuration used for centralized user management.

- Removes the CMM security certificate from the XClarity Administrator trust store.
- If Encapsulation is enabled on the device, configures the devices firewall rules to the settings before the device was managed.
- Removes access to the NTP server from the CMM.
- Removes the CIM subscriptions to the CMM from the XClarity Administrator configuration so that XClarity Administrator no longer receives events from that chassis.

When you unmanaged a chassis, XClarity Administrator retains certain information about the chassis. That information is reapplied when you manage the same chassis again.

When you unmanage a chassis, events that were sent from the chassis components are discarded. You can retain these events by forwarding the events to an external repository, such as a syslog (see Forwarding events).

Tip: All demo devices that are optionally added during initial setup are nodes in a chassis. To unmanage the demo devices, unmanage the chassis using the **Force unmanage even if the device is not reachable** option.

Procedure

To unmanage a chassis, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Chassis** to display the Chassis page.

Step 2. Select one or more chassis from the lists of managed chassis.

Step 3. Click **Unmanage Chassis**. The Unmanage dialog is displayed.

Step 4. Optional: **Optional:** Select **Force unmanage even if the device is not reachable**.

Important: When unmanaging demo hardware, ensure that you select this option.

Step 5. Click **Unmanage**.The Unmanage dialog shows the progress of each step in the unmanagement process.

Step 6. When the unmanagement process is complete, click **OK**.

What to do next

After the unmanage process is completed, you can log in to the CMM using the local CMM user accounts. If you do not remember the user names or passwords for any local CMM user accounts, reset the CMM to factory defaults to log in to the CMM. For information about resetting the CMM to factory defaults, see CMM Reset in the Flex Systems online documentation in the CMM product documentation.

Recovering a chassis that was not unmanaged correctly

If a chassis was not unmanaged correctly, you must recover the chassis before you can remanage it.

Procedure

Complete one of the following procedures to restore management on a CMM.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, manage the device again using the RECOVERY_ID account and password and the **Force management** option (see Managing chassis).
- Reset the CMM to factory defaults by pressing the pinhole button on the CMM using a paperclip for at least 10 seconds. For more information about resetting the CMM, including important notices, see CMM Reset in the Flex Systems online documentation.

- Reset the CMM configuration using the following steps:
  1. Through an SSH session, open a management command-line interface for the chassis, and log in with the `RECOVERY_ID` account.

     Note: The password for the `RECOVERY_ID` account was set when you selected the chassis for management on the Management Domain page. For more information about central account management, see Managing chassis.

     If this is the first time that you have used the `RECOVERY_ID` account to log in to the CMM, you must change the password.
  2. If you are prompted, type the new password for the `RECOVERY_ID` account.
  3. Restore the CMM configuration by performing one of the following steps:
     - If you are running CMM firmware release June 2015 or later, run the following command:
       `read -f unmanage -T mm[p]`
       For more information, see the read command in the CMM online documentation.
     - If you are running CMM firmware release earlier than June 2015, run the following commands in the order shown:
       a. **env -T mm[p]**
       b. **sslcfg -client disabled -tc1 remove**
       c. **accseccfg -am local**
       d. **ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""**
       e. **ntp -en disabled -i 0.0.0.0 -v3en disabled**
       f. **cimsub -clear all**
       g. **fsmcm -off**

          The **fsmcm** command disables XClarity Administrator user-account management and allows you to use local CMM user accounts to authenticate to the CMM and any management processor that is installed in the chassis.

          After you run the **fsmcm -off** command, the `RECOVERY_ID` account is removed from the CMM user registry. When you run the **fsmcm -off** command, the CMM CLI session terminates. You can now authenticate to the CMM and other chassis components by using local CMM credentials, and use local CMM credentials to access the CMM web interface or CLI for the chassis until user management by XClarity Administrator is restored.

          For more information, see the fsmcm command in the CMM online documentation.

  After XClarity Administrator is restored or replaced, you can manage the chassis again (see Managing chassis). All information about the chassis (such as network settings) is retained.

Chapter 8. Managing servers

Lenovo XClarity Administrator can manage several types of systems, including ThinkAgile, ThinkSystem, Converged, Flex System, NeXtScale, System x®, and ThinkServer® servers.

Learn more:  XClarity Administrator: Discovery

Before you begin

Note: Flex compute nodes are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed Flex compute nodes independent of the chassis.

You can discover and manage Flex Power Systems compute nodes; however, you can use XClarity Administrator only to view properties and status for those servers. You must use other management alternative (such as Flex System Manager or Flex Power Systems Hardware Management Console) to take any management-related actions on the devices, such as updating firmware or configuring the device. You cannot use the Flex System Manager management node and the XClarity Administrator to manage compute nodes in the same chassis.

Note: If you have a managed chassis that contains both Flex System and Flex Power System compute nodes, and you cannot log in to the Flex Power System compute nodes directly, see Cannot log in to managed Flex Power System compute nodes in the XClarity Administrator online documentation.

Before managing servers, ensure that the following conditions are met:

- Review the management considerations before managing a device. For information, see Management considerations in the XClarity Administrator online documentation.
- Certain ports must be available to communicate with devices. Ensure that all required ports are available before you attempt to manage servers. For information about ports, see Port availability in the XClarity Administrator online documentation.
- Ensure that the minimum required firmware is installed on each server that you want to manage using XClarity Administrator. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.
- Ensure that CIM over HTTPS is enabled on the device.
  1. Log in to the management web interface for the server using the `RECOVERY_ID` user account,
  2. Click **IMM Management → Security**.
  3. Click the **CIM Over HTTPS** tab, and ensure that **Enable CIM Over HTTPS** is selected.
- For ThinkSystem SR635 and SR655 servers:
  - Ensure that an operating system is installed, and that the server was booted to the OS, mounted bootable media, or efishell at least once so that XClarity Administrator can collect inventory for those servers.
  - Ensure that IPMI over LAN is enabled. IPMI over LAN is disabled by default on these servers and must be manually enabled before the servers can be managed. To enable IPMI over LAN using TSM, click **Settings → IPMI Configuration**. You might need to restart the server to activate the change.
- If the device's server certificate is signed by an external certificate authority, ensure that the certificate authority certificate and any intermediate certificates are imported into the XClarity Administrator trust store (see Deploying customized server certificates to managed devices).
- To discover a server that is on a *different* subnet from XClarity Administrator, ensure that one of the following conditions are met:

© Copyright Lenovo 2015, 2021

  - Ensure that you enable multicast SLP forwarding on the top-of-rack switches, as well as the routers in your environment. See the documentation that was provided with your specific switch or router to determine whether multicast SLP forwarding is enabled and to find procedures to enable it if it is disabled.
  - If SLP is disabled on the endpoint or on the network, you can use DNS discovery method instead by manually adding a service record (SRV record) to your domain name server (DNS), for XClarity Administrator for example
    `_lxca._tcp.labs.lenovo.com  service = 0 0 443 fvt-xhmc3.labs.lenovo.com.`

    Then, enable DNS discovery on the baseboard management console from the management web interface, by clicking **IMM Management → Network Protocol**, clicking the **DNS** tab, and selecting **Use DNS to discover Lenovo XClarity Administrator**.

    Notes:

    - The management controller must be running a firmware level dated May 2017 or later to support automatic discovery using DNS.
    - If there are multiple XClarity Administrator instances in your environment, the server is discovered only by the instance that is the first to respond to the discovery request. The server is not discovered by all instances.
- To discover and manage ThinkServer servers, ensure that the following requirements are met. For more information, see Cannot discover a device and Cannot manage a device in the XClarity Administrator online documentation.
  - The hostname of the server must be configured using a valid hostname or IP address if you want XClarity Administrator to discover the servers automatically.
  - The network configuration must allow SLP traffic between XClarity Administrator and the server.
  - Unicast SLP is required.
  - If you want XClarity Administrator to automatically discover ThinkServer servers, multicast SLP is required. In addition, SLP must be enabled on the ThinkServer System Manager (TSM).
  - If ThinkServer servers are on a different network than XClarity Administrator, ensure that the network is configured to allow inbound UDP through port 162 so that XClarity Administrator can receive events for those devices.
- For ThinkAgile, ThinkSystem, Converged, Flex System. NeXtScale, and System x servers, if you remove, replace, or configure any adapters in the server, restart the server at least once to update the new adapter information in the baseboard management controller and XClarity Administrator reports (Powering on and off a server).
- When performing management actions on a server, ensure that the server is either powered off or powered on to the BIOS/UEFI Setup or to a running operating system. (You can boot to BIOS/UEFI Setup from the Servers page in XClarity Administrator by clicking **All Actions → Power Actions → Restart to BIOS/UEFI Setup**.) If server is powered on without an operating system, the management controller continuously resets the server in an attempt to find an operating system.
- Ensure that all `UEFI_Ethernet_*` and `UEFI_Slot_*` settings are enabled in the server UEFI Settings. To verify the settings, restart the server and when the prompt `<F1> Setup` is displayed, press `F1` to start the Setup utility. Navigate to **System Settings → Devices and I/O Ports → Enable / Disable Adapter Option ROM Support**, and then locate the **Enable / Disable UEFI Option ROM(s)** section to verify that the settings are enabled.

  Note: If supported, you can also use the Remote Console feature in the baseboard management interface to review and modify the settings remotely.
- System x3950 X6 servers must be managed as two 4U enclosures, each with its own baseboard management controller.

About this task

XClarity Administrator can automatically discover rack and tower servers in your environment by probing for manageable devices that are on the same IP subnet as XClarity Administrator. To discover rack and tower servers that are in other subnets, specify an IP address or range of IP addresses, or import information from a spreadsheet.

Important: For System x3850 and x3950 X6 servers, you must manage each server in the scalable rack environment.

After the servers are managed by XClarity Administrator, Lenovo XClarity Administrator polls each managed server periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed server and perform management actions (such as configuring system settings, deploying operating-system images, and powering on and off).

By default, devices are managed using XClarity Administrator managed authentication to log in to the devices. When managing rack servers and Lenovo chassis, you can choose to use local authentication or managed authentication to log in to the devices.

- When *local authentication* is used for rack servers, Lenovo chassis, and Lenovo rack switches, XClarity Administrator uses a stored credential to authenticate to the device. The *stored credential* can be an active user account on the device or a user account in an Active Directory server.

  You must create a stored credential in XClarity Administrator that matches an active user account on the device or a user account in an Active Directory server before managing the device using local authentication (see Managing stored credentials in the XClarity Administrator online documentation).

  Notes:

  – RackSwitch devices support only stored credentials for authentication. XClarity Administrator user credentials are not supported.
- Using *managed authentication* allows you to manage and monitor multiple devices using credentials in the XClarity Administrator authentication server instead of local credentials. When managed authentication is used for a device (other than ThinkServer servers, System x M4 servers, and switches), XClarity Administrator configures the device and its installed components to use the XClarity Administrator authentication server for centralized management.

  – When managed authentication is enabled, you can manage devices using either manually-entered or stored credentials (see Managing user accounts and in the XClarity Administrator online documentation).

    The stored credential is used only until XClarity Administrator configures the LDAP settings on the device. After that, any change to the stored credential has no impact the management or monitoring of that device.

    Note: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.

  – If a local or external LDAP server is used as the XClarity Administrator authentication server, user accounts that are defined in the authentication server are used to log in to XClarity Administrator, CMMs and baseboard management controllers in the XClarity Administrator domain. Local CMM and management controller user accounts are disabled.

  – If an SAML 2.0 identity provider is used as the XClarity Administrator authentication server, SAML accounts are not accessible to managed devices. However, when using an SAML identity provider and an LDAP server together, if the identity provider uses accounts that exist in the LDAP server, LDAP user accounts can be used to log into the managed devices while the more advanced authentication methods that are provided by SAML 2.0 (such as multifactor authentication and single sign-on) can be used to log into XClarity Administrator.

- When managed authentication is enabled for ThinkSystem SR635 and SR655 servers:
  - Baseboard management-controller firmware supports up to five LDAP user roles. XClarity Administrator adds these LDAP user roles to the servers during management: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin**, and **lxc-os-admin**.

    Users must be assigned to at least one of the specified LDAP user roles to communicate with ThinkSystem SR635 and SR655 servers.
  - Management-controller firmware does not support LDAP users with the same username as local user of the sever.
- For ThinkServer and System x M4 servers, the XClarity Administrator authentication server is not used. Instead, an IPMI account is created on the device with the prefix “LXCA_” followed by a random string. (The existing local IPMI user accounts are not disabled.) When you unmanage a ThinkServer server, the “LXCA_” user account is disabled, and the prefix “LXCA_” is replaced with the prefix “DISABLED_”. To determine whether a ThinkServer server is managed by another instance, XClarity Administrator checks for IPMI accounts with the prefix “LXCA_”. If you choose to force management of a managed ThinkServer server, all the IPMI accounts on the device with the “LXCA_” prefix are disabled and renamed. Consider manually clearing IPMI accounts that are no longer used.

  In XClarity Administrator v2.4 and later, if you use manually-entered credentials, XClarity Administrator automatically creates a stored credential and uses that stored credential to manage the device.

  Notes: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.
  - Each time you manage a device using manually-entered credentials, a new stored credential is created for that device, even if another stored credential was created for that device during a previous management process.
  - When you unmanage a device, XClarity Administrator does not delete stored credentials there were automatically created for that device during the management process.

A device can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device on the initial XClarity Administrator, and then manage it with the new XClarity Administrator. If an error occurs during the unmanagement process, you can select the **Force management** option during management on the new XClarity Administrator.

Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a device is already managed by another manager until after it attempts to manage the device.

Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a ThinkServer device is already managed; therefore, managed ThinkServer devices might appear in the list of manageable devices.

During the management process, XClarity Administrator performs the following actions:

- Logs in to the server using the provided credentials.
- Collects inventory for each server.

  Note: Some inventory data is collected after the management process completes. You cannot perform certain tasks on a managed server (such as deploying a server pattern) until all inventory data is collected for that server and the server is no longer in the Pending state.
- Configures settings for the NTP server so all managed devices use the same NTP server configuration that is configured on XClarity Administrator.
- (System x and NeXtScale severs only) Assigns the last-edited firmware-compliance policy to the server.

- (Lenovo System x and NeXtScale severs only) Optionally configures the devices firewall rules so that incoming requests from only XClarity Administrator are accepted.
- (System x and NeXtScale severs only) Exchanges security certificates with the management controller, copying the CIM server certificate and the LDAP client certificate from the management controller into the XClarity Administrator trust store and sending the XClarity Administrator CA security certificate and LDAP trust certificates to the management controller. The management controller loads the certificates into the management-controller trust store so that the management controller can trust connections to the LDAP and CIM servers on the XClarity Administrator.

  Note: If the CIM server certificate or LDAP client certificate does not exist, it is created during the management process.
- Configures managed authentication, if applicable. For more information about managed authentication, see Managing the authentication server.
- Creates the recovery user account (`RECOVERY_ID`), when applicable. For more information about the `RECOVERY_ID` account, see Managing the authentication server.

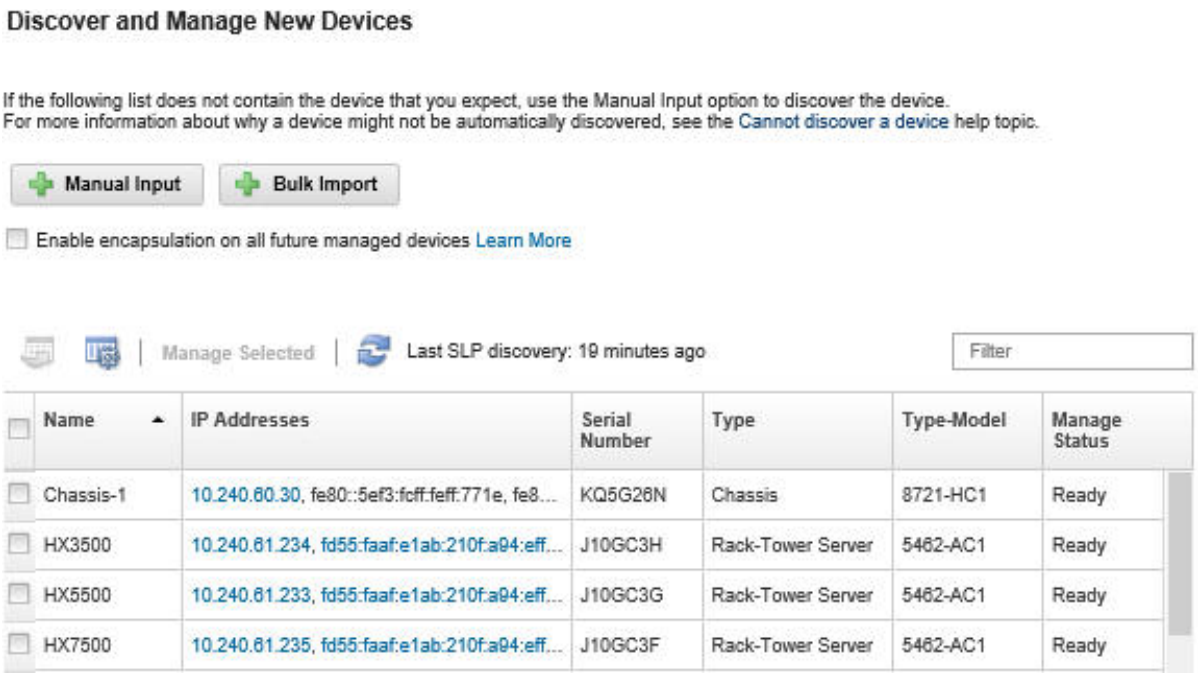
Note: The XClarity Administrator does not modify the security settings or cryptographic settings (cryptographic mode and the mode used for secure communications) during the management process. You can modify the cryptographic settings after the server is managed (see Configuring cryptography settings).

Important: If you change the IP address of a server after the server is managed by XClarity Administrator, XClarity Administrator recognizes the new IP address and continue to manage the server. however, XClarity Administrator does not recognize the IP address change for some servers. If XClarity Administrator shows that the server is offline after the IP address was changed, manage the server again using the **Force Management** option.

Procedure

To manage your rack and tower servers using XClarity Administrator, complete one of the following procedures.

- Discover and manage a large number of tower and rack servers and other devices using a bulk-import file (see Managing systems in the XClarity Administrator online documentation).
- Discover and manage rack and tower servers that are on the same IP subnet as XClarity Administrator.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage New Devices page is displayed.



You can sort the table columns to make it easier to find the servers that you want to manage. In addition, you can enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed. You can change the columns that are displayed and the default sort order by clicking the **Customize Columns** icon ( ).

2. Click the **Refresh** icon ( ) to discover all manageable devices in the XClarity Administrator domain. Discovery might take several minutes.
3. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

   Encapsulation can be enabled or disabled on specific devices after they are managed.

   Note: When the management network interface is configured to use the Dynamic Host Configuration Protocol (DHCP) and when encapsulation enabled, managing a rack server can take a long time.

   Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
4. Select one or more servers that you want to manage.
5. Click **Manage Selected**. The Manage dialog is displayed.
6. Choose to use XClarity Administrator managed authentication or local authentication for this device. Managed authentication is selected by default. To use local authentication, clear **Managed Authentication**.
7. Choose the type of credentials to use to authenticate to the device and specify the appropriate credentials:
   - **Use manually entered credentials**
     - Specify the user ID and password for authenticating to the server. You can use manually entered credentials only with XClarity Administrator managed authentication.

- (Optional) Set a new password for the specified user name if the password is currently expired on the device.

- **Use stored credentials**

  Select the stored credential to use for this managed device. You can create a new stored credential by clicking **Create New**.

  Note: If you choose to use local authentication, you must select a stored credential to manage the device.

- **Use identity-management system**

  Select the identity management system that you want to use for this managed device. Then, fill in the remaining fields, including the IP address or host name of the managed server, user name, and optionally application ID, safe and folder.

  If you specify the application ID, you must also specify the safe and folder, if applicable.

  If you do not specify the application ID, XClarity Administrator uses the paths that were defined when you setup CyberArk to identify the onboarded accounts in CyberArk (see Setting up a CyberArk identity-management system).

  Notes:

  - Accounts in an identity-management system can be used only with managed authentication.
  - Only ThinkSystem or ThinkAgile servers are supported. The identity management system must be configured in XClarity Administrator, and the Lenovo XClarity Controller for the managed ThinkSystem or ThinkAgile servers must be integrated with CyberArk (seeSetting up a CyberArk identity-management system).

It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

For more information about normal and stored credentials, see Managing user accounts and Managing stored credentials.

8. Specify the recovery password if managed authentication is selected.

   When a password is specified, the recovery account (`RECOVERY_ID`) is created on the server, and all local user accounts are disabled. If there is a problem with XClarity Administrator, and it stops working for some reason, you *cannot* log in to the management controller using normal user accounts. However, you can log in using the recovery account.

   Notes:

   - The recovery password is optional if you choose to use managed authentication and is not allowed if you if you choose to use local authentication.
   - You can choose to use a local recovery account or stored recovery credentials. In either case, the user name is always `RECOVERY_ID`.
   - Ensure that the password follows the security and password policies for the device. Security and password policies might vary.
   - Ensure that you record the recovery password for future use.
   - The recovery account is not supported for ThinkServer and System x M4 servers.

   For more information about the recovery ID, see Managing the authentication server.

9. Click **Change** to change the role groups that are to be assigned to the devices.

Notes:

- You can select from a list of role groups that are assigned to the current user.
- If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    - If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    - If the managing XClarity Administrator was taken down before the devices were unmanaged.
    - If the devices were not unmanaged successfully.

    Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

- Discover and manage rack and tower servers that are not on the same IP subnet as XClarity Administrator by manually specifying IP addresses.

  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

     Encapsulation can be enabled or disabled on specific devices after they are managed.

     Note: When the management network interface is configured to use the Dynamic Host Configuration Protocol (DHCP) and when encapsulation enabled, managing a rack server can take a long time.

     Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.

  3. Select **Manual Input**.
  4. Specify the network addresses of the servers that you want to manage:

     - Click **Single System**, and enter a single IP address domain name, or fully-qualified domain name (FQDN).

       Note: To specify an FQDN, ensure that a valid domain name is specified on Network Access page (see Configuring network access).

- Click **Multiple Systems**, and enter a range of IP addresses. To add another range, click the **Add** icon (). To remove a range, click the **Remove** icon ().

5. Click **OK**. The Manage dialog is displayed
6. Choose to use XClarity Administrator managed authentication or local authentication for this device. Managed authentication is selected by default. To use local authentication, clear **Managed Authentication**.
7. Choose the type of credentials to use to authenticate to the device and specify the appropriate credentials:
   - **Use manually entered credentials**
     - Specify the user ID and password for authenticating to the server. You can use manually entered credentials only with XClarity Administrator managed authentication.
     - (Optional) Set a new password for the specified user name if the password is currently expired on the device.
   - **Use stored credentials**

     Select the stored credential to use for this managed device. You can create a new stored credential by clicking **Create New**.

     Note: If you choose to use local authentication, you must select a stored credential to manage the device.
   - **Use identity-management system**

     Select the identity management system that you want to use for this managed device. Then, fill in the remaining fields, including the IP address or host name of the managed server, user name, and optionally application ID, safe and folder.

     If you specify the application ID, you must also specify the safe and folder, if applicable.

     If you do not specify the application ID, XClarity Administrator uses the paths that were defined when you setup CyberArk to identify the onboarded accounts in CyberArk (see Setting up a CyberArk identity-management system).

     Notes:

     - Accounts in an identity-management system can be used only with managed authentication.
     - Only ThinkSystem or ThinkAgile servers are supported. The identity management system must be configured in XClarity Administrator, and the Lenovo XClarity Controller for the managed ThinkSystem or ThinkAgile servers must be integrated with CyberArk (seeSetting up a CyberArk identity-management system).

   It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

   For more information about normal and stored credentials, see Managing user accounts and Managing stored credentials.
8. Specify the recovery password if managed authentication is selected.

   When a password is specified, the recovery account (`RECOVERY_ID`) is created on the server, and all local user accounts are disabled. If there is a problem with XClarity Administrator, and it stops working for some reason, you *cannot* log in to the management controller using normal user accounts. However, you can log in using the recovery account.

   Notes:

- The recovery password is optional if you choose to use managed authentication and is not allowed if you if you choose to use local authentication.
- You can choose to use a local recovery account or stored recovery credentials. In either case, the user name is always `RECOVERY_ID`.
- Ensure that the password follows the security and password policies for the device. Security and password policies might vary.
- Ensure that you record the recovery password for future use.
- The recovery account is not supported for ThinkServer and System x M4 servers.

For more information about the recovery ID, see Managing the authentication server.

9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   - You can select from a list of role groups that are assigned to the current user.
   - If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    - If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    - If the managing XClarity Administrator was taken down before the devices were unmanaged.
    - If the devices were not unmanaged successfully.

    Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

What to do next

- Discover and manage additional devices.
- Configure the system information, local storage, I/O adapters, boot topics, and firmware settings by creating and deploying server patterns (see Configuring servers using configuration patterns).
- Deploy operating-system images to servers that do not already have an operating system installed (see Installing operating systems on bare-metal servers).
- Update firmware on devices that are not in compliance with current policies (see Updating firmware on managed devices).
- Add the devices to the appropriate rack to reflect the physical environment (see Managing racks).

- Monitor hardware status and details (see Viewing the status of a managed server).
- Monitor events and alerts (see Working with events and Working with alerts).
- Resolve stored credentials that have become expired or invalid (see Managing stored credentials).

Viewing the status of a managed server

You can view a summary and detailed status for the managed servers and their installed components from the Lenovo XClarity Administrator.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

The following status icons are used to indicate the overall health of the device. If the certificates do not match, "(Untrusted)" is appended to the status of each applicable device, for example Warning (Untrusted). If there is a connectivity issue or a connection to the device is not trusted, "(Connectivity)" is appended to the status of each applicable device, for example Warning (Connectivity).

- ( ) Critical
- ( ) Warning
- ( ) Pending
- ( ) Informational
- ( ) Normal
- ( ) Offline
- ( ) Unknown

A device can be in one of the following power states:

- On
- Off
- Shutting down
- Standby
- Hibernate
- Unknown

Procedure

To view the status for a managed server, complete one or more of the following actions.

- From the XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of all managed devices and other resources.



- From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack and tower servers, and compute nodes).

  You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list, enter text (such as a name or IP address) in the **Filter** field, and click the status icons to list only those servers that meet the selected criteria.



  From this page, you can perform the following actions:

  - View detailed information about the server and its components (see Viewing the details of a managed server).
  - View a server in graphical rack or chassis view clicking **All Actions → Views → Show in Rack View** or **All Actions → Views → Show in Chassis View**.

- Launch the management controller web interface for the server by clicking the **IP address** link (see Launching the management controller interface for a server).
- Remotely manage the server (see Using remote control to manage Converged, Flex System, NeXtScale, and System x servers).
- Power the server on and off (see Powering on and off a server).
- Modify system information by selecting a server and clicking **All Actions → Inventory → Edit Properties**.
- Refresh inventory by selecting a server and clicking **All Actions → Inventory → Refresh Inventory**.
- Export detailed information about one or more servers to a single CSV file by selecting the servers and clicking **All Actions → Inventory → Export Inventory**.

  Note: You can export inventory data for a maximum of 60 devices at one time.

  Tip: When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Unmanage a server (see Unmanaging a rack or tower server).
- Reset the local storage adapters to their default manufacturing settings by clicking **All Action → Service → Reset Local Storage to Defaults**.
- Change the Location LED state on a server to on, off, or blinking by selecting the server and clicking **All Actions → Service → Toggle Location LED State**, selecting the state, and clicking **Apply**.

  Note: The Location LED on ThinkServer servers can be on or off. Blinking is not supported.
- Virtually reseat the server (see Virtually reseating a server in a Flex System chassis).
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Exclude events** icon () (see Excluding events).
- Restart the server using a non-maskable interrupt (NMI) by clicking **All Action → Service → Trigger NMI**.
- Enable or disable firewall rule changes on a server that limit incoming requests only from XClarity Administrator by selecting the server and clicking **All Actions → Security → Enable Encapsulation** or **All Actions → Security → Disable Encapsulation**.The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

  When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

  Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
- (Converged, Flex System, NeXtScale, System x, and ThinkSystem servers only) Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the baseboard management controller in the server by selecting a server and clicking **All Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).
- Resolve expired or invalid stored credentials for a device in the group (see Resolving expired or invalid stored credentials for a server).
- Add or remove a server from a static resource group by clicking **All Actions → Groups → Add to Group** or **All Actions → Groups → Remove from Group**.

Viewing the details of a managed server

You can view detailed information about the managed servers from Lenovo XClarity Administrator, including the firmware levels, server name, and universally unique identifier (UUID).

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

CPU usage is a measurement of the aggregated C-state residency. It is measured as a percentage of the used and maximum C0 residency, per second.

Memory usage is a measurement of the aggregated read/write volumes of all memory channels. This is calculated as a percentage of the used and maximum memory bandwidth that is available, per second.

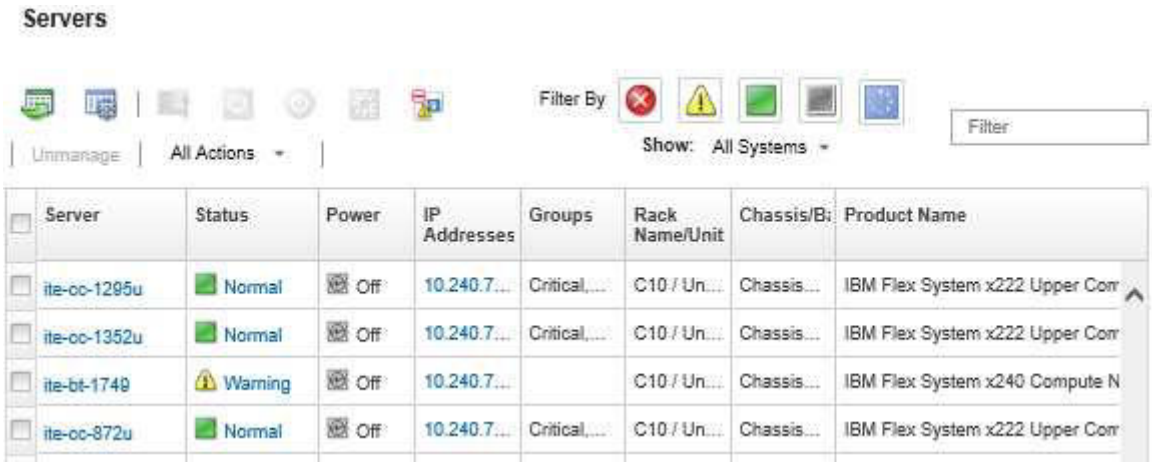
The system-level air temperature is measured by a physical sensor at the front of the server. This temperature represents inlet air temperature for the server. Note that the air temperature that is reported by XClarity Administrator and the CMM might differ if the temperature is captured at different points in time.

Procedure

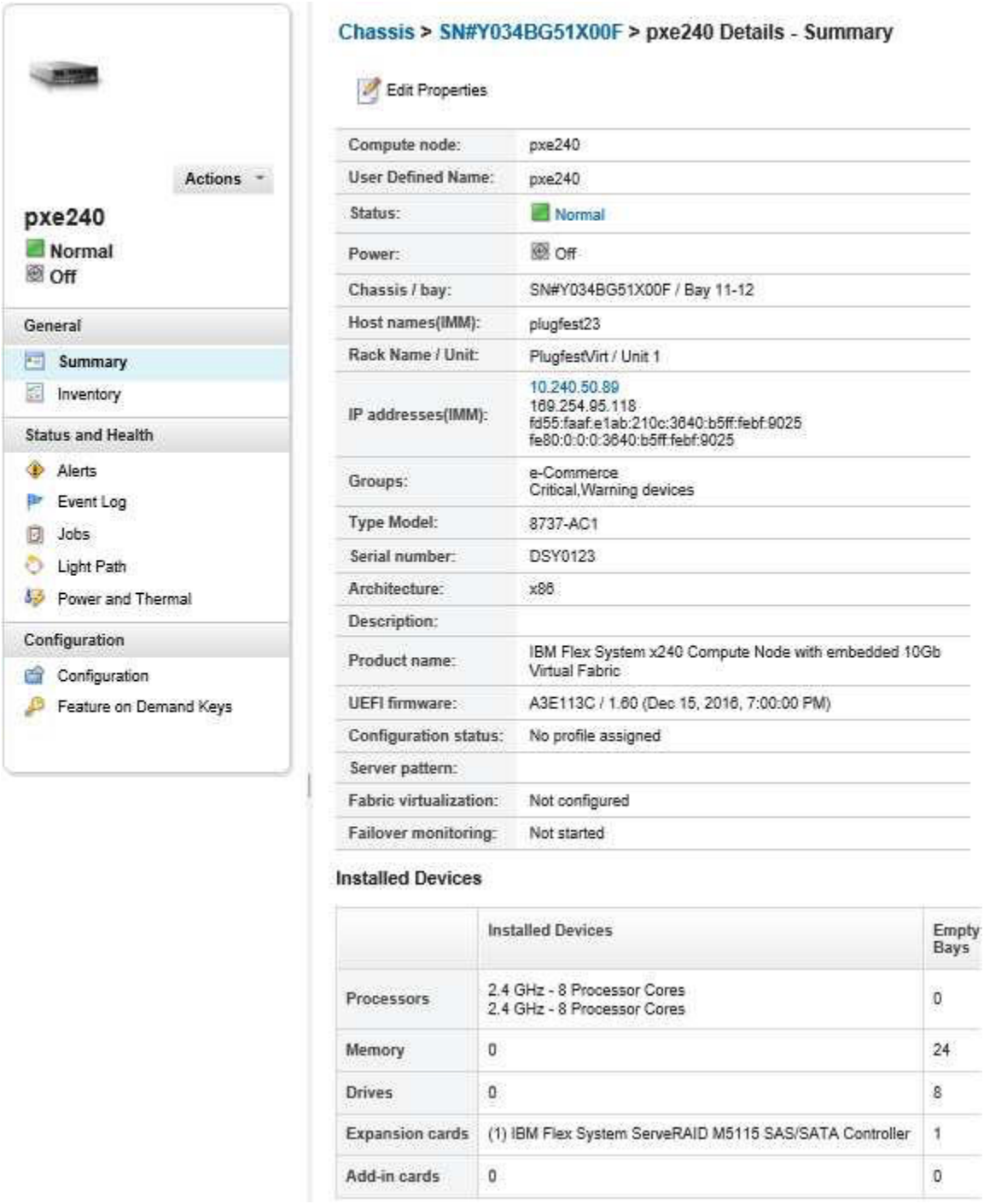
Complete the following steps to view the details for a managed server.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find the specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a system name or IP address) in the **Filter** field to further filter the servers that are displayed.



Step 2. Click the link for the server in the **Server** column. The status summary page for that server is displayed, showing the server properties and a list of components that are installed in that server.



Note: For System x and NeXtScale servers, the LAN over USB address is listed on this page; however, you cannot change that address from the XClarity Administrator. Instead, you must use the baseboard-management-controller interface for the server. For more information, see "Accessing the IMM2 using the LAN over USB interface" in the product documentation for the server. You can find the product documentation for your server in the BladeCenter online documentation.

Step 3. Complete one or more of the following actions:

- Click **Summary** to view a summary of the server, including system information and installed components (see Viewing the status of a managed server).

- Click **Inventory Details** to view details about the server components, including:
  - Firmware levels for the server and management controller.
  - Management-module network details, such as the hostname, IPv4 address, IPv6 address, and MAC addresses.
  - Asset details, including server name, universally unique identifier (UUID), and location.
  - Components details, including CPUs, memory, drives, and expansion cards.

  Notes:

  - All IP addresses for the server are listed. The IP address for the management controller port is listed first. If the management controller IP address is available, it is used to connect to the server.
  - If data is not available for a specific adapter, some fields for the adapter (such as product name) might be empty.
  - If a new adapter was installed in the server, the server must be rebooted for the adapter to show up in the inventory.
  - For some add-in cards, the Feature on Demand (FoD) information is displayed under the device name.
  - You can hover over links in the Type column to get to get more information about specific components, such as Intel Optain DCPMM memory.
- Click **Alerts** to display the list of current alerts for this server (see Working with alerts).

  Note: You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level (see Setting threshold preferences for generating alerts and events).
- Click **Event Log** to display the list of events for this server (see Monitoring events in the event log).
- Click **Jobs** to display a list of jobs associated with the server (see Monitoring jobs).
- Click **Light Path** to display the current status of the server LEDs, including Location, Fault, and Information. This is the equivalent of looking at the front panel of the server.
- Click **Power and Thermal** to display details about power use and air temperature.

  Tip: Use the refresh button on your web browser to collect the latest power and thermal data. Collecting data might take several minutes.
- Click **Configuration** to view configuration information for the server, including local storage, I/O adapters, SAN boot settings, and firmware settings (see Configuring servers using configuration patterns).
- Click **Feature on Demand Keys** to view a list of Feature on Demand keys that are currently installed on the managed server (see Viewing Features on Demand keys).

What to do next

In addition to displaying summary and detailed information about a server, you can perform the following actions:

- View the rack or chassis that is associated with the server by clicking rack or chassis name from the Summary page.
- View a server in graphical rack or chassis view clicking **All Actions → Views → Show in Rack View** or **All Actions → Views → Show in Chassis View**.
- Launch the management controller web interface for the server by clicking the **IP address** link (see Launching the management controller interface for a server).

- Remotely access the server (see Using remote control to manage Converged, Flex System, NeXtScale, and System x servers).
- Power the server on and off (see Powering on and off a server).
- Modify system information by selecting a server and clicking **Edit Properties**.
- Refresh inventory by selecting a server and clicking **Actions → Inventory → Refresh Inventory**.
- Export detailed information about the server to a CSV file clicking the **Actions → Inventory → Export Inventory**.

  Notes:

  – For more information about inventory data in the CSV file, see the GET /nodes/<*UUID_list*> in the XClarity Administrator online documentation.

  – When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Actions → Service Reset → Exclude events** (see Excluding events).
- Restarting the server using a non-maskable interrupt (NMI) by clicking **Actions → Service → Trigger NMI**
- Change the Location LED state on a server to on, off, or blinking by selecting the server and clicking **Actions → Service → Toggle Location LED State**, selecting the state, and clicking **Apply**.

  Note: The Location LED on ThinkServer servers can be on or off. Blinking is not supported.
- Enable or disable firewall rule changes on a server that limit incoming requests only from XClarity Administrator by selecting the server and clicking **Actions → Security → Enable Encapsulation** or **Actions → Security → Disable Encapsulation**. The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

  When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

  Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
- (non-ThinkServer servers only) Resolve issues that might arise between the Lenovo XClarity Administrator security certificate and the security certificate of the management controller in the server by selecting a server and clicking **Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).

Backing up and restoring server-configuration data

Lenovo XClarity Administrator does not include built-in backup functions for server-configuration data. Instead, use the backup functions that are available for your managed server.

- **Converged, Flex System, System x, ThinkSystem, and NeXtScale servers**
  – Back up server-configuration data

    Use the management web interface or CLI to back up the firmware.

    – From the IMM web interface, click **IMM Management → IMM Configuration**.

    – From the CLI, use the **backup** command.

For more information about backing up servers using the IMM, see the Integrated Management Module II online documentation.

Use tools that are provided by the operating system to back up applications that are running on the server. For more information, see the documentation that came with your operating system.

For Flex System compute devices, ensure that you back up the settings for options that are installed on the compute nodes. You can back up all compute node settings, including the option settings, using the Advanced Setup Utility (ASU). For information about ASU, see Advanced Settings Utility (ASU) website).

– Restore server-configuration data

Use the management web interface or the CLI to restore the firmware. For more information about restoring servers through the BMC, see Integrated Management Module II online documentation.

Use the documentation that is provided with the operating system and any applications that are running on the server to restore the software that is installed on the server.

– From the IMM web interface, click **IMM Management → IMM Configuration**.
– From the CLI, use the **restore** command.

Note: Tip: You can find additional information about backing up and restoring chassis components in the PureFlex and Flex System Backup and Restore Best Practices Guide.

- **ThinkServer servers**The restore procedures vary for each type of ThinkServer servers. See the product documentation that is provided with your server for information about restoring the device.

Using remote control

From the Lenovo XClarity Administrator web interface, you can open a remote-control session to a managed server as if you were at a local console. You can use the remote-control session to perform operations such as powering on or off the server, and logically mounting a local or remote drive.

To launch a remote-control session for any device, you must have **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin**, or **lxc-hw-manager** privileges.

Using remote control to manage ThinkSystem or ThinkAgile servers

From the Lenovo XClarity Administrator web interface, you can open a remote-control session to a managed ThinkSystem or ThinkAgile server as if you were at a local console. You can use the remote-control session to perform power operations and logically mount a local or network drive.

Before you begin

Encapsulation must be disabled on the server.

To open a remote-control session to a server, the server must be in the Online or Normal state. If a server has any other access state, the remote-control session cannot connect to the server. For more information about viewing the server status, see Viewing the details of a managed server.

Review the following considerations for ThinkSystem SR635 and SR655 servers.
- Baseboard management controller firmware v2.94 or later is required.
- Only multiple-user mode is supported; single-user mode is not supported.
- Internet Explorer 11 is not supported.
- You cannot power on or power off a server from a remote-control session.

About this task

You can launch a remote-control session to a single ThinkSystem or ThinkAgile server from XClarity Administrator.

For more information about using the remote console and media features, see your ThinkSystem or ThinkAgile server documentation.

Note: For the ThinkSystem and ThinkAgile servers, a Java Runtime Environment (JRE) with Java WebStart support is not required.

Procedure

To open a remote-control session to a specific server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Select the server to which you want to open a remote-control session.

Step 3. Click the **Remote Control** icon ( ).

Step 4. Accept any security warnings from your web browser.

What to do next

If the remote-control session does not open successfully, see Remote control issues in the XClarity Administrator online documentation.

Using remote control to manage ThinkServer and NeXtScale sd350 M5 servers

From the Lenovo XClarity Administrator web interface, you can open a remote-control session to managed ThinkServer and NeXtScale sd350 M5 servers as if you were at a local console. You can use the remote-control session to perform power and reset operations, logically mount a local or network drive on the server, and capture screen shots and record video.

Before you begin

- Remote control for these servers requires a Java Runtime Environment (JRE) with Java WebStart support installed on the client side. The following JREs are supported.
  - Oracle JRE 7 (see Oracle Java download website)
  - Oracle JRE 8, which requires a paid license (see Oracle Java download website)
  - Adopt OpenJDK 8 with the IcedTea-Web v1.8 plugin (see the Adopt OpenJDK website, IcedTea-Web website, and IcedTea-Web usage website)

  Attention: An open-source JDK is highly recommended. If you are using a vendor's JRE or JDK, ensure that it is properly licensed for commercial usage.
- Remote control requires that a Features on Demand key for ThinkServer System Manager Premium Upgrade is installed on ThinkServer servers. For more information about FoD keys that are installed on your servers, see Viewing Features on Demand keys .

About this task

You can launch a remote-control session to a single ThinkServer server from XClarity Administrator.

To open a remote-control session to a server, the server must be in the Online or Normal state. If a server has any other access state, the remote-control session cannot connect to the server. For more information about viewing the server status, see Viewing the details of a managed server.

For more information about using the ThinkServer remote console and media features, see your ThinkServer server documentation.

Procedure

To open a remote-control session to a specific server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Select the server to which you want to open a remote-control session.

Step 3. Click the **Remote Control** icon ().

Step 4. Accept any security warnings from your web browser.

What to do next

If the remote-control session does not open successfully, see Remote control issues in the XClarity Administrator online documentation.

Using remote control to manage Converged, Flex System, NeXtScale, and System x servers

From the Lenovo XClarity Administrator web interface, you can open a remote-control session to manage Converged, Flex System, NeXtScale, and System x servers as if you were at a local console.

Before you begin

 XClarity Administrator: Remote control

- Remote control for these servers requires a Java Runtime Environment (JRE) with Java WebStart support installed on the client side. The following JREs are supported.
  - Oracle JRE 7 (see Oracle Java download website)
  - Oracle JRE 8, which requires a paid license (see Oracle Java download website)
  - Adopt OpenJDK 8 with the IcedTea-Web v1.8 plugin (see the Adopt OpenJDK website, IcedTea-Web website, and IcedTea-Web usage website).

  Attention: An open-source JDK is highly recommended. If you are using a vendor's JRE or JDK, ensure that it is properly licensed for commercial usage.
- You can launch a remote-control session on servers running the following operating systems (either 32-bit or 64-bit):
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- Remote control requires that a Features on Demand key for remote presence is installed on Converged, NeXtScale, and System x servers. If the FoD key is not detected on a server, the remote-control session displays the `Missing activation key` message for that server when displaying the list of available servers. You can determine whether remote presence is enable, disabled, or not installed on a server from the

Servers page (see Viewing the status of a managed server). For more information about FoD keys that are installed on your servers, see Viewing Features on Demand keys.

- The user account that is used to start the remote-control session must be a valid user account that has been defined in the XClarity Administrator authentication server. The user account must also have sufficient user authority to access and manage a server.
- Review the security, performance and keyboard considerations before opening a remote-control session. For more information about these considerations, see Remote control considerations.
- The Remote Control dialog uses the locale and display language settings that are defined for the operating system on your local system.If your local system runs on Windows, see the Java website for information about how to change the locale setting. To change the display language, install a localized copy of Windows or install a language pack from the Windows website.

About this task

You can start multiple remote-control sessions from Lenovo XClarity Administrator. Each session can manage multiple servers.

To open a remote-control session to a server, the server must be in the Online or Normal state. If a server has any other access state, the remote-control session cannot connect to the server. For more information about viewing the server status, see Viewing the details of a managed server.

You can open an untargeted remote-control session by clicking **Provisioning → Remote Control** from the Lenovo XClarity Administrator menu bar. Then, accept any security warnings from your web browser.

Note: For Flex System x280, x480, and x880 compute nodes, you can start a remote-control session to only the primary node. If you attempt to start a remote-control session to a non-primary node in a multi-node system, the remote-control dialog starts, but no video is displayed.

Procedure

Complete the following steps to open a remote-control session to a specific Converged, Flex System, NeXtScale, and System x server.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Select the server to which you want to open a remote-control session.

Step 3. Click the **Remote Control** icon ().

Step 4. Accept any security warnings from your web browser.

Step 5. Optionally, choose to save the Remote Control icon to your desktop. You can use this icon to launch a remote-control session without logging in to the XClarity Administrator web interface.

Step 6. When you are prompted, select one of the following connection modes:

- **Single-user mode**. Establishes an exclusive remote-control session with the server. All other remote-control session to that server are blocked until you disconnect from the server. This option is available only if there are no other remote-control sessions established to the server.
- **Multi-user mode**. Allows multiple remote-control sessions to be established with the same server. XClarity Administrator supports up to six concurrent remote-control sessions to a single server.

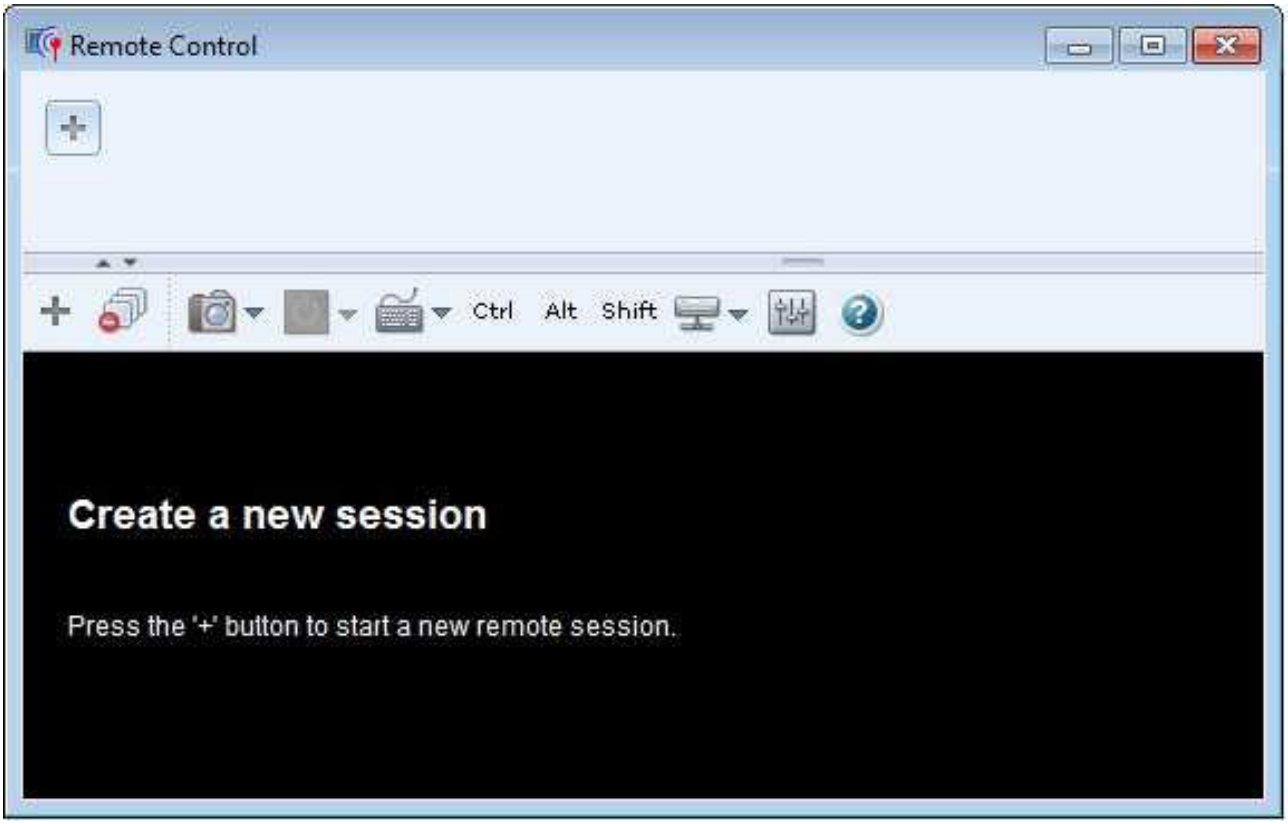
Step 7. When you are prompted, choose whether to save a shortcut to the remote-control session on your local system.

If you save the shortcut, you can then use this shortcut to open a remote-control session to the specified server without having to launch it from the XClarity Administrator web interface. However, your local system must have access to XClarity Administrator to validate the user account with the XClarity Administrator authentication server.

The shortcut contains a link that opens an empty remote-control session to which you can manually add servers.

Results

The Remote Control window is displayed.



The thumbnail area displays thumbnails of all server sessions that are currently managed through the remote-control session.

You can display multiple server sessions and move between server sessions by clicking a thumbnail, which displays the server console in the video session area. If you are accessing more servers than fit in the thumbnail area, click the **Scroll right** icon ( ) and **Scroll left** icon ( ) to scroll to additional server thumbnails. Click the **All sessions** icon ( ) to see a list of all open server sessions.

From the thumbnail area, click the **Add server** icon ( ) to add a new server to the list of servers that you are managing. For more information about adding a session, see Adding a server console to remote-control session. You can control whether the thumbnail area is displayed and how often the thumbnails are

refreshed from the Thumbnail page. For more information about thumbnail settings, see Setting remote-control preferences.

What to do next

If the remote-control session does not open successfully, see Remote control issues in the XClarity Administrator online documentation.

From the Remote Control dialog, you can perform the following actions:

- Add a session to other servers to the current remote-control session (see Adding a server console to remote-control session).
- Hide or show the thumbnail area by clicking the **Toggle Thumbnails** icon ().
- Display the remote-control session as a window or full screen by clicking the **Screen** icon () and then clicking **Toggle on full screen** or **Toggle off full screen**.
- Use Ctrl, Alt, and Shift keys in a remote-control session (see Using Ctrl, Alt, and Shift keys).
- Define custom key sequences, known as softkeys (seeDefining softkeys).
- Take a screen capture of the currently selected server session, and save that screen capture in a variety of formats by clicking the **Screen** icon (), and then clicking **Screenshot**.
- Mount remote media (such as CD, DVD, or USB device, disk image, or CD (ISO) image) to the selected server, or move a mounted device to another server (see Mounting or moving remote media).
- Upload images to a server from remote media (see Uploading an image to the server).
- Power the server on or off from a remote console (see Powering on and off a server from a remote control session).
- Change remote-control preferences (see Setting remote-control preferences).

Remote control considerations

Be aware of security, performance, and keyboard considerations that are related to accessing managed servers using a remote-control session.

Security considerations

The user account that is used to start the remote-control session must be a valid user account that has been defined in the Lenovo XClarity Administrator authentication server. The user account must also have sufficient user authority to access and manage a server.

By default, multiple remote-control sessions can be established to a server. However, when you start a remote-control session, you have the option to start the session in single-user mode, which establishes an exclusive session with the server. All other remote-control sessions to that server are blocked until you disconnect from the server.

Note: This option is available only if there are currently no other remote-control sessions established to the server.

To use Federal Information Processing Standard (FIPS) 140, you must enable it manually by completing the following steps on your local system:

1. Find the provider name of the FIPS 140 certified cryptographic provider that is installed on your local system.

   Tip: For more information about FIPS 140 compliance, see the FIPS 140 Compliant Mode for SunJSSE website.

2. Edit the file `$(java.home)/lib/security/java.security`.
3. Modify the line that includes `com.sun.net.ssl.internal.ssl.Provider` by appending the provider name of your FIPS 140 certified cryptographic provider. For example, change:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
   to:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Performance considerations

If a remote-control session becomes slow or unresponsive, close all video and remote media sessions that you have established with the selected server to reduce the number of open server connections. In addition, you might increase performance by changing the following preferences. For more information, see Setting remote-control preferences.

- **KVM**
  - Decrease the percentage of video bandwidth that is used by the application. The image quality of the remote-control session will be reduced.
  - Decrease the percentage of frames that are refreshed by the application. The refresh rate of the remote-control session will be reduced.
- **Thumbnails**
  - Increase the thumbnail refresh interval rate. The application will refresh thumbnails at a slower rate.
  - Turn off the display of thumbnails completely.

The size of the remote-control session window and the number of active sessions might affect workstation resources, such as memory and network bandwidth, which can influence performance. The remote-control session uses a soft limit of 32 open sessions. If more than 32 sessions are open, performance might be severely degraded, and the remote-control session might become unresponsive. You might see performance degradation with fewer than 32 open sessions if resources, including network bandwidth and local memory, are not sufficient.

Keyboard considerations

The remote-control session supports the following keyboard types:
- Belgian 105-key
- Brazilian
- Chinese
- French 105-key
- German 105-key
- Italian 105-key
- Japanese 109-key
- Korean
- Portuguese
- Russian
- Spanish 105-key
- Swiss 105-key
- UK 105-key
- US 104-key

For information about keyboard preferences, see Setting remote-control preferences.

Adding a server console to remote-control session

You can add one or more servers consoles to the current remote-control session.

Procedure

To add one or more servers consoles to the current remote-control session, complete the following steps.

Step 1. From the Remote Control window, click the **New Session** icon ().

A dialog is displayed with a list of available chassis and rack servers that are managed by Lenovo XClarity Administrator and that your user account has permission to manage.

Tip: If no servers are shown in the list, see Remote control issues in the XClarity Administrator online documentation for procedures to potentially resolve the issue.

Step 2. Select one or more servers to which you want to connect.

You can filter the servers that are displayed by selecting a system type from the **Type** drop-down list and entering text (such as a system name or enclosure name) in the **Filter** field.

You can select **Select all** to select all server in the list.

Step 3. Optional: **Optional:** Select **Single-user mode** to open an exclusive session to each selected server.

If you select this option, all other remote-control sessions to the selected servers are blocked until you disconnect from the selected servers. This option is available only if there are no other remote-control sessions established to the selected servers.

If you do not select this option, the multi-user mode is used by default.

Step 4. Click **Connect**.

Powering on and off a server from a remote control session

You can power on and off a server from a remote-control session.

Procedure

Complete the following steps to power on and off a server.

Step 1. From the Remote Control window, click the thumbnail for the server that you want to power on or off.

Step 2. Click the **Power** icon (), and then click one of the following power actions:

- **Power on**
- **Power Off Normally**
- **Power Off Immediately**
- **Restart Normally**
- **Restart Immediately**
- **Trigger NMI**
- **Restart to System Setup** (Lenovo Converged, Flex System, NeXtScale, and System x servers only)

Tip: The **Power** icon is green if the server is currently powered on.

Defining softkeys

You can define your own custom key sequences, called *softkeys*, for the current remote-control session.

Before you begin

To display the current list of softkey definitions, click the **Keyboard** icon ().

Softkey definitions are stored on the system from which you started the remote-control session. Therefore, if you launch the remote-control session from another system, you have to define the softkeys again.

You can choose to export user settings (which includes softkeys) from the **User Settings** tab on the Preferences dialog. For more information, see Importing and exporting user settings.

Note: If you use an international keyboard and define softkeys that require the Alternate Graphics key (AltGr), ensure that the operating system on the workstation that you use to invoke the remote-control application is the same type of operating system as the one on the server that you are remotely accessing. For example, if the server is running Linux, ensure that you invoke the remote-control session from a workstation that is running Linux.

Procedure

Complete the following procedure to add a softkey.

Step 1. From the Remote Control window, click the **Keyboard** icon (), and then click **Add softkey**. The **Softkey Programmer** tab on the Preference dialog is displayed.

Step 2. Click **New**.

Step 3. Type the key sequence that you want to define.

Step 4. Click **OK**. The new softkey is added to the softkey list.

Using Ctrl, Alt, and Shift keys

Some operating systems intercept certain keys instead of passing them to the remote server. You can use the sticky key buttons to send keystrokes directly to the server that you are managing.

Procedure

To send a Ctrl or Alt key combinations, click **Ctrl** or **Alt** in the toolbar, place the cursor in the video session area, and press a key on the keyboard.

For example, to send a Ctrl+Alt+Del key combination, complete the following steps:

1. Click **Ctrl** in the toolbar.
2. Click **Alt** in the toolbar.
3. Left-click anywhere inside the video session area.
4. Press the Delete key on the keyboard.

Note: If mouse-capture mode is enabled, press the left Alt key to move the cursor outside of the video session area. Although mouse-capture mode is disabled by default, you can enable it from the Toolbar page (see Setting remote-control preferences).

When you click **Ctrl**, **Alt**, or **Shift** in the toolbar to make the key active, the key remains active until you press a keyboard key or click the button again.

Mounting or moving remote media

You can use the remote- media feature to mount remote media (such as a CD, DVD, or USB device, disk image, or CD (ISO) image) that is on the local system to the selected server. You can also upload an image to the local storage that is available on the baseboard management-controller (BMC).

Before you begin

Only one user at a time can mount and upload data to the local storage on the management controller. Other users are prevented from accessing the local storage on the management controller while it is mounted or while data is being uploaded to the local storage.

On a server that is running the Linux operating system, mounting more than one ISO image is not supported.

Procedure

Complete the following steps to mount or move remote media.

Step 1. From the Remote Control window, click the **Remote Media** icon ().

Step 2. Click one of the following actions:

- **Mount remote media**

  This action makes local media resources available to the currently selected server. A media resource can be mounted to only one server at a time within a single remote-control session.

  When you click **Mount remote media**, the following options are available:

  - **Select an image to be mounted**. The image is available for the currently selected server until you unmount the device or close the remote-control session. Multiple images can be mounted to a single server, and each image can be mounted to multiple servers.
  - **Select a drive, such as a CD, DVD, or USB device, that is to be mounted**. The device is available to the currently selected server until you unmount the drive or close the remote-control session. Multiple devices can be mounted to a single server, but each device can be mounted to only one server at a time.

    Note: If you select a drive, be sure to unmount the drive before you remove media from the drive.
  - **Upload the image to the IMM**. Use this option to store an image in local storage on the management controller for the selected server. The image remains on the management controller even if you end the remote-control session or if the server is restarted.

    You can store approximately 50 MB of data on the management controller.

    You can upload multiple images to the management controller provided that the total space that is used for all images is less than 50 MB.

    Each image that is uploaded to the management controller is automatically mounted to the server. After you have uploaded an image to the management controller, you can also move that uploaded image to the management controller for a different server. When you move the image, the previously uploaded image is removed from the current server and uploaded to a selected server.

- **Move remote media**

  This action moves a previously mounted media resource between servers.

  Complete the following steps to make a resource available to a server:

  1. Select one or more resources.
  2. Click **Add** to move the resources to the **Selected Resources** list.
  3. Click **Mount** to mount the resources for use by the server. The remote-control session defines a device for the resource and maps that device to a mount point for the currently selected server. You have the option to write-protect the mounted media.

Uploading an image to the server

You can upload an image to the local storage that is available on the baseboard management-controller (BMC) for the selected server.

About this task

The image remains on the management controller even if you end the remote-control session or if the server is restarted.

You can store approximately 50 MB of data on the management controller.

You can upload multiple images to the management controller provided that the total space that is used for all images is less than 50 MB.

Each image that is uploaded to the management controller is automatically mounted to the server. After you have uploaded an image to the management controller, you can also move that uploaded image to the management controller for a different server. When you move the image, the previously uploaded image is removed from the current server and uploaded to a selected server.

Procedure

Complete the following steps to upload an image to the server.

Step 1. From the Remote Control window, click the **Remote Media** icon ( ).

Step 2. Click **Mount remote media**.

Step 3. Click **Upload the image to the IMM**.

Importing and exporting user settings

You can choose to import or export user settings for the current remote-control session.

About this task

When you export user settings, all user settings for the current remote-control session are stored in a properties file on your local system. You can copy this properties file to another system and import those settings into the remote-control application to use the settings.

Procedure

Complete the following steps to import or export user settings for the current remote-control session.

Step 1. From the Remote Control window, click the **Preference** icon ( ).

Step 2. Click the **User Settings** tab.

Step 3. Click **Import** to import settings from an exported file, or click **Export** to save the all current user settings in a properties file on the local system.

Setting remote-control preferences

You can modify preference settings for the current remote-control session.

Procedure

Complete the following steps to modify remote-control preferences.

Step 1. To modify the remote control preferences, click the **Preferences** icon ( ). All changes take effect immediately.

- **KVM**
  - **Percentage of Video Bandwidth**. Increasing the bandwidth improves the quality in the appearance of the remote-control session but might affect the performance of the remote-control session.

- **Percentage of Frames Refreshed**. Increasing the frame-refresh percentage increases how often the remote-control session is updated but might affect the performance of the remote-control session.
- **Keyboard type**. Select the type of keyboard that you are using for the remote-control session. The keyboard type that you select must match the keyboard settings in the local system and match the keyboard settings on the remote host.

  Note: If you select an international keyboard and you need to enter key combinations that require the Alternate Graphics key (AltGr), ensure that the operating system on the workstation that you use to invoke the remote-control session is the same type of operating system as the one on the server that you want to remotely access. For example, if the server is running Linux, ensure that you invoke the remote-control application from a workstation that is running Linux.
- **Scale image to window**. Select this option to scale the video image that is received from the server to the size of the video session area.

- **Security**
  - **Prefer single-user mode connections**. Specify whether single-user mode connections is the default choice when connecting to a server. When a connection is made in single-user mode, only one user can be connected to a server at a time. If this box is not selected, the default function is to connect to the server in multi-user mode.
  - **Require (secure) tunneling connections**. Select this option to access a server through the management node. You can use this option to access a server from a client that is not on the same network as the server.

    Note: The remote-control application always attempts to connect directly to the server from the local system where remote control was launched. If you select this option, the remote-control application accesses the server through Lenovo XClarity Administrator if the client workstation cannot access the server directly.
- **Toolbar**

  Note: Click **Restore defaults** to restore all settings on this page to the default settings
  - **Pin the toolbar to the window**. By default, the toolbar is hidden above the remote-control session window and displays only when you move your mouse pointer over it. If you select this option, the toolbar is pinned to the window and is always displayed between the thumbnail panel and the remote-control session window.
  - **Show keyboard buttons**. Specify whether to display the keyboard-button icons (CapsLock, NumLock, and ScrollLock) on the toolbar.
  - **Show power control**. Specify whether to display the power-control options on the toolbar.
  - **Show sticky key buttons**. Specify whether to display the sticky-key button icons (Ctrl, Alt, and Delete) on the toolbar.
  - **Hide local mouse pointer**. Specify whether to display the local mouse pointer when you position the cursor in the server session that is currently displayed in the video session area.
  - **Enable mouse-capture mode**. By default, mouse-capture mode is disabled. This means that you can freely move the cursor in and out of the video session area. If you enable mouse-capture mode, you must press the left Alt key before you can move the cursor out of the video session area. If mouse-capture mode is enabled, you can specify whether to use the Ctrl+Alt keys to exit mouse-capture mode. The default is to use the left Alt key.
  - **Specify toolbar background opacity**. Lowering the opacity percentage displays more of the video session area through the toolbar background.

    Note: This option is available only when the toolbar is not pinned to the window.

- **Thumbnails**
  - **Show thumbnails**. Select this option to show the thumbnail area in the remote-control session.
  - **Specify thumbnail refresh interval**. Decreasing the interval for refreshing thumbnails increases how often the server thumbnails are updated.
- **General**
  - **Debug mode**. Specify whether to set debug mode for the remote-control application. The settings determine the granularity of events that are logged in the log files. By default, only severe events are logged. For more information about log-file locations, see Viewing remote-control logs and traces.
  - **Inherit system appearance settings**. This setting changes the appearance to match color schemes that are configured for the local server (running Windows). You must restart the remote-control application for these settings to take effect.
  - C**reate desktop icon**. This setting creates a desktop icon on your local system so that you can start the remote-control application directly from your system. You must still have access to the management software from your system.
  - **Synchronize with management server**. This setting ensures that the server data that is displayed in the remote-control application matches the server data that is displayed from management software.

Viewing remote-control logs and traces

When you start a remote-control session, log files are created. The types of events that are logged in these files are based on the debug mode, which is set from **General** tab on the Preferences dialog. You can use these log files to resolve issues.

Procedure

Remote-control log files are stored in the following locations.

Operating system	Log directory
Windows 7 and 8	`%USERPROFILE%\lenovo\remoteaccess` For example: `C:\Users\win_user\lenovo\remoteaccess`

For more information about collecting diagnostic files and sending files to Lenovo Support, see Working with service and support in the Lenovo XClarity Administrator online documentation.

Managing access to operating-systems on managed servers

You can manage access to operating systems on the managed servers.

Before you begin

You must have **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** or **lxc-hw-admin** authority to manage and deploy device drivers and to perform power actions on managed servers from the Windows Driver Updates pages.

About this task

Before Lenovo XClarity Administrator can update OS device drivers on a managed system, you must provide information to access the host operating system, including the OS IP address and stored administrator credential for accessing the host operating system. For more information about updating OS device drivers, see Updating Windows device drivers on managed servers.

XClarity Administrator uses stored credentials to authenticate with the host operating system. For more information about creating stored credentials in XClarity Administrator, see Managing stored credentials.

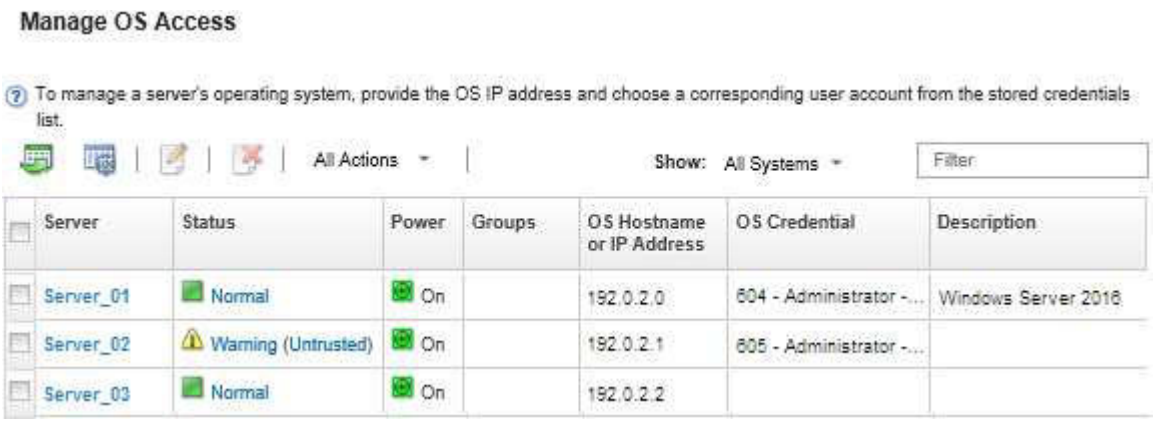
Tip: XClarity Administrator does not automatically validate the information that you specify on this page.

Procedure

Complete the following steps to modify the operating-system properties.

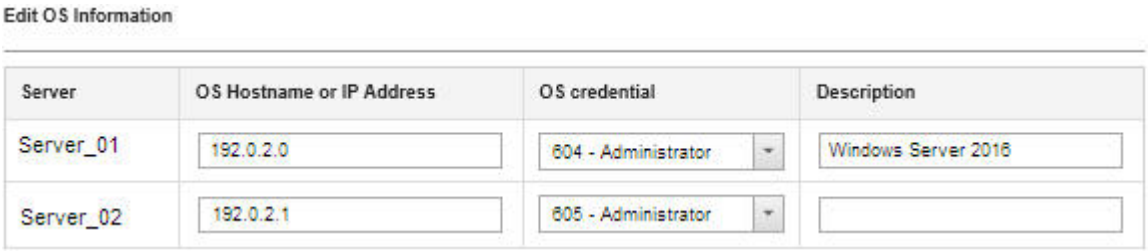
Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Access** to display the Manage OS Access page.

You can sort the table columns to make it easier to find the specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a system name or IP address) in the **Filter** field to further filter the servers that are displayed.



Step 2. Select the servers to be updated.

Step 3. Click **Edit OS information** icon ( ) to display the Edit OS information dialog.



Step 4. For each target server, specify the following information:
- IP address or host name of the host operating system
- (Optional) Stored credential for accessing the host operating system
- (Optional) Description of the host operating system

Step 5. Click **Save**.

What to do next

You can perform the following actions for managing operating-system access.

- Clear operating-system information (IP address, credentials, and description) by selecting the server, and clicking the **Remove OS Information** icon ( ).
- Test the authentication on Windows servers by clicking **Provisioning → Windows Driver Updates: Apply**, selecting the target server, and then clicking **Check Authentication**.

- View deployment information for the operating system on a specific server by hovering over the server name.

  Note: Deployment information is available only for operating systems that were successfully deploying by the XClarity Administrator instance. Deployment information is not available for failed deployments and for deployments there were performed by other means, including another XClarity Administrator instance.

Viewing Features on Demand keys

You can view a list of Features on Demand keys that are currently installed on the managed servers.

About this task

You cannot purchase, install, or manage Features on Demand key from the Lenovo XClarity Administrator web interface. For information about acquiring and installing Features on Demand keys, see Features on Demand in the XClarity Administrator online documentation.

Procedure

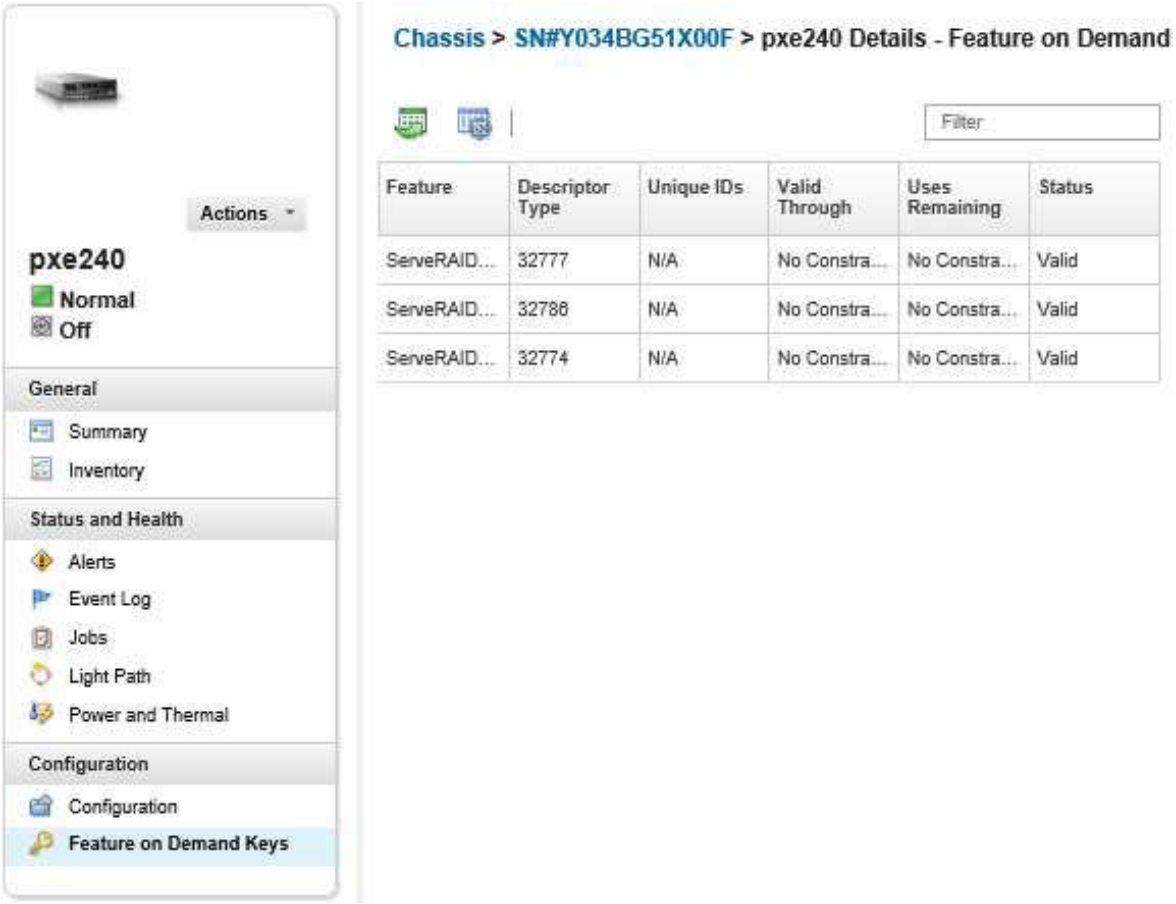
Complete the following steps to display a list of FoD keys that are installed in a specific managed server.

Step 1. From the XClarity Administrator menu, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack and tower servers and compute nodes).

Step 2. Click the server name in the **Server** column. The status summary page for that server is displayed, showing the server properties and a list of components that are installed in that server.

Step 3. Click **Inventory Details** under General in the left navigation, and expand each hardware component section to view the FoD unique IDs for those components.

Step 4. Click **Features on Demand keys** under Configuration in the left navigation to view information about all FoD keys that are installed on the server.



Managing energy and temperature

You can monitor and manage the power consumption and temperature of Converged, NeXtScale, System x, and ThinkServer servers, and improve energy efficiency using Lenovo XClarity Energy Manager.

Learn more: Lenovo XClarity Energy Manager

About this task

XClarity Administrator is a standalone user interface that you can use to monitor and manage the power consumption and temperature of supported servers, including:

- Monitoring energy consumption, estimating the power demand, and reallocating power to servers as needed.
- Monitoring the temperature and cooling capacity of servers.
- Sending notifications when certain events occur or when thresholds are exceeded.
- Limiting the amount of energy that a device consumes using policies.
- Optimizing energy efficiency by monitoring real-time inlet temperatures, identifying low-usage servers based on out-of-band power data, measuring power rangers for different server models, and evaluating how servers accommodate new workloads based on the availability of resources.
- Reducing the power consumption to a minimum level to prolong service time during an emergency power event (such as a data-center power failure).

For more information about how to download, install, and use XClarity Administrator, see Lenovo XClarity Energy Manager website.

Powering on and off a server

You can power on and off a server from Lenovo XClarity Administrator.

Before you begin

- For Red Hat® Enterprise Linux (RHEL) v7 and later, restarting the operating system from a graphical mode suspends the server by default. Before you can perform the **Restart Normally** or **Restart Immediately** actions from XClarity Administrator, you must manually configure the operating system to change the behavior of the power button to power off. For instructions, see the Red Hat Data Migration and Administration Guide: Changing behavior when pressing the power button in graphical target mode.
- For SUSE Linux Enterprise Server (SLES), powering off the operating system requires you to enter the root password on the SLES session. Before you can perform the **Power Off Normally** or **Power Off Immediately** actions from XClarity Administrator, you must manually power off the server using the local SLES interface and select the **Remember authentication** option when you enter the password, or check your security policy to see if mandatory authentication can be disabled.
- When enabled, the Wake-on-LAN boot option can interfere with XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.
- The power action **Restart to System Setup** restarts the server and then opens the BIOS/UEFI Startup utility in a remote-control session rather than a normal operating-system boot.
- The power actions **Power Off Normally** and **Power Off Immediately** depend on the configurations of the operating system that is installed on the device and work only if the operating system is configured to support them.
- You can restart the device with non-maskable interrupt (NMI) by clicking **All Actions → Service → Trigger NMI**.

Procedure

Complete the following procedure to power on or off a server.

Step 1. From the XClarity Administrator menu, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

Step 2. Select the server.

Step 3. Click **All Actions → Power Actions**, and then click one of the following power actions:
- **Power On** powers on the device.
- **Power Off Normally** shuts down the operating system and powers off the device.
- **Power Off Immediately** powers off the device.
- **Restart Normally** shuts down the operating system and restarts the device.
- **Restart Immediately** restarts the device
- **Restart to System Setup** restarts the device to BIOS/UEFI (F1) Setup. This is supported for non-ThinkServer servers that are supported without limitations.
- **Restart Management Controller** restarts the BMC.
- **Restart immediately and attempt PXE Network Boot** restarts the server immediately and boots the server to the Preboot Execution Environment (PXE) network. This is supported for Lenovo Flex System, System x, and ThinkSystem servers.

  Note: PXE-boot related UEFI settings must be configured on the server.

Virtually reseating a server in a Flex System chassis

You can simulate removing and reinserting a server in a Flex System chassis by restarting the server using a non-maskable interrupt (NMI).

About this task

During the virtual reseat, all existing network connections to the server are lost, and the power state of the server changes. Before performing a virtual reseat, ensure that you have saved all user data.

Attention:

- Do not perform a virtual reseat unless you are instructed by Lenovo Support.
- Performing a virtual reseat might result in the loss of data. Before reseating the server, perform necessary operations to protect user data.
- Instead of performing a virtual reseat, consider powering off the server. For information about power actions, see Powering on and off a server).

Procedure

Complete the following steps to virtually reseat a server in a Flex System chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers.

You can sort the table columns to make it easier to find the server that you want to reseat. In addition, you can select a device type from the **All Devices** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.



Step 2. Select the server in the table.

Step 3. Click **All Actions → Service → Virtual Reseat**.

Step 4. Click **Virtual Reseat**.

Launching the management controller interface for a server

You can launch the management controller web interface for a specific server from Lenovo XClarity Administrator.

Before you begin

To access ThinkSystem SR635 SR655 servers through XClarity Administrator, a user must have **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin**, or **lxc-os-admin** authority (see Managing the authentication server).

Single sign-on is supported for server, including ThinkSystem and ThinkAgile servers (except SR635, SR655, SR645, and SR665). This means that you can launch the management interface for a managed servers from XClarity Administrator without having the log in.

To login directly to the XCC using local or external LDAP user accounts without logging in to the XClarity Administrator, use the URL `https://{XCC_IP_adderss}/#/login`.

Procedure

Complete the following steps to launch the management controller interface for a server.

Note: Launching any management controller interface from Lenovo XClarity Administrator using the Safari web browser is not supported.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers** to display the Servers page.

You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.



Step 2. Click the link for the server in the **Server** column. The status summary page for that server is displayed.

Step 3. Click **All Actions → Launch → Management Web Interface**. The management controller web interface for the server is started.

Tip: You can also click the IP address in the **IP Addresses** column to launch the management controller interface.

Step 4. Log in to the management controller interface using your XClarity Administrator user credentials.

What to do next

For more information about using the management controller interface for a server, see Integrated Management Module II online documentation and XClarity Controller online documentation.

Modifying the system properties for a server

You can modify the system properties for a specific server.

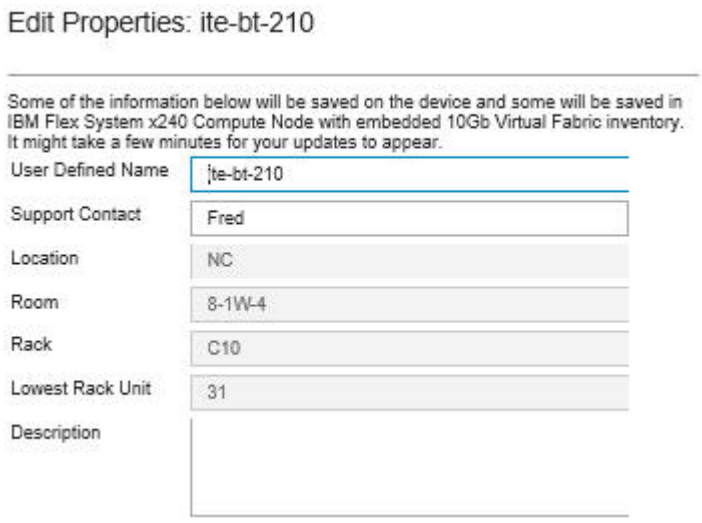
Procedure

Complete the following steps to modify the system properties.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Servers** to display the Servers page.

Step 2. Select the server to be updated.

Step 3. Click **All Actions → Inventory → Edit Properties** to display the Edit dialog.



Step 4. Change the following information, as needed.
- User-defined name for the server
- Support contact
- Description

Note: The location, room, rack, and lowest rack unit properties are updated by XClarity Administrator when you add or remove devices from a rack in the web interface (see Managing racks).

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface.

Resolving expired or invalid stored credentials for a server

When a stored credential becomes expired or inoperable on a device, the status for that device is shown as “Offline.”

Procedure

To resolve expired or invalid stored credentials for a server.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).



Step 2. Click the **Power** table column header to group all offline server at the top of the table.

In addition, you can select a system type from the All Systems drop-down list and enter text (such as a system name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 3. Select the server to be resolved.

Step 4. Click **All Actions → Security → Edit Stored Credentials**.

Step 5. Change the password for the stored credential or select another stored credential to use for the managed device.

Note: If you managed more than one device using the same stored credentials and you change the password for the stored credentials, that password change affects all devices that are currently using the stored credentials.

Recovering a failed server after deploying a server pattern

If a server fails after you deploy a server pattern, you can recover the server by unassigning the profile from the failed server and then reassigning that profile to a standby server.

Procedure

Complete the following steps to recover the failed server that uses Lenovo XClarity Administrator managed authentication.

Step 1. Identify the failed server.

Step 2. Unassign the server profile from the failed server (see Deactivating a server profile).

Attention: The failed server must be powered off to deactivate the assigned virtual addresses *before* you re-assign the profile. When you unassign the server profile, select **Power off server** on the Unassign Server Profile dialog to power off the failed server (see Powering on and off a server).

Step 3. Assign the server profile to a standby server (see Activating a server profile).

Step 4. Activate the profile by either powering on the standby server if it is currently powered off or by restarting the standby server if it is currently powered on (see Powering on and off a server).

Step 5. Migrate the VLAN settings on the attached switches to the standby server.

Step 6. Ensure that the failed server is powered off.

Step 7. Replace or repair the failed server. If you repair the server, perform the following steps to ensure that the newly repaired server is reset to default settings:

a. Reset the BMC to factory defaults by using the management web interface for the server. For information about resetting the BMC, see Recovering ThinkSystem, Converged, NeXtScale, or

System x M5 or M6 server management after a management server failure by resetting the management controller.

b. Clear the Unified Extensible Firmware Interface (UEFI) information, including any I/O adapter virtual addresses by using the UEFI menus. For information, see the UEFI documentation.

Recovering boot settings after server pattern deployment

If one or more servers do not start after you deployed a new server pattern to those servers, the problem might be that the boot settings were overwritten with the default boot settings that are in the server pattern. For operating systems that are installed in UEFI mode, restoring the default settings might require additional configuration steps to restore the boot configuration.

Procedure

Complete the following manual recovery procedure for each affected server to restore the original boot settings.

- For a server with Red Hat Enterprise Linux installed:
  1. If you are accessing the server remotely, establish a remote-control session to the server (see Using remote control to manage Converged, Flex System, NeXtScale, and System x servers).
  2. Restart the server by clicking **Tools → Power → On**. When the UEFI splash screen for the server is displayed in the Remote Control session, press F1 to display the Setup Utility.
  3. Select **Boot Manager**.
  4. Select **Add Boot Option**.
  5. Select **UEFI Full Path Option**.
  6. From the list that is displayed, select the entry that includes `SAS`.
  7. Select **EFI**.
  8. Select **redhat**.
  9. Select **grub.efi**.
  10. Select the **Input the Description** field.
  11. Type `Red Hat Enterprise Linux`.
  12. Select **Commit Changes**.
  13. Make `Red Hat Enterprise Linux` the first option in the Boot Order, and remove all other options in the Boot Order.
  14. Press Escape, and then select **Save changes then exit this menu**.
  15. Press Escape, and then select **Exit the Configuration Utility and Reboot**. The compute node restarts.
- For a server with Microsoft Windows Server 2008 installed:
  1. Power on the server, and when prompted, press F1 to enter setup.
  2. Select **Boot Manager**.
  3. Select **Boot from File**.
  4. Select the GUID Partition Tables (GPT) System Partition where you installed Microsoft Windows Server 2008.
  5. Select **EFI**.
  6. Select **Microsoft**.
  7. Select **Boot**.

8. Select **bootmgfw.EFI**.

Note: For more information, see RETAIN tip 5079636.

Recovering rack or tower server management after a management server failure

If a rack or tower server is being managed by Lenovo XClarity Administrator, and if XClarity Administrator fails, you can restore the management functions until the XClarity Administrator is restored or replaced.

About this task

To recover management for a Flex System server, see Recovering management with a CMM after a management server failure.

Recovering rack or tower server management after a management server failure by force management

You can recover server management by managing the server again using the force-management option

Procedure

If the replacement Lenovo XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the `RECOVERY_ID` account and password and the **Force management** option (see Managing servers).

Recovering a System x or NeXtScale M4 server that was not unmanaged correctly by using the management controller

You can recover management of a System x or NeXtScale M4 server by using the baseboard management-controller (BMC).

Procedure

Complete the following steps to recover server management. of a server that uses Lenovo XClarity Administrator managed authentication.

Step 1. Log in to the management-controller web interface using the user account and password that you created before the server was managed by XClarity Administrator

Step 2. Clear SNMP trap settings.

a. Click the **IMM Management → Network**.

b. Click the **SNMP** tab.

c. Click the **Communities** tab,

d. Locate the community entry for the previous XClarity Administrator, fox example.
- **LXCA IP address:** 10.240.198.84
- **LXCA host:** LXCA_maqCBlt86d
- **Community 2:**
- **Community name:** LXCA_maqCBlt86d
- **Access type:** Trap
- **Allow specific hosts to receive traps on this community:** 10.240.198.84

e. Remove the value in the fields for the community entry.

f. Click **Apply**.

Step 3. Clear the user accounts.

a. Click the **IMM Management → Users**.

b. Click the **User Accounts** tab.

c. Delete all user accounts that are XClarity Administrator, including user accounts with the following prefixes:
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

What to do next

After XClarity Administrator is restored or replaced, you can manage the System x or NeXtScale server again (see Managing servers). All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by resetting the management controller

You can recover management of a ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server by resetting the baseboard management-controller in the server to factory defaults.

Procedure

Complete the following steps to recover management of a server that uses Lenovo XClarity Administrator managed authentication.

Step 1. If Encapsulation is enabled on the device, connect to the target management controller from a system that is configured to use the IP address of the failed XClarity Administrator virtual appliance.

Step 2. Reset the management controller to the factory defaults.

a. Log in to the management controller web interface for the server using the recovery user account and password that you created before the server was managed by XClarity Administrator.

b. Click the **IMM Management tab**.

c. Click **IMM Reset to factory defaults**.

d. Click **OK** to confirm the reset action.

Important: After the BMC configuration is complete, the BMC is restarted. If this is a local server, your TCP/IP connection is broken and you must reconfigure the network interface to restore connectivity.

Step 3. Log on to the management controller web interface for the server again.

- The BMC is initially configured to attempt to obtain an IP address from a DHCP server. If it cannot, it uses the static IPv4 address `192.168.70.125`.
- The IMMBMC is set initially with a user name of `USERID` and password of `PASSWORD` (with a zero). This default user account has Supervisor access. Change this user name and password during your initial configuration for enhanced security.

Step 4. Reconfigure the network interface to restore connectivity. For more information, see the Integrated Management Module II online documentation.

What to do next

After XClarity Administrator is restored or replaced, you can manage the server again (see Managing servers). All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

If the server was configured using Configuration Patterns, you can deactivate and then re-activate the server profile that was assigned to the server to apply the configuration (see Working with server profiles).

Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by using cimcli

You can recover management of a ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server by using the **cimcli** utility to clear the CIM subscriptions.

Before you begin

OpenPegasus with the cimcli utility must be installed on a system that has network access to the target server. For information about downloading, configuring, and compiling OpenPegasus, see the OpenPegasus Release RPMs for Linux website.

Note: For Red Hat Enterprise Linux (RHEL) Server 7 and later, OpenPegasus source and binary RPMs are included as part of the Red Hat distribution. The `top-pegasus-test.x86_64` package includes the cimcli utility.

About this task

After the server is recovered, you can manage the server again. All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

Procedure

Complete the following steps from a server that uses Lenovo XClarity Administrator managed authentication and on which OpenPegasus is installed to recover server management.

Step 1. If Encapsulation is enabled on the device:

a. Connect to the target server from a system that is configured to use the IP address of the failed XClarity Administrator virtual appliance.

b. Disable Encapsulation by opening an SSH session to the device and running the following command:

```
encaps lite off
```

Step 2. Run the following commands to determine the CIM instances for CIM_ListenerDestinationCIMXML, CIM_Indicationfilter and CIM_IndicationSubscription.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

where, <*IP_address*>, <*user_ID*> and <*password*> are the IP address, user ID and password for the management controller. For example:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
```

```
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Step 3. Run following command to delete each the CIM instance for CIM_ListenerDestinationCIMXML, CIM_Indicationfilter and CIM_IndicationSubscription, one at a time.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

where, <*IP_address*>, <*user_ID*> and <*password*> are the IP address, user ID and password for the management controller, and <*cim_instance*> is the information returned for each CIM instance in the previous step, surrounded by single quotes. For example:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

What to do next

After Lenovo XClarity Administrator is restored or replaced, you can manage the System x or NeXtScale server again (see Managing servers). All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

Recovering ThinkServer server management after a management server failure by using the management controller interface

You can recover management of a ThinkServer server from the management controller interface.

Procedure

Complete the following steps to recover the server management.

Step 1. Log in to the management controller web interface for the server as an administrator (see Launching the management controller interface for a server).

Step 2. Remove the IPMI accounts created by Lenovo XClarity Administrator by selecting Users in the main menu and then removing all the user accounts with the “LXCA_” prefix.

Alternatively, you can rename the account user name, and remove the “LXCA_” prefix.

Step 3. Remove SNMP trap destinations by selecting **PEF Management** in the main menu, click the **LAN Destination** tab, and remove the entry that points to the IP address of the XClarity Administrator instance.

Step 4. Verify you have valid NTP settings by selecting **NTP Settings** in the main menu, and then either configuring the date and time manually or providing a valid NTP server address.

Unmanaging a rack or tower server

You can remove a rack or tower server from management by Lenovo XClarity Administrator. This process is called *unmanaging*.

Before you begin

You can enable XClarity Administrator to automatically unmanage devices (including Flex System chassis, Flex System and rack switches, Flex System servers, System x servers, ThinkAgile, and ThinkSystem servers) that are offline for a specific amount of time. This is disabled by default. To enable the automatic unmanagment of offline devices, click **Hardware → Discover and Manage New Devices** from the XClarity Administrator menu, and then click **Edit** next to **Unmanage offline devices is Disabled**. Then, select **Enable unmanage offline devices** and set the time interval. By default, devices are unmanaged after being offline for 24 hours.

Before you unmanage a rack or tower server, ensure that there are no active jobs running against the server.

If you want to remove the server pattern and any virtual addresses on the rack or tower server, deactivate the server profile before unmanaging the server (see Deactivating a server profile).

When Call Home is enabled in XClarity Administrator, Call Home is disabled on all managed chassis and servers to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time (see Re-enabling call home on all managed devices in the XClarity Administrator online documentation).

About this task

When you unmanage a rack or tower server, Lenovo XClarity Administrator performs the following actions:

- Clears the configuration used for centralized user management.
- Removes the baseboard-management-controller security certificate from the XClarity Administrator trust store.
- Removes access to the NTP server from the management controller.
- If Encapsulation is enabled on the device, configures the devices firewall rules to the settings before the device was managed.
- Removes the CIM subscriptions to the XClarity Administrator configuration so that XClarity Administrator no longer receives events from the rack or tower server.

- Disables Call Home on the rack or tower server if Call Home is currently enabled on XClarity Administrator.
- Discards events that were sent from the rack or tower server. You can retain these events by forwarding the events to an external repository, such as a syslog (see Forwarding events).

When you unmanaged a rack or tower server, XClarity Administrator retains certain information about the server. That information is reapplied when you manage the same rack or tower server again.

Important: If you unmanaged a ThinkServer server and then manage that server using another XClarity Administrator instance, information about the server is lost.

Tip: All demo devices that are optionally added during initial setup are nodes in a chassis. To unmanage the demo devices, unmanage the chassis using the **Force unmanage even if the device is not reachable** option.

Procedure

To umanage a rack or tower server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click the **Hardware → Servers** to display the Servers page.

Step 2. Select one or more rack or tower servers to be unmanaged.

Step 3. Click **Unmanage**. The Unmanage dialog is displayed.

Step 4. Optional: **Optional:** Select **Force unmanage even if the device is not reachable**.

Important: When unmanaging demo hardware, ensure that you select this option.

Step 5. Click **Unmanage**.The Unmanage dialog shows the progress of each step in the unmanagement process.

Step 6. When the unmanagement process is complete, click **OK**.

Recovering a rack or tower server that was not unmanaged correctly

If a Converged, NeXtScale, System x, or ThinkServer server was not unmanaged correctly, you must recover the server before you can remanage it.

Recovering a rack or tower server that was not unmanaged correctly by force management

You can recover server management by managing the server again using the force-management option

Procedure

If the replacement Lenovo XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the `RECOVERY_ID` account and password and the **Force management** option (see Managing servers).

Recovering a System x or NeXtScale M4 server that was not unmanaged correctly by using the management controller

You can recover System x or NeXtScale M4 server management by using the management controller.

Procedure

Complete the following steps to recover server management.

Step 1. Log in to the management-controller web interface using the user account and password that you created before the server was managed by XClarity Administrator

Step 2. Clear SNMP trap settings.

a. Click the **IMM Management → Network**.

b. Click the **SNMP** tab.

c. Click the **Communities** tab,

d. Locate the community entry for the previous XClarity Administrator, fox example.
   - **LXCA IP address:** 10.240.198.84
   - **LXCA host:** LXCA_maqCBIt86d
   - **Community 2:**
   - **Community name:** LXCA_maqCBIt86d
   - **Access type:** Trap
   - **Allow specific hosts to receive traps on this community:** 10.240.198.84

e. Remove the value in the fields for the community entry.

f. Click **Apply**.

Step 3. Clear the user accounts.

a. Click the **IMM Management → Users**.

b. Click the **User Accounts** tab.

c. Delete all user accounts that are XClarity Administrator, including user accounts with the following prefixes:
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

Step 4. Manage the server using Lenovo XClarity Administrator.

a. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.

b. Select **Manual Input**.

c. Click **Single System**, enter the IP address of the server that you want to manage, and click **OK**.

d. Specify the user ID and password for the authenticating to the server.

e. Click **Manage**.

   A dialog is displayed that shows the progress of this management process. Monitor the progress to ensure that the process completes successfully.

f. When the process is complete, click **OK**.

Recovering a ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server that was not unmanaged correctly by resetting the management controller to factory defaults

You can recover ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management by resetting the baseboard management-controller (BMC) in the server to factory defaults.

Procedure

Complete the following steps to recover server management.

Step 1. If Encapsulation is enabled on the device, connect to the target management controller from a system that is configured to use the IP address of the failed XClarity Administrator virtual appliance.

Step 2. Reset the management controller to the factory defaults.

a. Log in to the management controller web interface for the server using the recovery user account and password that you created before the server was managed by XClarity Administrator.

b. Click the **IMM Management tab**.

c. Click **IMM Reset to factory defaults**.

d. Click **OK** to confirm the reset action.

Important: After the BMC configuration is complete, the BMC is restarted. If this is a local server, your TCP/IP connection is broken and you must reconfigure the network interface to restore connectivity.

Step 3. Log on to the management controller web interface for the server again.

- The BMC is initially configured to attempt to obtain an IP address from a DHCP server. If it cannot, it uses the static IPv4 address `192.168.70.125`.
- The IMMBMC is set initially with a user name of `USERID` and password of `PASSWORD` (with a zero). This default user account has Supervisor access. Change this user name and password during your initial configuration for enhanced security.

Step 4. Reconfigure the network interface to restore connectivity. For more information, see the Integrated Management Module II online documentation.

Step 5. Manage the server using Lenovo XClarity Administrator.

a. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.

b. Select **Manual Input**.

c. Click **Single System**, enter the IP address of the server that you want to manage, and click **OK**.

d. Specify the user ID and password for the authenticating to the server.

e. Click **Manage**.

A dialog is displayed that shows the progress of this management process. Monitor the progress to ensure that the process completes successfully.

f. When the process is complete, click **OK**.

Step 6. If the server was configured using Configuration Patterns, re-activate the server profile that was assigned to the server.

a. From the XClarity Administrator menu bar, click **Provisioning → Server Profiles**. The Configuration Patterns: Server Profiles page is displayed.

b. Select the server profile, and click the **Deactivate server profile** icon ().

c. Click **Power off the ITE** to power off the server. When the server is powered back on, virtual address assignments revert back to the burned in defaults.

d. Click **Deactivate**. The state of the profile changes to “Inactive” in the Profile Status column. Note: Servers retain their identification information (for example, hostname, IP address, virtual MAC address) when a profile is deactivated.

e. Select the server profile again, and click the **Activate server profile** icon ().

f. Click **Activate** to activate the server profiles on the server. The state of the profile changes to “Active” in the Profile Status column.

Step 7. If a compliance policy was assigned to the server, reassign the compliance policy.

a. From the XClarity Administrator menu bar, click **Provisioning → Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed with a list of managed devices.

b. Select the appropriate policy for the server from the drop-down menu in the **Assigned Policy** column.

Recovering a ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server that was not unmanaged correctly by using the cimcli

You can recover ThinkSystem, Converged, NeXtScale, or System x server management by using the **cimcli** to clear the CIM subscriptions.

Before you begin

OpenPegasus with the cimcli utility must be installed on a system that has network access to the target server. For information about downloading, configuring, and compiling OpenPegasus, see the OpenPegasus Release RPMs for Linux website.

Note: For Red Hat Enterprise Linux (RHEL) Server 7 and later, OpenPegasus source and binary RPMs are included as part of the Red Hat distribution. The `top-pegasus-test.x86_64` package includes the cimcli utility.

About this task

After the server is recovered, you can manage the server again. All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

Procedure

Complete the following steps from a server that uses Lenovo XClarity Administrator managed authentication and on which OpenPegasus is installed to recover server management.

Step 1. If Encapsulation is enabled on the device:

a. Connect to the target server from a system that is configured to use the IP address of the failed XClarity Administrator virtual appliance.

b. Disable Encapsulation by opening an SSH session to the device and running the following command:

```
encaps lite off
```

Step 2. Run the following commands to determine the CIM instances for CIM_ListenerDestinationCIMXML, CIM_Indicationfilter and CIM_IndicationSubscription.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

where, <*IP_address*>, <*user_ID*> and <*password*> are the IP address, user ID and password for the management controller. For example:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
```

```
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Step 3. Run following command to delete each the CIM instance for CIM_ListenerDestinationCIMXML, CIM_Indicationfilter and CIM_IndicationSubscription, one at a time.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

where, <*IP_address*>, <*user_ID*> and <*password*> are the IP address, user ID and password for the management controller, and <*cim_instance*> is the information returned for each CIM instance in the previous step, surrounded by single quotes. For example:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Step 4. Manage the server using Lenovo XClarity Administrator.

a. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.

b. Select **Manual Input**.

c. Click **Single System**, enter the IP address of the server that you want to manage, and click **OK**.

d. Specify the user ID and password for the authenticating to the server.

e. Click **Manage**.

   A dialog is displayed that shows the progress of this management process. Monitor the progress to ensure that the process completes successfully.

f. When the process is complete, click **OK**.

Recovering a ThinkServer server management that was not unmanaged correctly by using the management controller interface

You can recover management of a ThinkServer server by using the management controller web interface.

Procedure

Complete the following steps to recover the server management.

Step 1. Log in to the management controller web interface for the server as an administrator (see Launching the management controller interface for a server).

Step 2. Remove the IPMI accounts created by Lenovo XClarity Administrator by selecting Users in the main menu and then removing all the user accounts with the “LXCA_” prefix.

Alternatively, you can rename the account user name, and remove the “LXCA_” prefix.

Step 3. Remove SNMP trap destinations by selecting **PEF Management** in the main menu, click the **LAN Destination** tab, and remove the entry that points to the IP address of the XClarity Administrator instance.

Step 4. Verify you have valid NTP settings by selecting **NTP Settings** in the main menu, and then either configuring the date and time manually or providing a valid NTP server address.

Chapter 9. Managing storage devices

Lenovo XClarity Administrator can manage several types of storage, including Lenovo Storage, Nimble, and Flex System storage systems.

Learn more:  XClarity Administrator: Discovery

Before you begin

Attention: Review the storage-management considerations before managing a storage device. For information, see Storage management considerations.

Note: Flex System storage devices are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed Flex System storage devices independent of the chassis.

Review the management considerations before managing a device. For information, see Management considerations in the XClarity Administrator online documentation.

Certain ports must be available to communicate with devices. Ensure that all required ports are available before you attempt to manage storage devices. For information about ports, see Port availability in the XClarity Administrator online documentation.

Ensure that the minimum required firmware is installed on each storage device that you want to manage using XClarity Administrator. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.

Important: Ensure that the following requirements are met before discovering and managing rack storage devices (other than ThinkSystem DE series). For more information, see Cannot discover a device and Cannot manage a device in the XClarity Administrator online documentation.

- The network configuration must allow SLP traffic between XClarity Administrator and the rack storage device.
- Unicast SLP is required.
- Multicast SLP is required if you want XClarity Administrator to discover the Lenovo Storage devices automatically. In addition, SLP must be enabled on the rack storage device.
- Multicast UDP is required if you want XClarity Administrator to discover Nimble storage devices and retrieve basic information. To verify that your network configuration allows multicast UDP traffic, use any client that is capable of browsing for mDNS or DNS-SD services (such as a “zeroconf” or “avahi-browse” client) to ensure that it can find the Nimble storage devices. The client must be run on a system in the same subnet as the XClarity Administrator instance.

  Note: Discovering and managing devices using bulk import does not require multicast UDP.

About this task

XClarity Administrator can automatically discover storage devices in your environment by probing for manageable devices that are on the same IP subnet as XClarity Administrator. To discover storage devices that are in other subnets, specify an IP address or range of IP addresses, or import information from a spreadsheet.

© Copyright Lenovo 2015, 2021

After the storage devices are managed by XClarity Administrator, XClarity Administrator polls each managed storage device periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed storage device and perform management actions (such as configuring system settings, updating firmware, and powering on and off).

A device can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device on the initial XClarity Administrator, and then manage it with the new XClarity Administrator. If an error occurs during the unmanagement process, you can select the **Force management** option during management on the new XClarity Administrator.

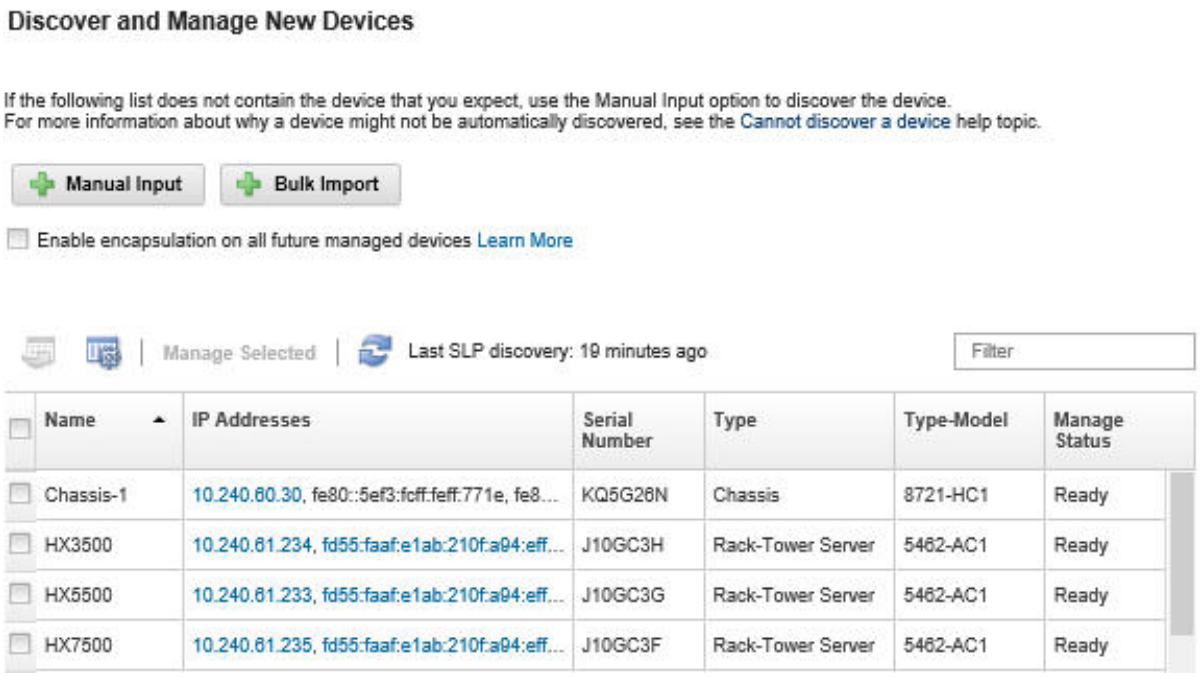
Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a device is already managed by another manager until after it attempts to manage the device.

- Management of Flex System storage devices by XClarity Administrator is limited. You can view status and detailed information for the storage devices, power on and off the storage device, virtually reseat the storage device, and launch the CMM for the chassis in which the storage device is installed. However, to perform other actions on a storage device (such as updating or configuring the storage device), you must use the management controller web interface or the command-line interface (CLI) for the storage device.
- You can use Flex System Manager to manage Flex System storage devices. However, you cannot use Flex System Manager and XClarity Administrator to manage storage devices in the same chassis at the same time.
- For more information about using the management controller web interface for Flex System storage devices, see Flex System Storage product documentation.

Procedure

Complete one of the following procedures to manage your Lenovo Storage or Nimble storage systems using XClarity Administrator.

- Discover and manage a large number of storage devices and other types of devices using a bulk-import file (see Managing systems in the XClarity Administrator online documentation).
- Discover and manage storage devices that are on the same IP subnet as XClarity Administrator.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage New Devices page is displayed.



You can sort the table columns to make it easier to find the storage devices that you want to manage. In addition, you can enter text (such as a name or IP address) in the **Filter** field to further filter the storage systems that are displayed. You can change the columns that are displayed and the default sort order by clicking the **Customize Columns** icon ( ).

2. Click the **Refresh** icon ( ) to discover all manageable devices in the XClarity Administrator domain. Discovery might take several minutes.
3. Select one or more storage devices that you want to manage.
4. Click **Manage Selected**. The Manage dialog is displayed.
5. Specify the user ID and password for authenticating to the storage device.

   Tip: It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).
6. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   – You can select from a list of role groups that are assigned to the current user.

   – If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.
7. Click **Manage**.

   A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.
8. When the process is complete, click **OK**.

   The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

   If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

– If the managing XClarity Administrator failed and cannot be recovered.

Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

– If the managing XClarity Administrator was taken down before the devices were unmanaged.

– If the devices were not unmanaged successfully.

Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

- Discover and manage storage devices that are not on the same IP subnet as XClarity Administrator by manually specifying IP addresses.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Select **Manual Input**.
  3. Specify the network addresses of the storage devices that you want to manage:
     – Click **Single System**, and enter a single IP address domain name, or fully-qualified domain name (FQDN).

     Note: To specify an FQDN, ensure that a valid domain name is specified on Network Access page (see Configuring network access).

     – Click **Multiple Systems**, and enter a range of IP addresses. To add another range, click the **Add** icon (). To remove a range, click the **Remove** icon ().
  4. Click **OK**.
  5. Specify the user ID and password for authenticating to the storage device.

     Tip: It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).
  6. Click **Change** to change the role groups that are to be assigned to the devices.

     Notes:

     – You can select from a list of role groups that are assigned to the current user.

     – If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.
  7. Click **Manage**.

     A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.
  8. When the process is complete, click **OK**.

     The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

     If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

     – If the managing XClarity Administrator failed and cannot be recovered.

Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

- If the managing XClarity Administrator was taken down before the devices were unmanaged.
- If the devices were not unmanaged successfully.

Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

What to do next

- Discover and manage additional devices.
- Update firmware on devices that are not in compliance with current policies (see Updating firmware on managed devices).
- Add the new devices to the appropriate rack to reflect the physical environment (see Managing racks).
- Monitor hardware status and details (see Viewing the status of storage devices).
- Monitor events and alerts (see Working with events and Working with alerts).

Storage management considerations

Before managing a storage device, review the following important considerations.

For information about port requirements, see Port availability in the Lenovo XClarity Administrator online documentation.

Important: Ensure that the following requirements are met before discovering and managing rack storage devices (other than ThinkSystem DE series). For more information, see Cannot discover a device and Cannot manage a device in the XClarity Administrator online documentation.

- The network configuration must allow SLP traffic between XClarity Administrator and the rack storage device.
- Unicast SLP is required.
- Multicast SLP is required if you want XClarity Administrator to discover the Lenovo Storage devices automatically. In addition, SLP must be enabled on the rack storage device.
- Multicast UDP is required if you want XClarity Administrator to discover Nimble storage devices and retrieve basic information. To verify that your network configuration allows multicast UDP traffic, use any client that is capable of browsing for mDNS or DNS-SD services (such as a “zeroconf” or “avahi-browse” client) to ensure that it can find the Nimble storage devices. The client must be run on a system in the same subnet as the XClarity Administrator instance.

  Note: Discovering and managing devices using bulk import does not require multicast UDP.

For Lenovo Storage devices, the system-level air temp is measured by the temperature sensor closest to the mid-plane of the system and reflects the ambient temperature after the airflow passes through the drives. Note that the air temperature that is reported by XClarity Administrator and the management controller might differ if the temperature is captured at different points in time.

For some storage devices, SNMP traps are in English only.

Viewing the status of storage devices

You can view a summary and detailed status for the managed storage devices from Lenovo XClarity Administrator.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

The following status icons are used to indicate the overall health of the device. If the certificates do not match, “(Untrusted)” is appended to the status of each applicable device, for example Warning (Untrusted). If there is a connectivity issue or a connection to the device is not trusted, “(Connectivity)” is appended to the status of each applicable device, for example Warning (Connectivity).

- () Critical
- () Warning
- () Pending
- () Informational
- () Normal
- () Offline
- () Unknown

Procedure

To view the status for a managed storage device, complete one or more of the following actions.

- From the Lenovo XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of all managed storage devices and other resources.



- From the Lenovo XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all storage devices that are installed in managed chassis.

  You can sort the table columns to make it easier to find the storage devices that you want to manage. In addition, enter text (such as a system name or IP address) in the **Filter** field and click the status icons to list only those storage devices that meet the selected criteria.



  From this page, you can perform the following actions:

  – View detailed information about the storage device and its components (see Viewing the details of a storage device).
  – View a storage device in graphical rack or chassis view by clicking **All Actions → Views → Show in Rack View** or **All Actions → Views → Show in Chassis View**.
  – Launch the management controller web interface for the storage device by clicking the **IP address** link (see Launching the management controller interface for a storage device).

- Power the storage controller in the storage device on and off (see Powering on and off a storage device).
- Modify system information by selecting a storage device and clicking **All Actions → Inventory → Edit Properties**.
- Refresh inventory by selecting a storage device and clicking **All Actions → Inventory → Refresh Inventory**.
- Export detailed information about one or more storage devices to a single CSV file by selecting the storage devices and clicking **All Actions → Inventory → Export Inventory**.

  Note: You can export inventory data for a maximum of 60 devices at one time.

  Tip: When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Unmanaged the storage device (see Unmanaging a Lenovo Storage or Nimble storage system).
- (Flex System storage devices only) Virtually reseat the storage controller in the storage device (see Virtually reseating storage controllers in a Flex System storage device).
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Exclude events** icon (). (see Excluding events).
- Resolve issues that might arise between the Lenovo XClarity Administrator security certificate and the security certificate of the CMM in the chassis where the storage device is installed by selecting a storage device and clicking **All Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).
- Add or remove a storage device from a static resource group by clicking **All Actions → Groups → Add to Group** or **All Actions → Groups → Remove from Group**.

Viewing the details of a storage device

You can view detailed information about managed storage devices from Lenovo XClarity Administrator, including the IP address, product name, serial number, and details about each canister.

About this task

Learn more:

-  XClarity Administrator: Inventory
-  XClarity Administrator: Monitoring

For Lenovo Storage devices, the system-level air temp is measured by the temperature sensor closest to the mid-plane of the system and reflects the ambient temperature after the airflow passes through the drives. Note that the air temperature that is reported by Lenovo XClarity Administrator and the management controller might differ if the temperature is captured at different points in time.

Procedure

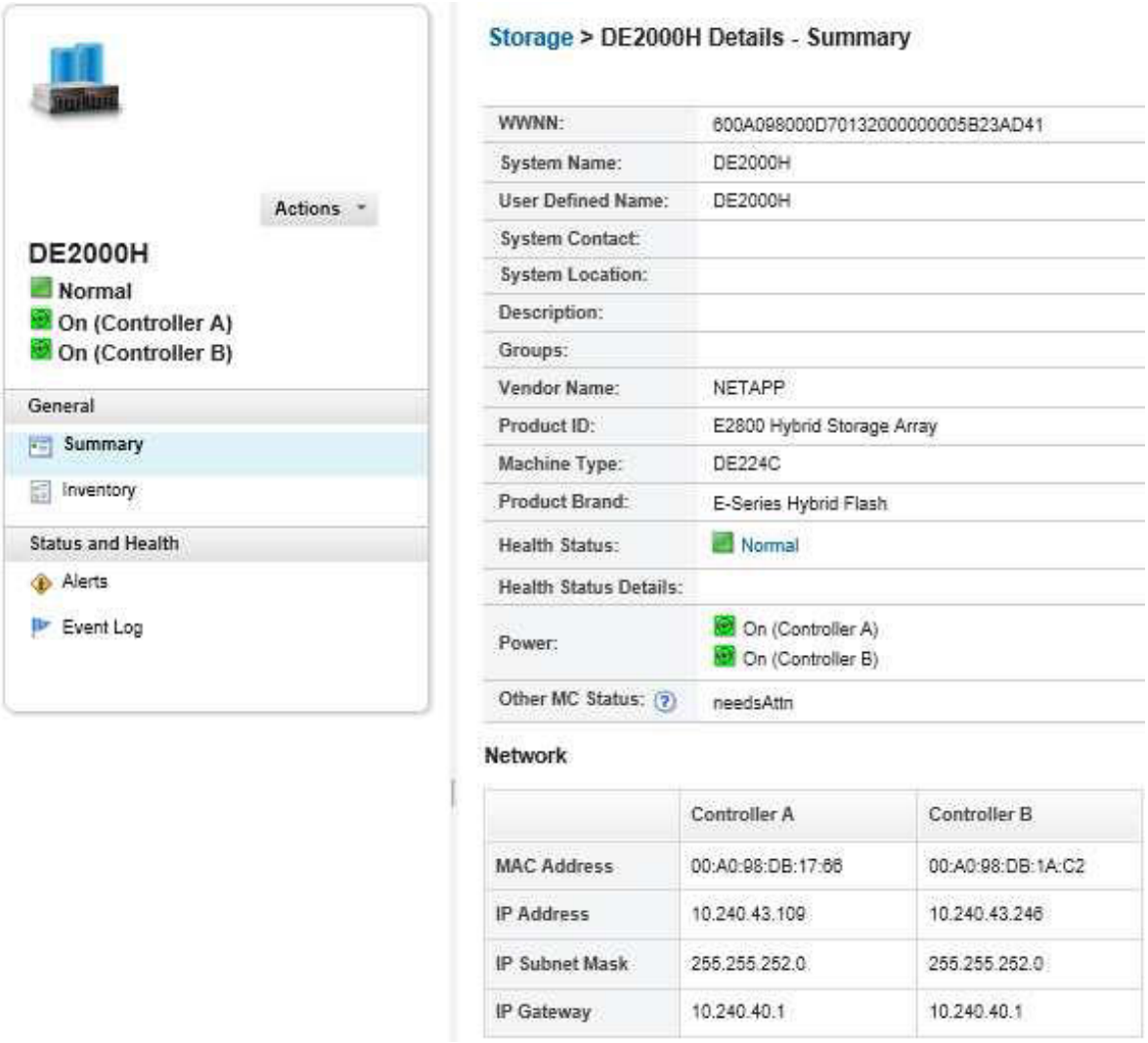
To view the details of a specific managed storage device, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all storage devices that are installed in managed chassis.

You can sort the table columns to make it easier to find specific storage devices. In addition, enter text (such as a system name or IP address) in the **Filter** field to further filter the storage devices that are displayed.



Step 2. Click the storage device name in the **Storage** column. The Summary page is displayed, showing the properties and a list of components that are installed in that storage device.



Step 3. Complete one or more of the following actions:

- Click **Summary** to view a summary of the server and its installed components, including system information and installed devices (see Viewing the status of storage devices).
- Click **Inventory Details** to view details about the storage device components, including:

  - Firmware levels for the storage device.
  - Details of the management-controller network, such as the hostname, IPv4 address, IPv6 address, and MAC addresses.
  - Asset details of the storage device.
  - Details about each canister in the storage device.

  Tip: If an expansion node, such as the Flex System Storage Expansion Node or the Flex System PCIe Expansion Node is installed in the chassis and connected to a storage device, inventory details for the expansion node is displayed as well.
- Click **Alerts** to display alerts in the alerts list that are related to the storage device (see Working with alerts).
- Click **Event Log** to display the events in the event log that are related to the storage devicestorage device (see Working with events).
- Click **Jobs** to display a list of jobs that are associated with the storage device (see Monitoring jobs).
- Click **Light Path** to display the current state of each LED on the storage device.
- Click **Power and Thermal** to display the power and thermal characteristics for the storage device.

  Tip: Use the refresh button on your web browser to collect the latest power and thermal data. Collecting data might take several minutes.

What to do next

In addition to displaying summary and detailed information about a storage device, you can perform the following actions:

- View a storage device in graphical rack or chassis view by clicking **Actions → Views → Show in Rack View** or **Actions → Views → Show in Chassis View**.
- Export detailed information about the storage device to a CSV file clicking the **Actions → Inventory → Export Inventory**.

  Notes:

  - For more information about inventory data in the CSV file, see the GET /storage/<*UUID_list*> REST API in the Lenovo XClarity Administrator online documentation.
  - When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Launch the management controller web interface for the storage device by clicking the **IP address** link (see Launching the management controller interface for a storage device).
- Power a storage controller in the storage device on and off (see Powering on and off a storage device).
- Virtually reseat the storage controller in the storage device (see Virtually reseating a server in a Flex System chassis).
- Modify system information by selecting a storage device and clicking **Edit Properties**.
- Refresh inventory by selecting a storage device and clicking **Actions → Inventory → Refresh Inventory**.
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Actions → Service Reset → Exclude Events** (see Excluding events).
- Resolve issues that might arise between the Lenovo XClarity Administrator security certificate and the security certificate of the CMM in the chassis where the storage device is installed by selecting a storage device and clicking **Actions → Service → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).

Backing up and restoring storage-configuration data

Lenovo XClarity Administrator does not include built-in backup functions for storage-configuration data. Instead, use the backup functions that are available for your managed storage device.

See the product documentation that is provided with your storage device for information about recovering the device.

- For Flex System storage devices, see Flex System Storage product documentation.
- For Lenovo Storage devices, see the Lenovo Storage S2200/S3200 product documentation.
- For Lenovo ThinkSystem storage devices, see the ThinkSystem Storage product documentation.
- For Nimble Storage devices, see Nimble Storage InfoSight website.

Powering on and off a storage device

You can power on and off a storage device from Lenovo XClarity Administrator.

About this task

For Flex System storage devices, when a storage controller is powered off, data is first stored on the internal drive and the storage device enters a standby state. In standby state, volumes that are provided by the storage device are no longer accessible.

To power on a ThinkSystem DM Series storage device, ensure that storage controller that is used for management is online and that its IP address is able to communicate directly to the service processor of the powered-off storage controller over the external network.

Procedure

Complete the following steps to power on and off a managed storage device.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all storage devices that are installed in managed chassis.

You can sort the table columns to make it easier to find specific storage device. In addition, enter text (such as a system name or IP address) in the **Filter** field to further filter the storage devices that are displayed.



Step 2. Select the storage device to be powered on or off.

Step 3. Click **All Actions**, and then click one of the following power actions:

- **Power On Controller A**
- **Power On Controller B**
- **Power off Controller A**

- **Power off Controller B**
- **Restart Controller A**
- **Restart Controller B**

Virtually reseating storage controllers in a Flex System storage device

You can perform a virtual reseat, which simulates the removal and reinsertion of a storage controller (canister) in the storage device bay

About this task

During the virtual reseat, all existing network connections to the storage device are lost, and the power state of the storage device changes. Before performing a virtual reseat, ensure that you have saved all user data.

Procedure

Complete the following steps virtually reseat a storage controller.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all storage devices.

You can sort the table columns to make it easier to find specific storage devices. In addition, enter text (such as a system name or IP address) in the **Filter** field to further filter the storage devices that are displayed.



Step 2. Select the Flex System storage device.

Step 3. Click **All Actions → Service**, and then click **Virtual Reseat Controller A** or **Virtual Reseat Controller B**.

Step 4. Click **Virtual Reseat**.

Launching the management controller interface for a storage device

You can launch the management controller web interface for the chassis in which the storage device is installed from Lenovo XClarity Administrator.

Procedure

To launch a management controller web interface, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all managed storage devices.

You can sort the table columns to make it easier to find specific storage devices. In addition, enter text (such as a device name or IP address) in the **Filter** field to further filter the storage devices that are displayed.



Step 2. Select the storage device.

Step 3. Click **Actions → Launch → Management Web Interface**. The management controller web interface is started.

Step 4. Log in to the management controller interface.

Note: For Flex System storage devices, use the XClarity Administrator user credentials.

Modifying the system properties for a storage device

You can modify the system properties for a specific storage device.

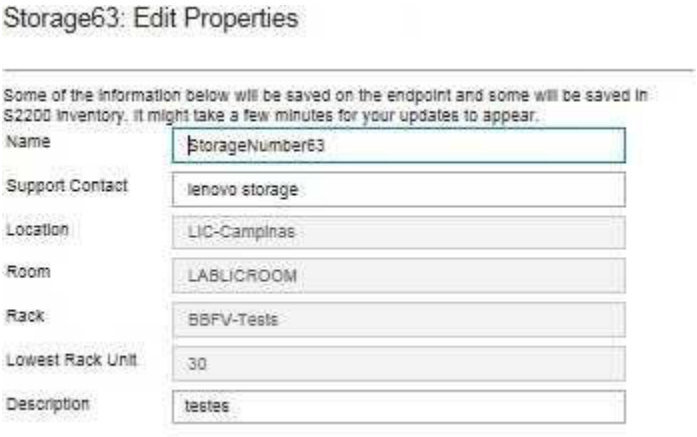
Procedure

To modify the system properties, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Storage** to display the Storage page.

Step 2. Select the storage device to be updated.

Step 3. Click **All Actions → Inventory → Edit Properties** to display the Edit dialog.



Step 4. Change the following information, as needed.

- Name
- Support contact

- Description

Note: XClarity Administrator updates the location, room, rack, and lowest rack unit properties when you add or remove devices from a rack in the web interface (see Managing racks).

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface.

Recovering management of a rack storage device after a management server failure

If a rack storage device was not unmanaged correctly, you must recover the storage device before you can remanage it. You can recover management by clearing specific parts of the storage-device configuration that was previously set by Lenovo XClarity Administrator.

Procedure

Complete one of the following steps to recovery a rack storage device.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the **Force management** option (see Managing storage devices).
- Remove all user accounts with the prefix “LXCA_” and optionally remove user accounts with the prefix “SYSMGR_” and type “SNMPv3” from the storage device.

What to do next

After XClarity Administrator is restored or replaced, you can manage the storage device again (see Managing storage devices). All information about the storage device (such as system properties) is retained.

Recovering management of a Lenovo ThinkSystem DE Series storage device after a management server failure

If a Lenovo ThinkSystem DE series storage device was not unmanaged correctly, you must recover the storage device before you can remanage it. You can recover management by clearing specific parts of the storage-device configuration that was previously set by Lenovo XClarity Administrator.

Procedure

Complete one of the following steps to recovery a Lenovo ThinkSystem DE Series storage device.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the **Force management** option (see Managing storage devices).
- Remove the “LXCA_REMOTE_MANAGMENT_VERIFICATION” key-pair register from the storage device key-pair API.

What to do next

After XClarity Administrator is restored or replaced, you can manage the storage device again (see Managing storage devices). All information about the storage device (such as system properties) is retained.

Unmanaging a Lenovo Storage or Nimble storage system

You can remove a Lenovo Storage or Nimble storage system from management by Lenovo XClarity Administrator. This process is called *unmanaging*.

Before you begin

Before you unmanage a Lenovo Storage or Nimble storage system, ensure that there are no active jobs running against the switch.

About this task

When you unmanaged a storage device, Lenovo XClarity Administrator retains certain information about the storage device. That information is reapplied when you manage the same storage device again.

Tip: All demo devices that are optionally added during initial setup are nodes in a chassis. To unmanage the demo devices, unmanage the chassis using the **Force unmanage even if the device is not reachable** option.

Procedure

To umanage a Lenovo Storage or Nimble storage system, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Storage** to display the Storage page.

Step 2. Select one or more Lenovo Storage or Nimble storage systems from the lists of managed switch.

Step 3. Click **Unmanage**. The Unmanage dialog is displayed.

Step 4. Optional: **Optional:** Select **Force unmanage even if the device is not reachable**.

Important: When unmanaging demo hardware, ensure that you select this option.

Step 5. Click **Unmanage**.The Unmanage dialog shows the progress of each step in the unmanagement process.

Step 6. When the unmanagement process is complete, click **OK**.

Recovering a rack storage device that was not unmanaged correctly

If Lenovo XClarity Administrator is managing a rack storage device, and if XClarity Administrator fails, you can recover the management functions until the management server is restored or replaced. You can recover system management by clearing specific parts of the storage-device configuration that was previously set by XClarity Administrator.

Procedure

Complete one of the following steps to recovery a rack storage device.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the **Force management** option (see Managing storage devices).
- Remove all user accounts with the prefix “LXCA_” and optionally remove user accounts with the prefix “SYSMGR_” and type “SNMPv3” from the storage device.

What to do next

After XClarity Administrator is restored or replaced, you can manage the storage device again (see Managing storage devices). All information about the storage device (such as system properties) is retained.

Chapter 10. Managing switches

Lenovo XClarity Administrator can manage network switches.

Learn more:

- XClarity Administrator: Discovery
- XClarity Administrator: Managing switches

Before you begin

Attention: Review the switch management considerations before managing a switch. For information, see Switch management considerations.

Note: Flex switches are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed Flex switches independent of a chassis.

Certain ports must be available to communicate with the switches. Ensure that all required ports are available before you attempt to manage a switch. For information about ports, see Port availability in the XClarity Administrator online documentation.

Ensure that the minimum required firmware is installed on each switch that you want to manage using XClarity Administrator. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.

Ensure that you create stored credentials in XClarity Administrator before you manage rack switches. XClarity Administrator uses only stored credentials to authenticate to the rack switches. The stored credential must match an active user account on the device. You can create stored credentials from the management dialogs or from the Stored Credentials page. For more information, see Managing stored credentials.

Management using loopback interfaces is supported for all RackSwitch devices. Ensure that XClarity Administrator has connectivity to the loopback interface, either by adding a static route or advertising the address via a routing protocol. Note that routing cannot be performed between the management port and *any* data ports (including loopback).

About this task

XClarity Administrator can automatically discover RackSwitch switches in your environment by probing for manageable devices that are on the same IP subnet as XClarity Administrator. To discover switches that are in other subnets, specify an IP address or range of IP addresses, or import information from a spreadsheet.

Note: If you upgraded from XClarity Administrator v2.0 to v2.1, the upgrade process converted the manual credential to individual stored credentials for all managed rack switches. Manual credential are not supported for rack switches in XClarity Administrator v2.1 and later.

After the switches are managed by XClarity Administrator, XClarity Administrator polls each managed switch periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed switch and perform management tasks such as launching the management console, and powering on and off.

If the XClarity Administrator looses communication with the switch (for example, due to power loss or network failure or if the switch is offline) while collecting inventory during the management process, the

© Copyright Lenovo 2015, 2021

management completes successfully; however, some inventory information might be incomplete. Either wait for the switch to come online and for XClarity Administrator to poll the switch for inventory or manually collect inventory on the switch from the Switches page by selecting the switch and clicking **All Actions → Inventory → Refresh inventory**.

Note: Switches can be stacked. A *stacked switch* is a group of switches that operate as a single network switch. The stack includes a *master switch* and one or more *member switches*. For Flex switches, you can view and monitor each switch in the stack and collect diagnostic data; however, you cannot perform management tasks (such as firmware updates and server configuration) on any stacked switch. These XClarity Administrator management tasks are disabled for all stacked switches, including the master switch. You can update firmware on the stacked switch directly from master switch CLI. For RackSwitch switches you can view and monitor only the master switch information. The member switches are not discovered by XClarity Administrator.

Management tasks are also disabled for Flex switches that are in protected mode.

A device can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device on the initial XClarity Administrator, and then manage it with the new XClarity Administrator. If an error occurs during the unmanagement process, you can select the **Force management** option during management on the new XClarity Administrator.

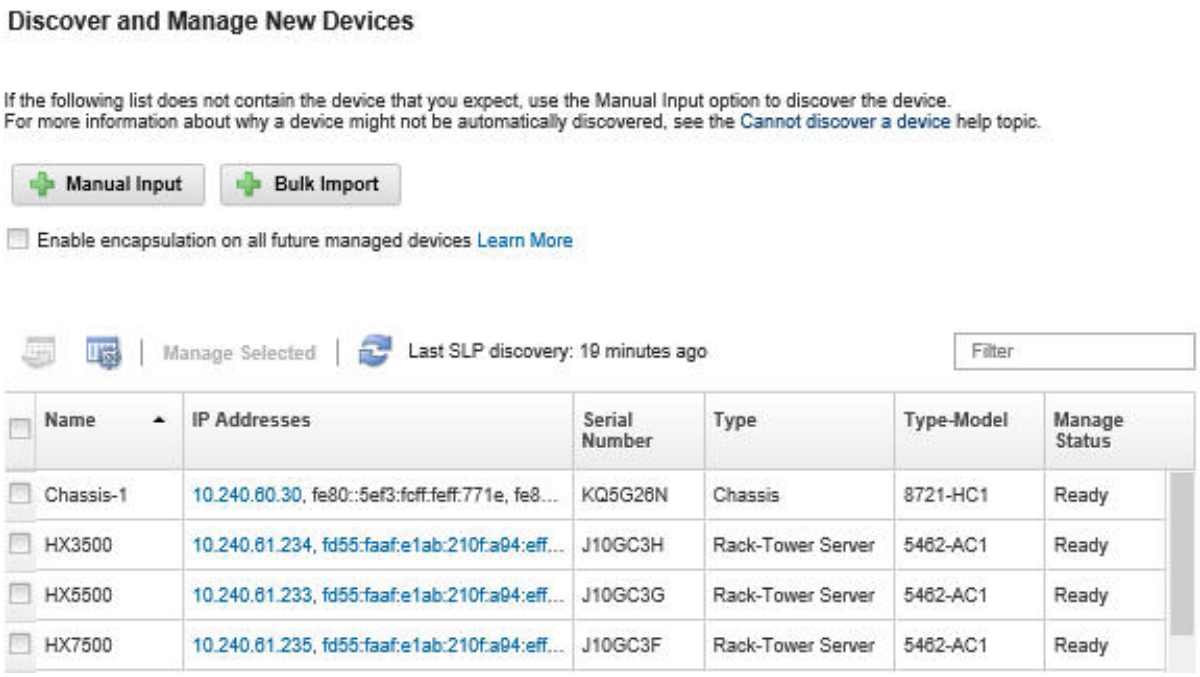
Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a device is already managed by another manager until after it attempts to manage the device.

When a switch is managed either directly using SSH or indirectly through a CMM, the switch is identified as managed by XClarity Administrator, necessary configuration is performed for interaction, and inventory is collected.

Procedure

Complete one of the following procedures to manage your RackSwitch switches using XClarity Administrator.

- Discover and manage a large number of switches and other devices using a bulk-import file (see Managing systems in the Lenovo XClarity Administrator online documentation).
- Discover and manage RackSwitch switches that are on the same IP subnet as XClarity Administrator.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage New Devices page is displayed.



You can sort the table columns to make it easier to find the switches that you want to manage. In addition, you can enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed. You can change the columns that are displayed and the default sort order by clicking the **Customize Columns** icon ( ).

2. Click the **Refresh** icon ( ) to discover all manageable devices in the XClarity Administrator domain. Discovery might take several minutes.
3. Select one or more switches that you want to manage.
4. Click **Manage Selected**.
5. Specify the stored credentials for authenticating to the switches.

   Tip:

   – Click **Manage Stored Credentials** to create and managed stored credentials in XClarity Administrator (see Managing stored credentials).
   – It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).
6. (Switches running ENOS only) If set, specify the “enable” password that is used to enter Privileged Exec Mode on the switch.

   When you manage a RackSwitch switch running ENOS, access to Privileged Exec Mode on the switch is required. This is used by XClarity Administrator when issuing the “enable” command to the switch. By default, there is no password set for this command on the switch. However, if the switch administrator configured a password for this command for added security, it must be specified for XClarity Administrator to manage the switch successfully.
7. Optional: (Switches running ENOS only) Choose whether to enable HTTPS on the switch by clicking **Advanced** and then selecting **Enable HTTPS**. This is enabled by default.

   Notes:

- For switches running CNOS, HTTPS must be enabled on the switch before management (see Switch management considerations).
- If you choose not to enable HTTPS, the current setting on the switch is used.
- When the switch is ununmanaged, XClarity Administrator restores HTTPS to the original setting.

8. Optional: Choose whether to replace the NTP configuration on the switch with the NTP configuration and time zone settings that are defined for Lenovo XClarity Administrator by clicking **Advanced** and then selecting **Configure NTP clients to use the NTP settings from the management server**. This is enabled by default.

   Notes:

   - If you choose *not* to replace the NTP configuration and time zone, the timestamp for log entries and events might become out of synch between the managed switch and the management server.
   - When the switch is ununmanaged, XClarity Administrator restores NTP configuration and time zone to the original settings.

9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   - You can select from a list of role groups that are assigned to the current user.
   - If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the job progress.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    - If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    - If the managing XClarity Administrator was taken down before the devices were unmanaged.
    - If the devices were not unmanaged successfully.

    Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

- Discover and manage RackSwitch switches that are not on the same IP subnet as XClarity Administrator by manually specifying IP addresses:

  1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Select **Manual Input**.
  3. Specify the network addresses of the switches that you want to manage:

- Click **Single System**, and enter a single IP address domain name, or fully-qualified domain name (FQDN).

  Note: To specify an FQDN, ensure that a valid domain name is specified on Network Access page (see Configuring network access).
- Click **Multiple Systems**, and enter a range of IP addresses. To add another range, click the **Add** icon (). To remove a range, click the **Remove** icon ().

4. Click **OK**.
5. Specify the stored credentials for authenticating to the switches.

   Tip:
   - Click **Manage Stored Credentials** to create and managed stored credentials in XClarity Administrator (see Managing stored credentials).
   - It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).
6. (Switches running ENOS only) If set, specify the “enable” password that is used to enter Privileged Exec Mode on the switch.

   When you manage a RackSwitch switch running ENOS, access to Privileged Exec Mode on the switch is required. This is used by XClarity Administrator when issuing the “enable” command to the switch. By default, there is no password set for this command on the switch. However, if the switch administrator configured a password for this command for added security, it must be specified for XClarity Administrator to manage the switch successfully.
7. Optional: (Switches running ENOS only) Choose whether to enable HTTPS on the switch by clicking **Advanced** and then selecting **Enable HTTPS**. This is enabled by default.

   Notes:
   - For switches running CNOS, HTTPS must be enabled on the switch before management (see Switch management considerations).
   - If you choose not to enable HTTPS, the current setting on the switch is used.
   - When the switch is ununmanaged, XClarity Administrator restores HTTPS to the original setting.
8. Optional: Choose whether to replace the NTP configuration on the switch with the NTP configuration and time zone settings that are defined for Lenovo XClarity Administrator by clicking **Advanced** and then selecting **Configure NTP clients to use the NTP settings from the management server**. This is enabled by default.

   Notes:
   - If you choose *not* to replace the NTP configuration and time zone, the timestamp for log entries and events might become out of synch between the managed switch and the management server.
   - When the switch is ununmanaged, XClarity Administrator restores NTP configuration and time zone to the original settings.
9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:
   - You can select from a list of role groups that are assigned to the current user.
   - If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the job progress.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    – If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    – If the managing XClarity Administrator was taken down before the devices were unmanaged.

    – If the devices were not unmanaged successfully.

    Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

What to do next

- Discover and manage additional devices.
- Add the newly managed devices to the appropriate rack to reflect the physical environment (see Managing racks).
- Monitor hardware status and details (see Viewing the status of switches).
- Monitor events (see Working with events).

Switch management considerations

Before managing a switch, review the following important considerations.

For information about port requirements, see Port availability in the Lenovo XClarity Administrator online documentation.

RackSwitch devices can be managed using either a management port or one of the data ports. Rackswitch devices running CNOS can be managed only on interfaces that belong to either “management” or “default” VRF.

Note: Managing RackSwitch devices using IPv6 link local through a data port or management port is not supported.

XClarity events and SNMP trap configuration

When a RackSwitch device running ENOS (any version) is managed, the SNMP trap source is set to the interface that has the IP address that is used for management.

When a RackSwitch device running CNOS v10.8.1 or later is managed, the SNMP trap source VRF is checked and changed to match the port that is used for management.

For RackSwitch devices running CNOS earlier than v10.8.1, XClarity Administrator requires the SNMP trap source to be the VRF that is connected to the port that is used for management. The default value “all” allows either management or data ports to be used. If the switch configuration does not use the default value, it must be changed to match the port that is used for management.

- If the management port is used for management, set the SNMP trap source VRF to “all” or “management.”
- If one of the data ports is used for management, set the SNMP trap source VRF to “all” or “default.”

RackSwitch switches running CNOS

HTTPS must be enabled for management, and SLP must be enabled for discovery.

Note: HTTPS is enabled by default on CNOS. If you changed the default configuration of restApi (using the **feature restApi http** command), you can change it back to HTTPS using the **feature restApi** command. To check the current status, use the **display restApi server** command. The output reflects the current status. If the port number is followed by “(HTTP)”, it means HTTPS is *disabled*. Otherwise, the port should be 443.

When a RackSwitch device is unmanaged, XClarity Administrator might not restore the “prefer” option to the value that it was before the device was managed depending on the CNOS firmware version.

RackSwitch switches running ENOS

- If RackSwitch switches are on a different network than XClarity Administrator, the network must be configured to allow inbound UDP through ports 161 and 162 so that XClarity Administrator can receive events and manage those devices.
- SSH must be enabled for management, and SLP must be enabled for discovery. HTTPS is optional; however, must be enabled to launch the switch web interface
- Depending on the firmware version of the RackSwitch switch, you might need to enable multicast SLP forwarding and SSH on each RackSwitch switch manually using the following commands before the switch can be discovered and managed by XClarity Administrator. For more information, see the Rack switches in the System x online documentation.
  - `ip slp enable`
  - `ssh enable`
- When a RackSwitch switch is managed, XClarity Administrator modifies the following configuration settings. Changing these settings on a managed switch might disrupt connectivity and prevent management actions from performing correctly. When a RackSwitch switch is unmanaged, the configuration settings are restored to their original values (before management).
  - snmp-server access 32
  - snmp-server group 16
  - snmp-server notify 16
  - snmp-server target-parameters 16
  - snmp-server target-address 16
  - snmp-server trap-source <*IP interface*>
  - snmp-server user 16
  - snmp-server vesrion <*v3only or v1v2v3*>
  - ntp enable
  - ntp primary-server <*hostname or IP address*> MGT
  - ntp secondary-server <*hostname or IP address*> MGT
  - ntp interval 1500
  - ntp offset 500
  - access https enable

  You can use XClarity Administrator to modify the following configuration settings by modifying the support contact information, name, or location properties for the switch. The location is modified when adding the switch to a rack.

- hostname "<*device_name*>"
- snmp-server location "Location:<*location*>,Room:<*room*>,Rack:<*rack*>,LRU:<*lru*>"
- snmp-server contact "<*contact_name*>"

Viewing the status of switches

You can view the status of all switches that Lenovo XClarity Administrator manages.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

The following status icons are used to indicate the overall health of the device. If the certificates do not match, "(Untrusted)" is appended to the status of each applicable device, for example Warning (Untrusted). If there is a connectivity issue or a connection to the device is not trusted, "(Connectivity)" is appended to the status of each applicable device, for example Warning (Connectivity).

- ( ) Critical
  - One or more temperature sensors are in the failure range.
  - Fan modules or fans are not working correctly, as follows:
    - RackSwitch G8124-E: One or more fans are running at less than or equal to 100 RPM.
    - RackSwitch G8052: Fewer than three fan modules are in good state. If the fans in that module are running at more than 500 RPM, a fan module is considered good.
    - RackSwitch G8264, G8264CS, G8332, G8272: Fewer than four fan modules are in good state. If the fans in that module are running at more than 500 RPM, a fan module is considered good.
    - RackSwitch G8296: Fewer than three fan mare in good state. If the fans in that module are running at more than 480 RPM, a fan module is considered good.
    - RackSwitch G7028, G7052: Fewer than three fan modules are in good state. If the fans in that module are running at more than 500 RPM, a fan module is considered good.
  - One power supply is off.
- ( ) Warning
  - One or more temperature sensors are in the warning range.
  - A panic dump exists in flash.
- ( ) Pending
- ( ) Informational
- ( ) Normal
  - All temperature sensors are in the normal range.
  - All fan modules or fans are working correctly.
  - Both power supplies are on.
  - No panic dump in flash.
- ( ) Offline
- ( ) Unknown

A device can be in one of the following power states:

- On
- Off
- Shutting down
- Standby
- Hibernate
- Unknown

Procedure

To view the status for a managed switch, complete one or more of the following actions.

- From the XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of the all managed switches and other resources.



- From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all managed switches.

  You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field and click the status icons to list only those switches that meet the selected criteria.



  From this page, you can perform the following actions:

- View detailed information about the switch (see Viewing the details of a switch).
- View a Flex switch in graphical rack or chassis view by clicking **All Actions → Views → Show in Rack View** or **All Actions → Views → Show in Chassis View**.
- View a RackSwitch switch in graphical rack view by clicking **All Actions → Views → Show in Rack View**.
- Launch the management controller web interface for the switch by clicking the **IP address** link (see Launching the management controller interface for a switch).
- Launch the switch SSH console (see Launching a remote SSH session for a switch).
- Power the switch on and off (see Powering on and off a switch).
- (RackSwitch switches only) Modify system information by selecting a switch and clicking **All Actions → Inventory → Edit Properties**.
- Refresh inventory by selecting a server and clicking **All Actions → Inventory → Refresh Inventory**.
- Export detailed information about one or more switches to a single CSV file by selecting the switches and clicking **All Actions → Inventory → Export Inventory** (see Excluding events).

  Note: You can export inventory data for a maximum of 60 devices at one time.

  Tip: When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Exclude events** icon ( ) (see Excluding events).
- (Flex switches only) Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the CMM in the chassis where the switch is installed by selecting a switch and clicking **All Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).
- Add or remove a switch from a static resource group by clicking **All Actions → Groups → Add to Group** or **All Actions → Groups → Remove from Group**.

Viewing the details of a switch

You can view detailed information about a managed switch from Lenovo XClarity Administrator, including the firmware levels and IP addresses.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

Procedure

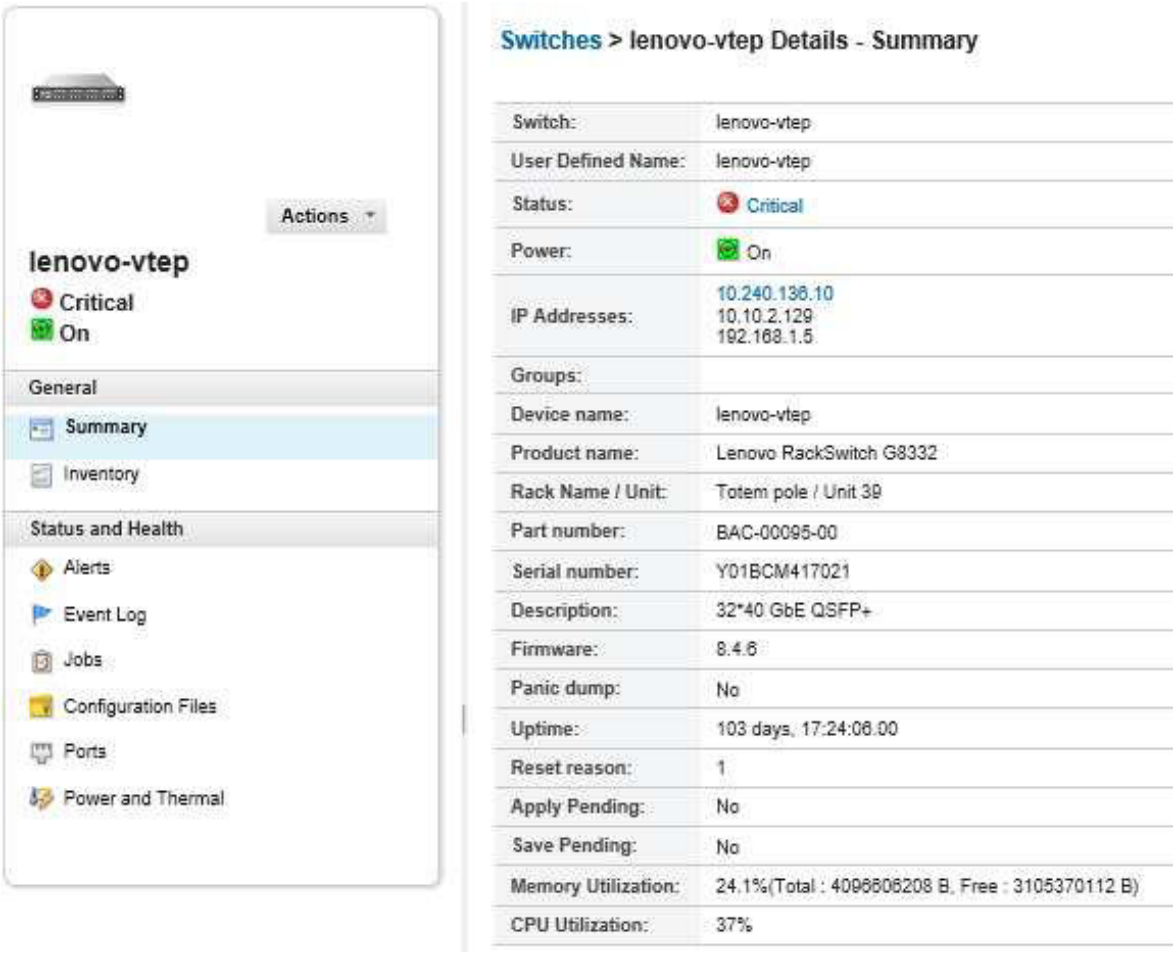
To view the details of a specific switch that is managed by XClarity Administrator, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.



Step 2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.



Step 3. Complete one or more of the following steps to view detailed inventory information:

Note: Some details might not be available for all switches.

- Click **Summary** to view a summary of the switch, including system information and firmware (see Viewing the status of storage devices).
- Click **Inventory Details** to view details about the switch components, including:
  - Firmware levels for the switch

  - Details of the management-controller network, such as the hostname, IPv4 address, IPv6 address, and MAC addresses
  - Asset details of the switch
- Click **I/O Connectivity** to display connectivity details for the selected switch and the associated network adapters that are installed in switch.
- Click **Alerts** to display alerts in the alerts list that are related to the switch (see Working with alerts).
- Click **Event Log** to display the events in the event log that are related to the switch (see Working with events).
- Click **Configuration Files** to backup and restore the switch configuration (see Backing up and restoring switch-configuration data).
- Click **Deployment History** to view information about switch-configuration templates that have been deployed to switch (see Viewing switch-configuration deployment history).
- Click **Jobs** to display configuration-data files for the switch (see Monitoring jobs).
- Click **Ports** to display the status and configuration of all ports in a managed switch , and to enable or disable switch ports.

  Note: For Flex switches, click the **Refresh** icon () to collect the current port data. Collecting data might take several minutes.
- Click **Light Path** to display the current state of each LED on the switch.
- Click **Power and Thermal** to display information about temperature, power supplies, and fans.

  Tip: To collect the latest power and thermal data, Use the refresh button on your web browser. Collecting data might take several minutes.

What to do next

In addition to displaying summary and detailed information about a switch, you can perform the following actions:

- View a Flex switch in graphical rack or chassis view by clicking **Actions → Views → Show in Rack View** or **Actions → Views → Show in Chassis View**.
- View a RackSwitch switch in graphical rack view by clicking **Actions → Views → Show in Rack View**.
- Launch the management controller web interface for the switch by clicking the **IP address** link (see Launching the management controller interface for a switch).
- Launch the switch SSH console (see Launching a remote SSH session for a switch).
- Power the switch on and off (see Powering on and off a switch).
- (RackSwitches only) Modify system information by selecting a switch and clicking **Edit Properties**.
- Export detailed information about the switch to a CSV file by clicking the **Actions → Inventory → Export Inventory**.

  Notes:

  - For more information about inventory data in the CSV file, see the GET /switches/<*UUID_list*> REST API in the XClarity Administrator online documentation.
  - When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking **Actions → Service Reset → Excluded Events** (see Excluding events).

- Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the RackSwtich or the CMM in the chassis where the Flex System switch is installed by selecting a switch and clicking **Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).

Powering on and off a switch

You can power on and off and restart a Flex System or RackSwitch switch from Lenovo XClarity Administrator.

Procedure

Complete the following steps to power on or off a managed switch.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.



Step 2. Select the switch to be powered on or off or restarted.

Step 3. Click **All Actions**, and then click one of the following power actions:
- **Power on** (Flex System switches only)
- **Power Off** (Flex System switches only)
- **Restart**. The switch is restarted after all currently running operations are complete. Operations that are started while the switch is restarting are rejected.

Enabling and disabling switch ports

You can enable or disable specific ports on a RackSwitch or Flex System switch

Procedure

To enable or disable switch ports, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

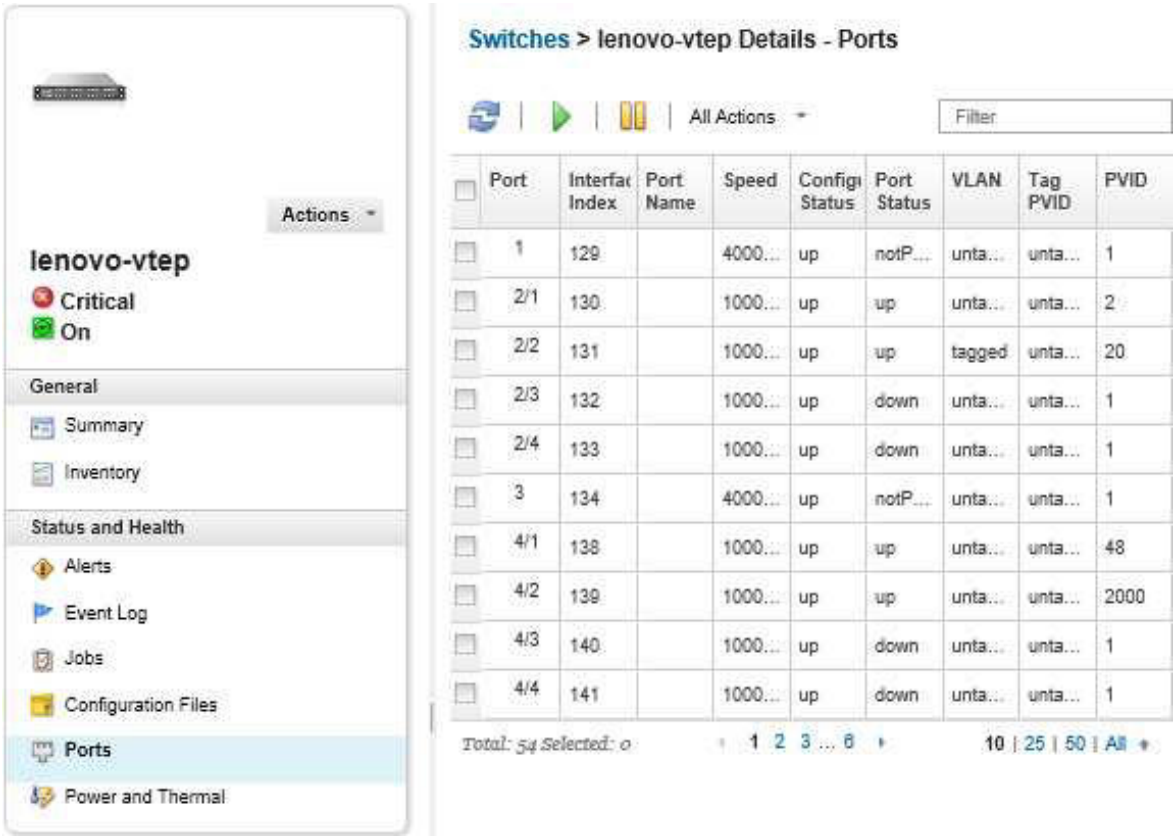
You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.



Step 2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.

Step 3. Click **Ports** in the left navigation to display the status and configuration of all ports in the switch:

Note: For Flex switches, click the **Refresh** icon ( ) to collect the current port data. Collecting data might take several minutes



Step 4. Select the port, and then click the **Enable** icon ( ) or **Disable** icon ( ).

Backing up and restoring switch-configuration data

You can use Lenovo XClarity Administrator to back up and restore configuration data for your RackSwitch and Flex System switches. You can also export switch-configuration files to your local system and import switch-configuration files into XClarity Administrator.

Backing up switch-configuration data

You can back up configuration data for a Flex System or RackSwitch switch. When backing up a switch, the configuration data is imported into Lenovo XClarity Administrator from the target switch as a switch-configuration file.

Procedure

To back up configuration data for a managed switch, complete the following steps.

- For a single switch:
  1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

     You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

  2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.
  3. Click **Configuration** to view the configuration files for the switch.
  4. Click **Back up configuration data** icon ( ) to back up the switch configuration.
  5. (Optional) Specify a name for the switch-configuration file.

     For CNOS devices, the file name can contain alphanumeric characters and the following special characters: underscore (_), hyphen (-) and period (.). For ENOS switches, the file name can contain alphanumeric characters and any special characters.

     If a file name is not specified, the following default name is used: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."
  6. (Optional) Add a comment that describes the backup.
  7. Click **Back up** to back up with switch-configuration data immediately or click **Schedule** to schedule this backup to run at a later time.

     If you chose to schedule a backup, you can select **Overwrite** to back up the switch-configuration data into the same file at each job run, overwriting its contents. If you choose not to overwrite file, the file names of subsequent backups are appended with a unique number (for example, MyBackup_33.cfg).

     Note: When scheduling a backup, you cannot choose dynamic file names or comments for each scheduled job.
- For multiple switches:

1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.
2. Select one or more switches.
3. Click **All Actions → Configuration → Backup configuration file**.
4. (Optional) Specify a name for the switch-configuration file.

   For CNOS devices, the file name can contain alphanumeric characters and the following special characters: underscore (_), hyphen (-) and period (.). For ENOS switches, the file name can contain alphanumeric characters and any special characters.

   If a file name is not specified, the following default name is used: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."
5. (Optional) Add a comment that describes the backup.
6. Click **Back up** to back up with switch-configuration data immediately or click **Schedule** to schedule this backup to run at a later time.

   If you chose to schedule a backup, you can select **Overwrite** to back up the switch-configuration data into the same file at each job run, overwriting its contents. If you choose not to overwrite file, the file names of subsequent backups are appended with a unique number (for example, MyBackup_33.cfg).

   Note: When scheduling a backup, you cannot choose dynamic file names or comments for each scheduled job.

What to do next

When the backup process is complete, the switch-configuration file is added to the **Configuration Files** tab on the switch details page.

From this page, you can perform the following actions on selected switch-configuration file:

- Restore the switch configuration by selecting the switch-configuration file and clicking the **Restore configuration data** icon ( ).
- Delete switch configuration files from XClarity Administrator by clicking the **Delete** icon ( ).
- Export switch-configuration files to your local system by selecting the files and clicking the **Export configuration file** icon ( ).
- Import switch-configuration files to XClarity Administrator by clicking the **Import configuration file** icon ( ).

Restoring switch-configuration data

You can restore configuration data that has been backed up or imported into Lenovo XClarity Administrator for a Flex System or RackSwitch switch. The switch-configuration file is downloaded from XClarity Administrator to the target switch, and the configuration takes effect automatically.

Configuration files are associated with a specific switch. You can restore a configuration file only on the switch with which it is associated. You cannot use a configuration file that was backed up for one switch to restore the configuration on another switch.

Procedure

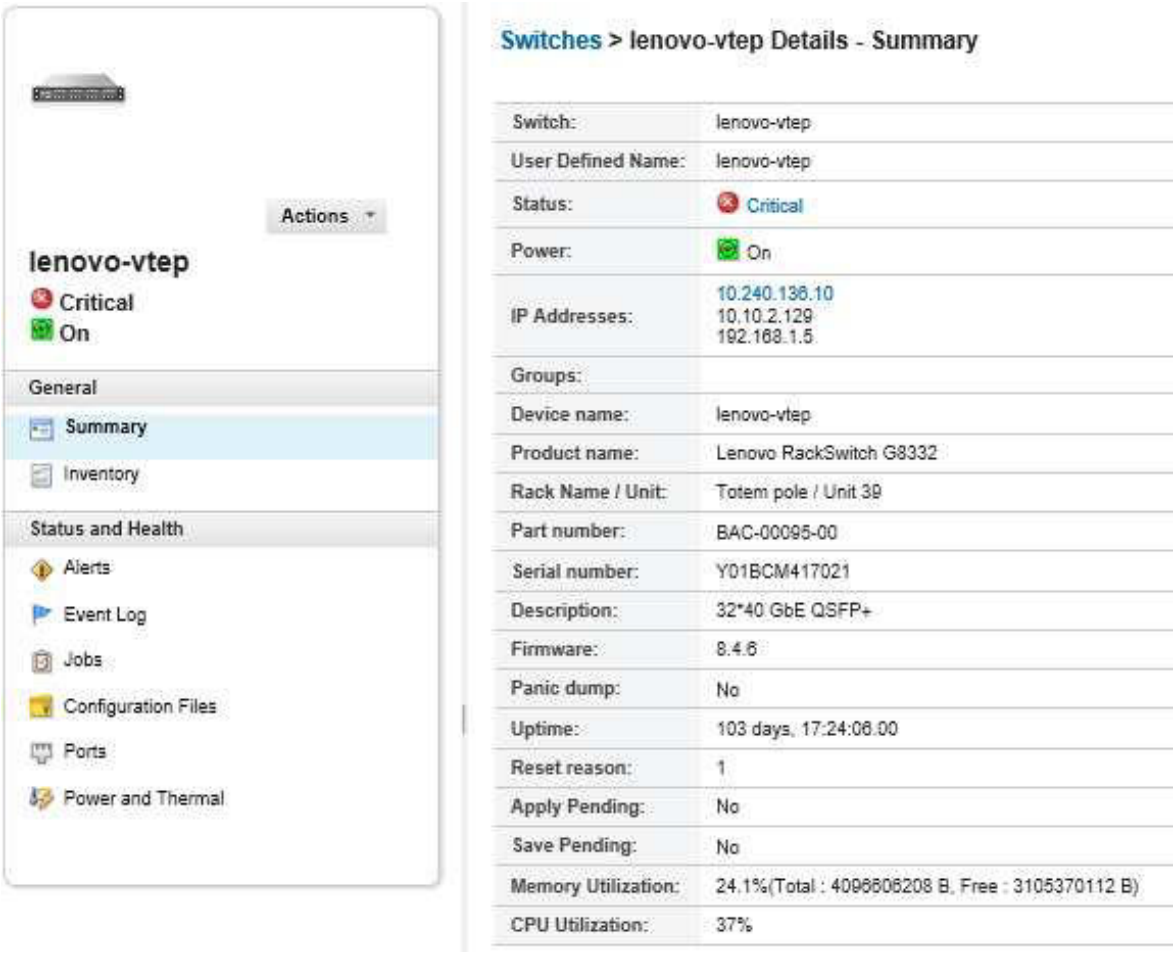
To restore configuration data on a managed switch, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.



Step 2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.



Step 3. Click **Configuration Files** to view the configuration files for the switch.

Step 4. Select the configuration file that you want to restore on the switch, and click **Restore configuration data** icon ( ). The Restore dialog is displayed.

Step 5. (Switches running CNOS only) Choose whether to restart the switch after the restore operation completes.

If you choose not to restart the switch automatically, you must manually restart the CNOS switch to activate the restored configuration data. If you wait too long and a save operation occurs (for example, if a port is enabled or disabled), the restore operation is aborted and the running configuration data is used.

Step 6. Click **Restore** to restore with configuration data on the switch immediately, or click **Schedule** to schedule this restore job to run at a later time.

Note: Take care when scheduling a recurring restore jobs. If your switch resets to an earlier configuration, check the Scheduled Jobs page for scheduled restore jobs.

Exporting and importing switch-configuration files

You can export switch-configuration files to your local system and import switch-configuration files into Lenovo XClarity Administrator.

Procedure

To back up configuration data for a managed switch, complete the following steps.

- Export switch-configuration files
  1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

     You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.



  2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.
  3. Click **Configuration** to view the configuration files for the switch.
  4. Select the switch-configuration files to export.
  5. Click **Export configuration file** icon ( ) to back up the switch configuration.
- Import switch-configuration files
  1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.



2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.
3. Click **Configuration** to view the configuration files for the switch.
4. Click **Import configuration file** icon ( ) to back up the switch configuration.
5. Enter the switch-configuration file name or click **Browse** to find the boot file that you want to import.
6. **Optional:** Enter a description for the switch-configuration file.
7. Click **Import**.

   If you close the web browser tab or window in which the file is being uploaded before the upload completes, the import fails.

Launching the management controller interface for a switch

You can launch the management controller web interface for a RackSwitch or Flex System switch running ENOS from Lenovo XClarity Administrator.

Procedure

Complete the following steps to launch the management controller interface for a switch.

Note: Launching any management controller web interface from XClarity Administrator using the Safari web browser is not supported.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.



Step 2. Select the switch, and click **All Actions → Launch → Management Web Interface**. The management controller web interface for the switch is displayed.

Tip: You can also launch the management controller interface by clicking the IP address link in the **IP Address** column, and on the switch summary and switch details pages.

Step 3. Log in to the management controller interface.

Tip: For Flex switches, use your XClarity Administrator user credentials. For XClarity Administrator switches, use the switch credentials.

Launching a remote SSH session for a switch

You can launch a remote SSH session for a managed RackSwitch or Flex switch from Lenovo XClarity Administrator. From the remote SSH session, you can use the command-line interface to perform management tasks that are not provided by XClarity Administrator.

Before you begin

Ensure that the switch is configured to enable SSH. For RackSwitch switches, SSH is enabled when the switch is managed by XClarity Administrator. For Flex switches, SSH is typically enabled by default. If not enabled, SSH must be enabled before the switch is managed by XClarity Administrator.

Procedure

Complete the following steps to launch a remote SSH session for a managed switch.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.



Step 2. Select the switch to launch an SSH session.

Step 3. Click **All Actions → Launch → SSH Console**.

Step 4. If required, log in to the switch using your user ID and password.

Modifying the system properties for a switch

You can modify the system properties for a specific Flex System or RackSwitch switch.

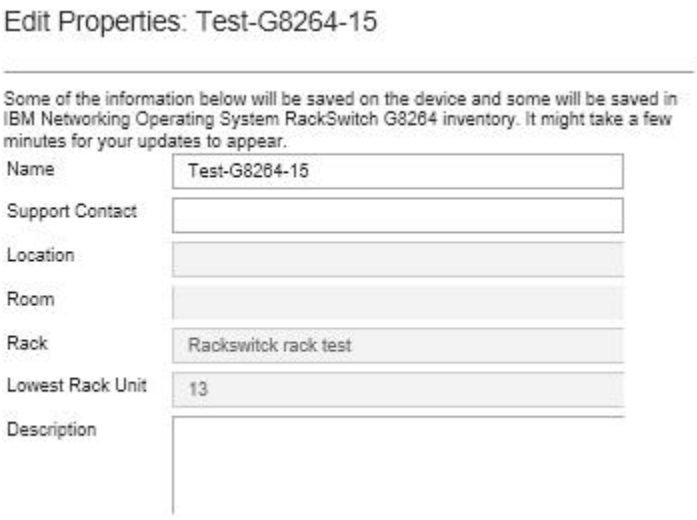
Procedure

Complete the following steps to modify the system properties.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Switches** to display the Switches page.

Step 2. Select the switch to be updated.

Step 3. Click **All Actions → Inventory → Edit Properties** to display the Edit dialog.



Step 4. Change the following information, as needed.

- Switch name
- Support contact
- Description

Note: The location, room, rack, and lowest rack unit properties are updated by XClarity Administrator when you add or remove devices from a rack in the web interface (see Managing racks).

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface.

Resolving expired or invalid stored credentials for a switch

When a stored credential becomes expired or inoperable on a device, the status for that device is shown as “Offline.”

Procedure

To resolve an expired or invalid stored credential for a switch, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all managed switches.

Step 2. Click the **Power** column header to group all offline switches at the top of the table.

You can sort the table columns to make it easier to find the switch that you want to manage. In addition, you can enter text (such as a system name or IP address) in the **Filter** field to further filter the switches that are displayed.



Step 3. Select the switch to be resolved.

Step 4. Click **All Actions → Security → Edit Stored Credentials**.

Step 5. Change the password for the stored credential or select another stored credential to use for the managed device.

Note: If you managed more than one device using the same stored credentials and you change the password for the stored credentials, that password change affects all devices that are currently using the stored credentials.

Recovering management with a RackSwitch switch after a management server failure

You can recover management of a RackSwitch switch that was not unmanaged cleanly (for example, due to connectivity issues during unmanagement or failure of the managing Lenovo XClarity Administrator).

Procedure

- Manage the switch again using the **Force management** option (see Managing switches).
- To permanently remove XClarity Administrator specific configuration on a RackSwitch switch that was not unmanaged cleanly and will not be managed again, complete these steps.

- Manage the switch again using the **Force management** option (see Managing switches), and then unmanage the switch to clean up the configuration (see Unmanaging a RackSwitch switch).
- (ENOS) Log in to the switch using the switch console port or an SSH or telnet session, and run the following configuration commands in the order specified to clear the switch configuration.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Unmanaging a RackSwitch switch

You can remove a RackSwitch switch from management by Lenovo XClarity Administrator. This process is called *unmanaging*.

Before you begin

You can enable XClarity Administrator to automatically unmanage devices (including Flex System chassis, Flex System and rack switches, Flex System servers, System x servers, ThinkAgile, and ThinkSystem servers) that are offline for a specific amount of time. This is disabled by default. To enable the automatic unmanagment of offline devices, click **Hardware → Discover and Manage New Devices** from the XClarity Administrator menu, and then click **Edit** next to **Unmanage offline devices is Disabled**. Then, select **Enable unmanage offline devices** and set the time interval. By default, devices are unmanaged after being offline for 24 hours.

Before you unmanage a RackSwitch switch, ensure that there are no active jobs running against the switch.

About this task

When you unmanaged a RackSwitch switch, XClarity Administrator retains certain information about the switch. That information is reapplied when you manage the same switch again.

Tip: All demo devices that are optionally added during initial setup are nodes in a chassis. To unmanage the demo devices, unmanage the chassis using the **Force unmanage even if the device is not reachable** option.

Procedure

To umanage a RackSwitch switch, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches** to display the Switches page.

Step 2. Select one or more RackSwitch switches from the lists of managed switch.

Step 3. Click **Unmanage Switch**. The Unmanage dialog is displayed.

Step 4. Optional: **Optional:** Select **Force unmanage even if the device is not reachable**.

Important: When unmanaging demo hardware, ensure that you select this option.

Step 5. Click **Unmanage**.The Unmanage dialog shows the progress of each step in the unmanagement process.

Step 6. When the unmanagement process is complete, click **OK**.

Recovering a RackSwitch switch that was not unmanaged correctly

If a RackSwitch switch is being managed by Lenovo XClarity Administrator, and if XClarity Administrator fails, you can recover the management functions until the management server is restored or replaced.

Procedure

- Manage the switch again using the **Force management** option (see Managing switches).
- To permanently remove XClarity Administrator specific configuration on a RackSwitch switch that was not unmanaged cleanly and will not be managed again, complete these steps.
  - Manage the switch again using the **Force management** option (see Managing switches), and then unmanage the switch to clean up the configuration (see Unmanaging a RackSwitch switch).
  - (ENOS) Log in to the switch using the switch console port or an SSH or telnet session, and run the following configuration commands in the order specified to clear the switch configuration.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Chapter 11. Configuring servers using configuration patterns

Server patterns are used to quickly provision or preprovision multiple servers (rack and tower servers and compute nodes) from a single set of defined configuration settings.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Configuration patterns

Before you begin

After the 90-day free trial expires, you can continue to use XClarity Administrator to manage and monitor your hardware for free; however, you must purchase full-function-enablement licenses for each managed server that supports XClarity Administrator advanced functions to continue using the server configuration function. Lenovo XClarity Pro provides entitlement to service and support and the full-function-enablement license. For more information about purchasing Lenovo XClarity Pro, contact your Lenovo representative or authorized business partner. For more information, see Installing the full-function enablement license in the XClarity Administrator online documentation.

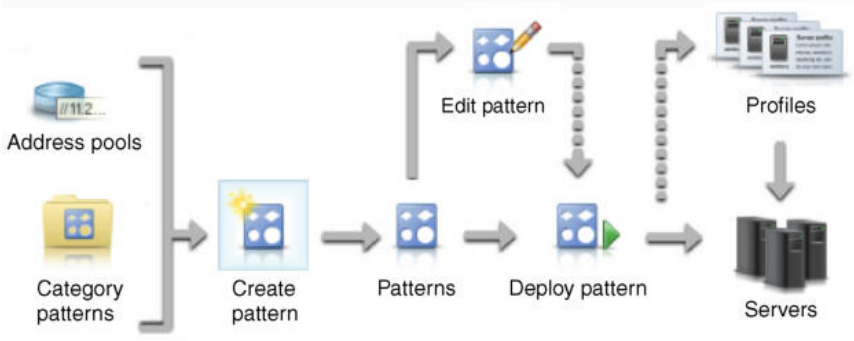
Review Configuration considerations for important information about configuration support for specific servers and devices.

About this task

You can use server patterns in XClarity Administrator to configure local storage, I/O adapters, boot order, and other baseboard management controller and Unified Extensible Firmware Interface (UEFI) settings on managed servers. Server patterns also integrate support for virtualizing I/O addresses, so you can virtualize server fabric connections or repurpose servers without disruption to the fabric. You can also initiate SAN-zoning change requests in advance of receiving new hardware by virtualizing (preconfiguring) Fibre Channel addresses.

Procedure

The following figure illustrates the workflow for configuring managed servers. The solid arrows indicate actions taken by you. The dashed arrows indicate actions that are performed automatically by XClarity Administrator.



Step 1. **Create address pools.**An *address pool* is a defined set of address ranges. Lenovo XClarity Administrator uses address pools to assign IP and I/O addresses to individual servers when the server patterns are deployed to those servers.

© Copyright Lenovo 2015, 2021

For more information about creating address pools, see Defining address pools.

Step 2. **Create category patterns.**

A *category pattern* groups together related firmware settings and can be reused in multiple server patterns. You can create patterns for the following firmware categories:

- System information
- Management interfaces
- Devices and I/O ports
- FC boot targets
- I/O adapter ports

For more information about category patterns, see Working with server patterns.

Step 3. **Create a server pattern.**

A *server pattern* represents pre-OS server configurations, including local storage configuration, I/O adapter configuration, boot settings, and other baseboard management controller and UEFI firmware settings. A server pattern is used as an overall pattern to quickly configure multiple servers at one time.

You can define multiple server patterns to represent different configurations that are used in your data center.

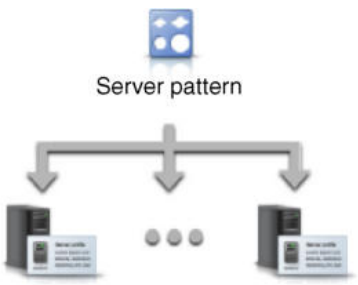
When defining a server pattern, select category patterns and address pools as needed to construct the desired configuration for a specific group of servers. A category pattern groups together related configuration settings that can be reused by multiple server patterns.

You can create a server pattern from scratch for Converged, Flex System, NeXtScale, and System x servers to define the desired configuration before the hardware arrives. Or, you can create a server pattern from an existing managed server. When you create a server pattern from an existing server, XClarity Administrator learns category patterns from the selected server.

For more information about creating server patterns, see Creating a server pattern.

Step 4. **Deploy the server pattern.**

You can deploy a server pattern to one or more individual servers or to groups of servers. For example, you can deploy a server pattern to a chassis so all the compute nodes in that chassis are configured the same. During deployment, XClarity Administrator creates a server profile for each server to which the server pattern was deployed. Each *server profile* represents the specific configuration for a single server. It inherits settings from the server pattern and also contains server-specific information (such as assigned IP addresses and MAC addresses). Because the server profile inherits settings from the server pattern, if you change the server pattern, changes are automatically updated in the server profile. This way, you can maintain common configurations in one place.



Note: The settings on a server can become out of compliance with its server profile if settings are changed without using Configuration Patterns or if an issue occurred during deployment, such a firmware issue or an invalid setting. You can determine the compliance status of each server from the Configuration Patterns: Server Profiles page.

You can deploy a server pattern to:

- **Existing servers**. A server profile is created for each server. The server profile is activated after the associated server is rebooted.
- **Empty bays in an existing chassis**. A server profile is created for each empty bay. The server profile that is associated with the empty bay can then be activated after the compute node is physically installed.
- **Placeholder for a chassis that you do not yet have**. You can pre-provision compute nodes in a chassis that you do not yet have by defining a *placeholder chassis* to act as a target for the server pattern before the hardware arrives. The placeholder chassis bundles all of the server profiles that are created for each empty compute-node bay. So, when the hardware arrives, you can assign the server profiles to all compute nodes in the new chassis by deploying the placeholder chassis to the new chassis. Each server profile is activated after the associated compute node is rebooted.

Note: You can deploy a server pattern to multiple servers; however, multiple patterns cannot be deployed to a single server.

For more information about deploying a server pattern, see Deploying a server pattern to a server and Deploying a placeholder chassis.

Step 5. **Edit the server pattern.**

You use server patterns to control a common configuration from a single place. You no longer update settings directly on servers. Instead, you update category patterns and server patterns, and the changes are automatically deployed to all associated profiles and their servers.

For more information about editing a server pattern, see Modifying a server pattern.

Configuration considerations

Before you begin configuring servers through Lenovo XClarity Administrator, review the following important considerations.

- XClarity Administrator v2.8 does not support configuration patterns for ThinkSystem SR635 and SR655 servers in the following situations.
  - If XClarity Administrator v2.7 manages ThinkSystem SR635 and SR655 servers running 20A firmware, and you upgrade to 20B firmware using the baseboard management controller before upgrading to XClarity Administrator v2.8
  - If XClarity Administrator v2.7 manages ThinkSystem SR635 and SR655 servers running 20B firmware before upgrading to XClarity Administrator v2.8
  - If XClarity Administrator v2.8 manages ThinkSystem SR635 and SR655 servers running 20A firmware, and you upgrade to 20B firmware using the baseboard management controller
- The QLogic 8200 2-Port 10GbE SFP+ VFA adapter has invalid values for these settings: iSCSIFirstTargetParameters_iSCSIName, iSCSISecondTargetParameters_iSCSIName and IPv6LinkLocalAddress. You must manually correct these values in the system setup before learning the configuration pattern from the server or correct the values in the learned configuration pattern.
- For Flex System x240 and x440 Compute Nodes with embedded RAID adapters, server patterns that define RAID configuration definitions can be deployed only to one or more servers that do not have

existing RAID configurations. If a server pattern is deployed to a server that has an existing RAID configuration, the existing arrays and volumes are not overwritten. To apply the RAID configuration that is defined in the server pattern, you must first clear the servers existing RAID configuration (see Resetting storage adapters to default values), and then redeploy the server profile by selecting the server and clicking **More → Deploy Server Profile**.

- The onboard storage controllers in Flex System x220, Flex System x222, and ThinkSystem servers support software-based RAID. However, configuration of software RAID using Configuration Patterns is not supported.
- When configuring RAID using Configuration Patterns, if the server is powered off, the server boots to BIOS/UEFI Setup automatically before activating the server profile.
- For ThinkServer servers, Configuration Patterns are not supported.
- Certain I/O devices cannot be configured using server patterns. For more information, see XClarity Administrator Support – Compatibility webpage.
- If advanced features (such as SPAR, Easy Connect, and stack) are enabled on Flex switches EN4093R, CN4093, SI4093, or SI4091, network configurations might not be applied correctly on internal ports.
- By default, Flex switch SI4093 is shipped with SPAR enabled. If you want to deploy network settings using port patterns to internal ports on these switches, you must manually remove the switch internal ports from SPAR or remove the SPAR configurations from the switch.
- It is recommended that you *do not* use XClarity Administrator to configure the Converged and ThinkAgile appliances using Configuration Patterns.
- Ensure that all available ports are enabled on the installed adapters before creating the Configuration Patterns from an existing server so that all available ports and settings are included in the pattern. Then, if needed, you can disable any ports using the appropriate settings defined in the pattern. If ports are disabled when the pattern is created, the pattern might not be created correctly and the pattern might not deploy successfully.

Defining address pools

An *address pool* is a defined set of address ranges. Lenovo XClarity Administrator uses address pools to assign IP and I/O addresses to individual servers when the server patterns are deployed to those servers.

About this task

XClarity Administrator supports IP and I/O address pools.

IP address pools

IP address pools define ranges of IP addresses for use when configuring the baseboard management controller network interface of your servers. You can use or customize predefined address pools or you can create new pools as needed. When creating server patterns, you can choose which IP address pool to use during deployment. When the server pattern is deployed, IP addresses are allocated from the selected pool and assigned to individual management controllers.

Note: If you are satisfied with your management-controller network configuration, do not use this option.

Attention:

- Ensure that you select an IP address subrange that does not conflict with existing I/O addresses in your data center.
- Ensure that the IP addresses in the specified ranges are part of the same subnetwork and are reachable by XClarity Administrator.

- Ensure that the IP addresses in the specified ranges are unique for each XClarity Administrator domain and existing IP management tools to prevent address conflicts.

The overall address pool range is derived from the specified routing prefix length and the gateway or initial range. You can create pools of different sizes based on the specific routing prefix length, but overall pool ranges must be unique within the XClarity Administrator domain. Ranges are then created from the overall pool range.

Address ranges can be used to separate hosts (for example, by operating system type, workload types, and business type). Address ranges can also be tied to organizational network rules.

Ethernet address pools

Ethernet address pools are collections of unique MAC addresses that can be assigned to network adapters when configuring servers. You can use or customize predefined address pools as needed, or you can create new pools. When creating server patterns, you can choose which Ethernet address pool is to be used during deployment. When the server pattern is deployed, addresses are allocated from the selected pool and assigned to individual adapter ports.

The following predefined MAC addresses pool is available:
- Lenovo MAC address pool

For a list of MAC address ranges in this pool, see Ethernet address (MAC) pools.

Fibre Channel address pools

Fibre Channel address pools are collections of unique WWNN and WWPN addresses that can be assigned to Fibre Channel adapters when configuring servers. You can use or customize predefined address pools as needed, or you can create new pools. When creating server patterns, you can choose which Fibre Channel address pool is to be used during deployment. When the server pattern is deployed, addresses are allocated from the selected pool and assigned to individual adapter ports.

The following predefined Fibre Channel addresses pools are available:
- Lenovo WWN addresses
- Brocade WWN addresses
- Emulex WWN addresses
- QLogic WWN addresses

For a list of WWN address ranges in these pools, see Fibre Channel address (WWN) pools.

The range of addresses in the address pools must be unique within the XClarity Administrator domain. XClarity Administrator ensures that the defined ranges and assigned addresses are unique within its management domain.

Important: In large environments with multiple XClarity Administrator instances, ensure that unique address ranges are used by each XClarity Administrator to prevent address duplication.

Ethernet and Fibre Channel address pools are used with I/O adapter virtual addressing to assign organizationally unique I/O addresses. When you create a server pattern for a compute node, you can enable virtual addressing as part of the devices and I/O adapter configuration. When virtual addressing is enabled, addresses are assigned from the Ethernet and Fibre Channel address pools to prevent address conflicts.

Restriction: Virtual addressing is supported for only Flex System compute nodes. Standalone rack and tower servers are not supported.

For information about creating server patterns, see Creating a server pattern.

Creating an IP address pool

An *IP address pool* defines a range of IP addresses for use when configuring the baseboard-management-controller network interface of your servers. When the associated server pattern is deployed, IP addresses are allocated from the specified pool and assigned to individual servers.

About this task

The data in the Overall Network Information table on the New IP Address Pool dialog is derived from the specified subnet mask and gateway or initial range. You can create pools of different sizes based on the specific subnet mask, but overall pool ranges must be unique within the management domain. Ranges are then created from the overall pool range. All ranges must be part of the same sub network and are bound by the limits shown in the Overall Network Information table.

The pool and ranges have Lenovo XClarity Administrator scope. In large environments with multiple XClarity Administrator instances, create unique pools and ranges for each XClarity Administrator to avoid address conflicts and to avoid address conflicts with existing IP management tools. Ranges can also be used to separate hosts (for example, by operating system type, workload type, and business function) and to tie organization network rules.

Procedure

Complete the following steps to create an IP address pool.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Address Pools**. The Configuration Patterns: Address Pools page is displayed.

Step 2. Click the **IP Address Pools** tab.

Step 3. Click the **Create** icon ( ). The New IP Address Pools Wizard dialog is displayed.

Step 4. Fill in the following information.

- Name and description for the address pool.
- Choose to use IPv4 or IPv6 addresses.
- Select a subnet mask (for IPv4) or a routing prefix length (for IPv6).
- Specify the gateway address.The network information values are derived from the specified subnet mask and gateway or initial range and are filled in the table.
- Add one or more ranges of addresses:
  1. Click **Add Range** to add a range of addresses. The New Add IP Address Range dialog is displayed.
  2. Enter a range name, first address, and range size.The last address is calculated automatically.
  3. Click **OK**.The range is added to the **Define IP pool address ranges** table, and the fields in the summary section are updated automatically.

  You can edit the range by clicking the **Edit** icon ( ) or remove the range by clicking the **Remove** icon ( ).

Step 5. Click **Create**.

What to do next

The new IP address pool is listed in the table on the IP Address Pools page:



From this page, you can perform the following actions on a selected address pool:

- Modify the address pool by clicking the **Edit** icon ( ).
- Rename the address pool by clicking the **Rename** icon.
- Delete the address pool by clicking the **Delete** icon ( ).
- View details about the address pool, including a mapping between the virtual addresses and the installed adapter's ports and reserved virtual addresses, by clicking the pool name in the **Pool Name** column.

Creating an Ethernet address pool

Ethernet address pools are collections of unique media access control (MAC) addresses that can be assigned to network adapters. You can use or customize predefined address pools as needed, or you can create new address pools. When you create a server pattern, if you enable virtual addressing for Ethernet adapters, you can choose which Ethernet address pool is to be used when the pattern is deployed. When the associated server pattern is deployed, MAC addresses are allocated from the selected address pool and assigned to individual network adapters in the servers.

Procedure

Complete the following steps to create an Ethernet address pool.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Address Pools**. The Configuration Patterns: Address Pools page is displayed.

Step 2. Click the **Ethernet Address Pools** tab.

Step 3. Click the **Create** icon ( ). The New Ethernet (MAC) Address Pools dialog is displayed.

Step 4. Enter a name and description for the address pool.

Step 5. Add one or more ranges of addresses:

a. Click **Add Range** to add a range of addresses. The Ethernet (MAC) Address Range dialog is displayed.

b. Enter a range name, first MAC address, and range size.

The last MAC address is calculated automatically.

c. Click **Add**.

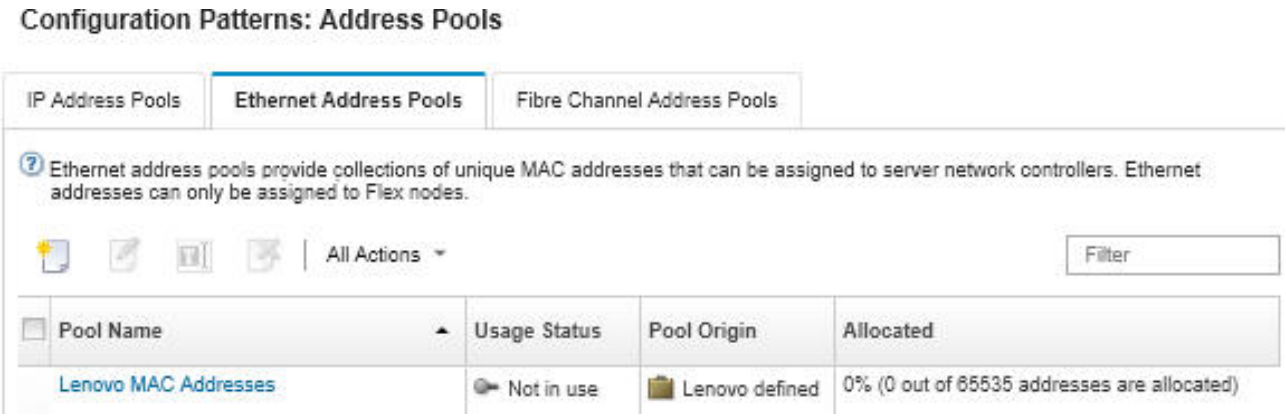
The range is added to the **Define Ethernet (MAC) pool address ranges** table, and the fields in the summary section are updated automatically.

You can edit the range by clicking the **Edit** icon ( ) or remove the range by clicking the **Remove** icon ( ).

Step 6. Click **Save**.

What to do next

The new Ethernet address pool is listed in the Ethernet Address Pools page.



From this page, you can perform the following actions on a selected address pool:

- Modify the address pool by clicking the **Edit** icon ( ).
- Rename the address pool by clicking the **Rename** icon.
- Delete the address pool by clicking the **Delete** icon ( ).
- View details about the address pool, including a mapping between the virtual addresses and the installed adapter's ports and reserved virtual addresses, by clicking the pool name in the **Pool Name** column.

Ethernet address (MAC) pools

Ethernet address pools are collections of unique media access control (MAC) addresses that can be assigned to network adapters. You can use the following predefined address pool in your server patterns.

Table 4. Lenovo MAC address pool

Predefined range	Starting address	Ending address
Range 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
Range 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
Range 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
Range 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
Range 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34
Range 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
Range 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
Range 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
Range 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Creating a Fibre Channel address pool

Fibre Channel address pools are collections of unique World Wide Node Name (WWNN) and World Wide Port Name (WWPN) addresses that can be assigned to Fibre Channel adapters. You can use or customize predefined address pools as needed, or you can create new pools. When creating server patterns, if you enable virtual addressing for Ethernet adapters, you can choose which Fibre Channel address pool is to be used when the pattern is deployed. When the associated server pattern is deployed, WWNN and WWPN addresses are allocated from the pool and assigned to individual servers.

Procedure

Complete the following steps to create a Fibre Channel address pool.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Address Pools**. The Configuration Patterns: Address Pools page is displayed.

Step 2. Click the **Fibre Channel Address Pools** tab.

Step 3. Click the **Create** icon ( ). The Fibre Channel Address Pools dialog is displayed.

Step 4. Enter a name and description for the address pool.

Step 5. Add one or more ranges of addresses:

a. Click **Add Range** to add a range of addresses. The Fibre Channel (WWN) Address Range dialog is displayed.

b. Enter a range name, range size, and the first address for each fabric.

The last addresses are calculated automatically.

c. Click **Add**.

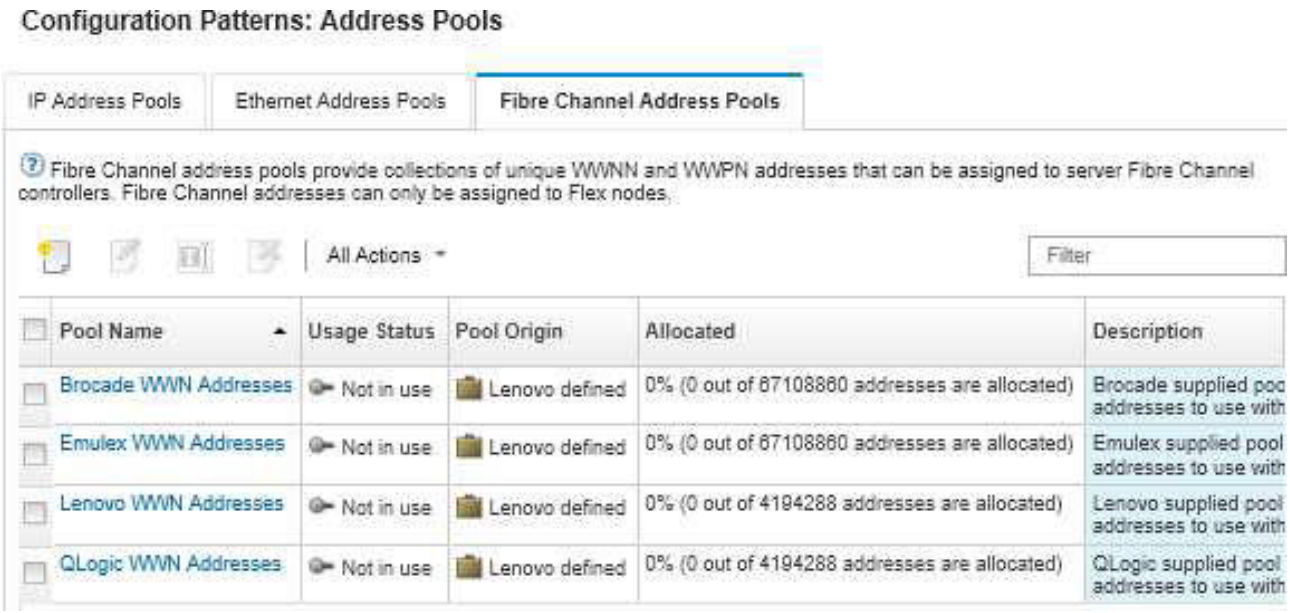
The range is added to the **Define Fibre Channel pool address ranges** table, and the fields in the summary section are updated automatically.

You can edit the range by clicking the **Edit** icon ( ) or remove the range by clicking the **Remove** icon ( ).

Step 6. Click **Save**.

What to do next

The new Fibre Channel address pool is listed in the Fibre Channel Address Pools table.



From this page, you can perform the following actions on a selected address pool:

- Modify the address pool by clicking the **Edit** icon ( ).
- Delete the address pool by clicking the **Delete** icon ( ).

- View details about the address pool, including a mapping between the virtual addresses and the installed adapter's ports and reserved virtual addresses, by clicking the pool name in the **Pool Name** column.

Fibre Channel address (WWN) pools

Fibre Channel address pools are collections of unique World Wide Node Name (WWNN) and World Wide Port Name (WWPN) addresses that can be assigned to Fibre Channel adapters. You can use the following predefined address pools in your server patterns.

Table 5 "Brocade WWN address pool" on page 310 lists the Brocade World Wide Name (WWN) address pools. Each Brocade range contains 1,864,135 addresses.

Table 6 "Emulex WWN address pool" on page 311 lists the EmulexWWN address pools. Each Emulex range contains 1,864,135 addresses.

Table 7 "Lenovo WWN address pool" on page 312 lists the Lenovo WWN address pools. Each Lenovo WWN range contains 116,508 addresses.

Table 8 "QLogic WWN address pool" on page 313 lists the QLogic WWN address pools. Each QLogic WWN range contains 116,508 addresses.

Table 5. Brocade WWN address pool

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Fabric A				
Range 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C:71:C6
Range 2	2B:FA:00:05:1E:1C:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C:71:C7	2B:FC:00:05:1E:38:E3:8D
Range 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54
Range 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
Range 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E:38:E2
Range 6	2B:FA:00:05:1E:8E:38:E3	2B:FA:00:05:1E:AA:AA:A9	2B:FC:00:05:1E:8E:38:E3	2B:FC:00:05:1E:AA:AA:A9
Range 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA:AA:AA	2B:FC:00:05:1E:C7:1C:70
Range 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
Range 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF:FF:FE
Fabric B				
Range 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C:71:C6
Range 2	2B:FB:00:05:1E:1C:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C:71:C7	2B:FD:00:05:1E:38:E3:8D
Range 3	2B:FB:00:05:1E:38:E3:8E	2B:FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38:E3:8E	2B:FD:00:05:1E:55:55:54

Table 5. Brocade WWN address pool (continued)

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Range 4	2B:FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71:C7:1B	2B:FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71:C7:1B
Range 5	2B:FB:00:05:1E:71:C7:1C	2B:FB:00:05:1E:8E:38:E2	2B:FD:00:05:1E:71:C7:1C	2B:FD:00:05:1E:8E:38:E2
Range 6	2B:FB:00:05:1E:8E:38:E3	2B:FB:00:05:1E:AA:AA:A9	2B:FD:00:05:1E:8E:38:E3	2B:FD:00:05:1E:AA:AA:A9
Range 7	2B:FB:00:05:1E:AA:AA:AA	2B:FB:00:05:1E:C7:1C:70	2B:FD:00:05:1E:AA:AA:AA	2B:FD:00:05:1E:C7:1C:70
Range 8	2B:FB:00:05:1E:C7:1C:71	2B:FB:00:05:1E:E3:8E:37	2B:FD:00:05:1E:C7:1C:71	2B:FD:00:05:1E:E3:8E:37
Range 9	2B:FB:00:05:1E:E3:8E:38	2B:FB:00:05:1E:FF:FF:FE	2B:FD:00:05:1E:E3:8E:38	2B:FD:00:05:1E:FF:FF:FE

Table 6. Emulex WWN address pool

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Fabric A				
Range 1	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:1C:71:C6	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:1C:71:C6
Range 2	2F:FE:00:00:C9:1C:71:C7	2F:FE:00:00:C9:38:E3:8D	2F:FC:00:00:C9:1C:71:C7	2F:FC:00:00:C9:38:E3:8D
Range 3	2F:FE:00:00:C9:38:E3:8E	2F:FE:00:00:C9:55:55:54	2F:FC:00:00:C9:38:E3:8E	2F:FC:00:00:C9:55:55:54
Range 4	2F:FE:00:00:C9:55:55:55	2F:FE:00:00:C9:71:C7:1B	2F:FC:00:00:C9:55:55:55	2F:FC:00:00:C9:71:C7:1B
Range 5	2F:FE:00:00:C9:71:C7:1C	2F:FE:00:00:C9:8E:38:E2	2F:FC:00:00:C9:71:C7:1C	2F:FC:00:00:C9:8E:38:E2
Range 6	2F:FE:00:00:C9:8E:38:E3	2F:FE:00:00:C9:AA:AA:A9	2F:FC:00:00:C9:8E:38:E3	2F:FC:00:00:C9:AA:AA:A9
Range 7	2F:FE:00:00:C9:AA:AA:AA	2F:FE:00:00:C9:C7:1C:70	2F:FC:00:00:C9:AA:AA:AA	2F:FC:00:00:C9:C7:1C:70
Range 8	2F:FE:00:00:C9:C7:1C:71	2F:FE:00:00:C9:E3:8E:37	2F:FC:00:00:C9:C7:1C:71	2F:FC:00:00:C9:E3:8E:37
Range 9	2F:FE:00:00:C9:E3:8E:38	2F:FE:00:00:C9:FF:FF:FE	2F:FC:00:00:C9:E3:8E:38	2F:FC:00:00:C9:FF:FF:FE
Fabric B				
Range 1	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:1C:71:C6	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:1C:71:C6
Range 2	2F:FF:00:00:C9:1C:71:C7	2F:FF:00:00:C9:38:E3:8D	2F:FD:00:00:C9:1C:71:C7	2F:FD:00:00:C9:38:E3:8D
Range 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54

Table 6. Emulex WWN address pool (continued)

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Range 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B
Range 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E:38:E2
Range 6	2F:FF:00:00:C9:8E:38:E3	2F:FF:00:00:C9:AA:AA:A9	2F:FD:00:00:C9:8E:38:E3	2F:FD:00:00:C9:AA:AA:A9
Range 7	2F:FF:00:00:C9:AA:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA:AA:AA	2F:FD:00:00:C9:C7:1C:70
Range 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
Range 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF:FF:FE

Table 7. Lenovo WWN address pool

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Fabric A				
Range 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C7:1B
Range 2	20:80:00:50:76:01:C7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C7:1C	21:80:00:50:76:03:8E:37
Range 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
Range 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
Range 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E3:8B
Range 6	20:80:00:50:76:08:E3:8C	20:80:00:50:76:0A:AA:A7	21:80:00:50:76:08:E3:8C	21:80:00:50:76:0A:AA:A7
Range 7	20:80:00:50:76:0A:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A:AA:A8	21:80:00:50:76:0C:71:C3
Range 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
Range 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:FF:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:FF:FB
Fabric B				
Range 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C7:1B
Range 2	20:81:00:50:76:21:C7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C7:1C	21:81:00:50:76:23:8E:37
Range 3	20:81:00:50:76:23:8E:38	20:81:00:50:76:25:55:53	21:81:00:50:76:23:8E:38	21:81:00:50:76:25:55:53

Table 7. Lenovo WWN address pool (continued)

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Range 4	20:81:00:50:76:25:55:5-4	20:81:00:50:76:27:1C:-6F	21:81:00:50:76:25:55:5-4	21:81:00:50:76:27:1C:-6F
Range 5	20:81:00:50:76:27:1C:-70	20:81:00:50:76:28:E3:8B	21:81:00:50:76:27:1C:-70	21:81:00:50:76:28:E3:8B
Range 6	20:81:00:50:76:28:E3:8C	20:81:00:50:76:2A:AA:A7	21:81:00:50:76:28:E3:8C	21:81:00:50:76:2A:AA:A7
Range 7	20:81:00:50:76:2A:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A:AA:A8	21:81:00:50:76:2C:71:C3
Range 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
Range 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:FF:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:FF:FB

Table 8. QLogic WWN address pool

Predefined range	WWNN starting address	WWNN ending address	WWPN ending address	WWPN ending address
Fabric A				
Range 1	20:80:00:E0:8B:00:00:00	20:80:00:E0:8B:01:C7:1B	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:01:C7:1B
Range 2	20:80:00:E0:8B:01:C7:1C	20:80:00:E0:8B:03:8E:37	21:80:00:E0:8B:01:C7:1C	21:80:00:E0:8B:03:8E:37
Range 3	20:80:00:E0:8B:03:8E:38	20:80:00:E0:8B:05:55:53	21:80:00:E0:8B:03:8E:38	21:80:00:E0:8B:05:55:53
Range 4	20:80:00:E0:8B:05:55:54	20:80:00:E0:8B:07:1C:6F	21:80:00:E0:8B:05:55:54	21:80:00:E0:8B:07:1C:6F
Range 5	20:80:00:E0:8B:07:1C:70	20:80:00:E0:8B:08:E3:8B	21:80:00:E0:8B:07:1C:70	21:80:00:E0:8B:08:E3:8B
Range 6	20:80:00:E0:8B:08:E3:8C	20:80:00:E0:8B:0A:AA:A7	21:80:00:E0:8B:08:E3:8C	21:80:00:E0:8B:0A:AA:A7
Range 7	20:80:00:E0:8B:0A:AA:A8	20:80:00:E0:8B:0C:71:C3	21:80:00:E0:8B:0A:AA:A8	21:80:00:E0:8B:0C:71:C3
Range 8	20:80:00:E0:8B:0C:71:C4	20:80:00:E0:8B:0E:38:DF	21:80:00:E0:8B:0C:71:C4	21:80:00:E0:8B:0E:38:DF
Range 9	20:80:00:E0:8B:0E:38:E0	20:80:00:E0:8B:0F:FF:FB	21:80:00:E0:8B:0E:38:E0	21:80:00:E0:8B:0F:FF:FB
Fabric B				
Range 1	20:81:00:E0:8B:20:00:00	20:81:00:E0:8B:21:C7:1B	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:21:C7:1B
Range 2	20:81:00:E0:8B:21:C7:1C	20:81:00:E0:8B:23:8E:37	21:81:00:E0:8B:21:C7:1C	21:81:00:E0:8B:23:8E:37
Range 3	20:81:00:E0:8B:23:8E:38	20:81:00:E0:8B:25:55:53	21:81:00:E0:8B:23:8E:38	21:81:00:E0:8B:25:55:53

Table 8. QLogic WWN address pool (continued)

Prede-fined range	WWNN starting address	WWNN ending address	WWPN ending address	WWPN ending address
Range 4	20:81:00: E0:8B:25:55:54	20:81:00: E0:8B:27:1C:6F	21:81:00: E0:8B:25:55:54	21:81:00: E0:8B:27:1C:6F
Range 5	20:81:00: E0:8B:27:1C:70	20:81:00:E0:8B:28: E3:8B	21:81:00: E0:8B:27:1C:70	21:81:00:E0:8B:28: E3:8B
Range 6	20:81:00:E0:8B:28: E3:8C	20:81:00:E0:8B:2A:AA: A7	21:81:00:E0:8B:28: E3:8C	21:81:00:E0:8B:2A:AA: A7
Range 7	20:81:00:E0:8B:2A:AA: A8	20:81:00:E0:8B:2C:71: C3	21:81:00:E0:8B:2A:AA: A8	21:81:00:E0:8B:2C:71: C3
Range 8	20:81:00:E0:8B:2C:71: C4	20:81:00:E0:8B:2E:38: DF	21:81:00:E0:8B:2C:71: C4	21:81:00:E0:8B:2E:38: DF
Range 9	20:81:00:E0:8B:2E:38: E0	20:81:00:E0:8B:2F:FF: FB	21:81:00:E0:8B:2E:38: E0	21:81:00:E0:8B:2F:FF: FB

Working with server patterns

A *server pattern* represents pre-OS server configuration, including local storage, I/O adapter, SAN boot, and other baseboard-management-controller and UEFI firmware settings. Server patterns also integrate support for virtualizing I/O addresses so that you can virtualize server fabric connections or repurpose servers without disruption. A server pattern is used as an overall pattern to quickly configure multiple servers at one time.

About this task

You can define multiple server patterns to represent different configurations that are used in your data center.

When defining a server pattern, select or create category patterns and address pools as needed to construct the desired configuration for a specific group of servers. A *category pattern* defines specific firmware settings that can be reused by multiple server patterns. You can use address pools to define address ranges to use to assign addresses to individual servers when deploying server patterns. There are IP address pools, Ethernet Address (MAC) pools, and Fibre Channel Address (WWN) pools.

When a server pattern is deployed to multiple servers, multiple server profiles are generated automatically (one profile for each server). Each profile inherits settings from the parent server pattern, so you can control a common configuration from a single place.

You can create a server pattern from scratch, defining your desired configuration before your hardware arrives. Or, you can create a server pattern from an existing server and then use that pattern to provision your remaining servers. If you create a server pattern from an existing server, extended category patterns are learned and dynamically created from the current settings for the server. If you want to change the category settings, you can edit them directly from the server patterns.

Attention: When you create a new server pattern from scratch, you must define the boot settings for the servers. When you deploy the server pattern to servers, the existing boot order on the servers is overwritten with the default boot-order settings in the server pattern. If the servers do not start after you deploy a server pattern to those servers, the problem might be that the original boot settings were overwritten by the default boot order settings in the new server pattern. To restore the original boot settings on the servers, see Recovering boot settings after server pattern deployment.

Important: When you create server patterns, ensure that you create them for each type of server. For example, create a server pattern for all Flex System x240 compute nodes and another server pattern for all Flex System x440 compute nodes. Do not deploy a server pattern that was created for one server type to another server type.

Important: If the management node fails, you might lose your server patterns. Always back up the management software after you create or modify server patterns (see Backing up Lenovo XClarity Administrator).

Settings for network devices

Some Flex System network devices offer more configuration options in server patterns than others.

Although server patterns can be applied to any network device, some server-patterns functionality is limited to certain network adapters. Additionally, some advanced settings for Ethernet network adapters (such as adapter and port compatibility preferences) are not currently supported.

Server patterns can learn existing configuration data and settings for supported network adapters and can change configuration settings through pattern deployment.

Category patterns

The firmware settings are organized into categories that group together related settings. For each category, you can create a *category pattern* that contains common firmware settings and can be reused by multiple server patterns. Most of the firmware settings that you can configure directly on the baseboard management controller and UEFI can also be configured through category patterns. The firmware settings that are available depend on the server type, your Flex System environment, and the scope of the server pattern.

You can create category patterns separately from server patterns.

Category patterns can be predefined, learned from existing servers, or user-defined.

- **Extended category patterns**

  Extended category patterns are patterns for some I/O adapter ports, advanced Unified Extensible Firmware Interface (UEFI), and baseboard management-controller (BMC) settings that are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended category patterns; however, you can edit the patterns after they are created.

  The following Extended UEFI patterns are predefined by XClarity Administrator to optimize your servers for specific environments.
  - **ESXi Install Options**
  - **Efficiency – Favor Performance**
  - **Efficiency – Favor Power**
  - **Maximum Performance**
  - **Minimal Power**

- **User-defined category patterns**

  User-defined category patterns are patterns that you can create, including system information, management interfaces, devices and I/O ports, Fibre Channel boot targets, and I/O adapter ports. You can create the following category patterns:

  - **System information**. Settings include automatically generated system name, location, contacts.
  - **Management interface**. Settings include the automatically generated hostname, IP address, domain name space (DNS), interface speed, and port assignments for the management interface.Duplex settings are not supported by server patterns.

– **Devices and I/O ports**. Settings include console redirection and COM ports. You can use server patterns to enable serial over LAN in the Console Redirection area. However, when serial over LAN is enabled, the only serial-port access mode setting that is supported by server patterns is **Dedicated**; the **Shared** and **Pre-Boot** IPMI settings for serial-port access mode are not available in server patterns.

  Important: If you create a server pattern from an existing server, and that server has the serial-port access mode setting **Shared** or **Pre-Boot**, the device and I/O ports pattern that is learned from the server has the serial-port access mode setting **Dedicated**.

– **Fibre Channel boot targets**. Settings include specific primary and secondary Fibre Channel WWN boot targets.

– **Ports**. Settings include I/O adapters and ports for configuring fabric interconnects.

Creating a server pattern

When you create a server pattern, you define the configuration characteristics for a specific type of server. You can create a server pattern from scratch using default settings or using settings from an existing server.

About this task

Before you create a server pattern, consider the following suggestions.

- The first time that you create a server pattern, consider creating it from an existing server. When you create a server pattern from an existing server, Lenovo XClarity Administrator learns and creates extended category patterns for some I/O adapter ports, UEFI, and baseboard management controller settings. Then, those category patterns are available for use in any server pattern that you create later. For more information about category patterns, see Defining firmware settings.
- Identify groups of servers that have the same hardware options and that you want to configure the same way. You can use a server pattern to apply the same configuration settings to multiple servers, thereby controlling a common configuration from one place.
- Identify the aspects of configuration that you want to customize for the server pattern (for example, local storage, network adapters, boot settings, management controller settings, UEFI settings).
- You cannot manage local user accounts or configure the LDAP server using Configuration Patterns.

Important: If the management node fails, you might lose your server patterns. Always back up the management software after you create or modify server patterns (see Backing up Lenovo XClarity Administrator).

Procedure

To create a server pattern, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

Step 3. Click the **Create** icon ( ). The New Server Pattern Wizard is displayed.

Step 4. To create the server pattern, perform one of the following actions.

- Click **Create a new pattern from an existing server** to use settings from an existing server. Then, select the managed server on which the new pattern is to be based from the displayed list.

  When you create a server pattern from an existing server, XClarity Administrator learns the settings from the specified managed server (including the extended port, UEFI, and management-controller settings) and dynamically creates category patterns for those settings. If the server is brand new, Lenovo XClarity Administrator learns the manufacturing settings. If XClarity Administrator is managing the server, XClarity Administrator uses the customized

settings. You can then customize the settings specifically for the servers to which this pattern is to be deployed.

- Click **Create a new pattern from scratch** to use default settings. Then, select the server type in the **Form Factor** field.

Note: The options that are presented on the remaining tabs might differ depending on the type of server for which you are creating a pattern.

Step 5. Enter the name of the pattern and a description.

Step 6. Optional: Customize the server-profile name by selecting the **Custom** toggle and then selecting one or more elements to include in the naming schema (such as custom text, server name, and incrementing number) and the order.

Step 7. Click **Next**

Step 8. Choose the local storage configuration to be applied when this pattern is deployed to a server, and click **Next**.

For information about local storage settings, see Defining local storage.

Step 9. Optional: **Optional:** Modify the I/O adapter addressing, and define additional I/O adapters to match the hardware that you expect to configure with this pattern, and click **Next**.

For information about I/O adapter settings, see Defining I/O adapters.

Step 10. Define the boot order to be applied when this pattern is deployed to a server, and click **Next**.

For information about SAN boot targets settings, see Defining boot options.

Step 11. Select firmware settings from the list of existing category patterns.

You can create new category patterns by clicking the **Create** icon ( ).

For information about firmware settings, see Defining firmware settings.

Step 12. Click **Save** to save the pattern, or click **Save and Deploy** to save and immediately deploy the pattern to one or more servers.

For information about deploying a server pattern, see Deploying a server pattern to a server.

What to do next

If you clicked **Save and Deploy**, the Deploy Server Pattern page is displayed. From this page, you can deploy the server pattern to specific servers.

If you clicked **Save**, the server pattern and all category patterns are saved to the Server Patterns page.



From this page, you can perform the following actions on selected server patterns:

- View details about the pattern by clicking the pattern name in the **Name** column.
- Deploy the pattern (see Deploying a server pattern to a server).
- Copy the pattern by clicking the **Copy** icon ( ).
- Edit the pattern (see Modifying a server pattern).
- Rename the pattern by clicking the **Rename** icon ( ).
- Delete the pattern by clicking the **Delete** icon ( ).
- Export and import server patterns (see Exporting and importing server and category patterns).

Defining local storage

You can define the local-storage configuration to be applied to target servers when this pattern is deployed.

About this task

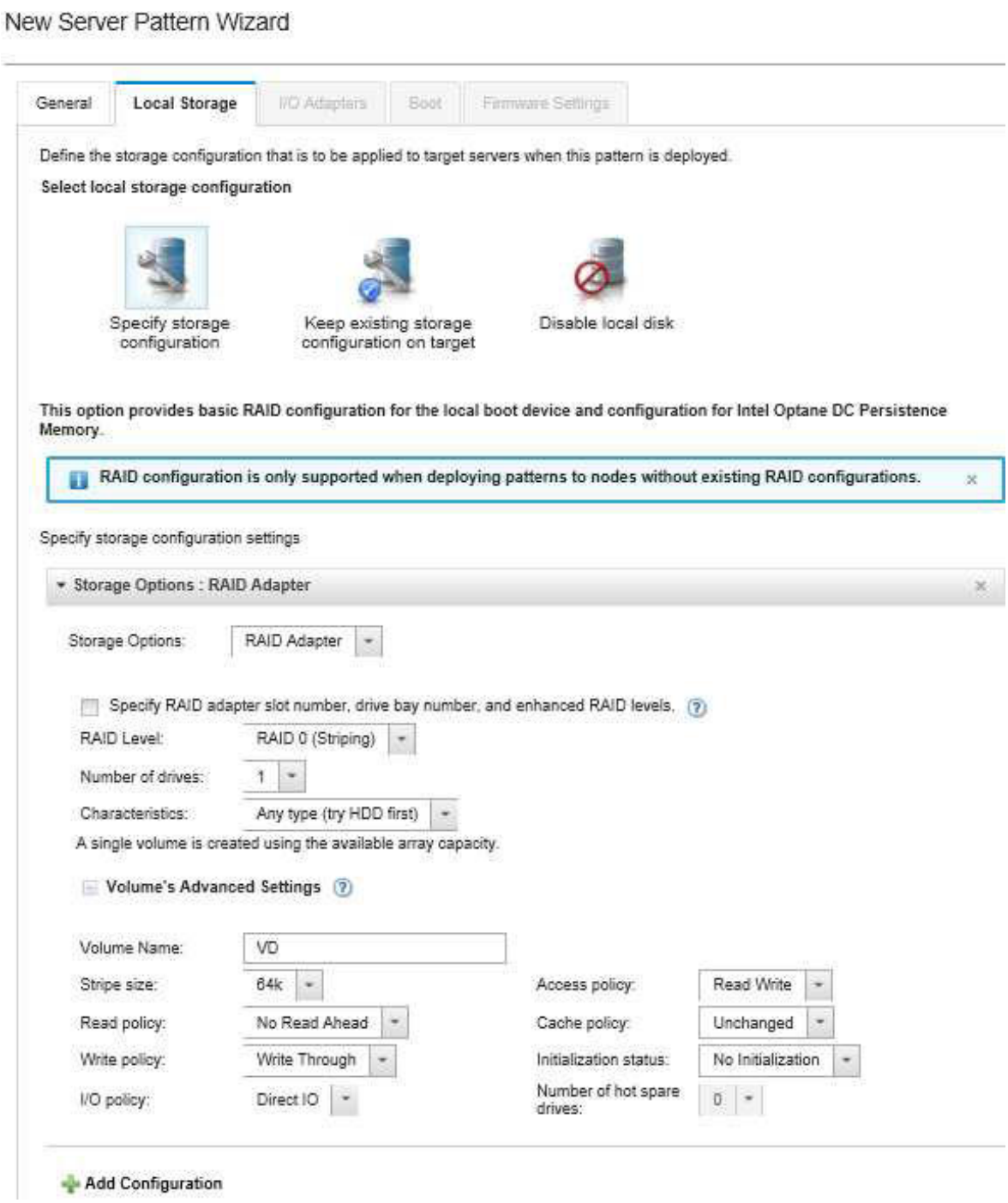
Notes:

- The onboard storage controllers in Flex System x220, Flex System x222, and ThinkSystem servers support software-based RAID. However, configuration of software RAID using Configuration Patterns is not supported.
- When configuring RAID using Configuration Patterns, if the server is powered off, the server boots to BIOS/UEFI Setup automatically before activating the server profile.

Procedure

To define the local-storage configuration, complete the following steps.

Step 1. From the New Server Pattern Wizard, click the **Local Storage** tab.



Step 2. To define local-storage settings, choose one of the following options.

- **Specify storage configuration**. (Devices without exiting RAID configurations only) Basic RAID settings are configured on the local boot device during deployment

  Specify the storage configuration based on the storage option. You can add additional storage options by clicking the **Add** (➕) icon.

  – **RAID Adapter**. Choose the RAID level, characteristics, and the number of drives that are installed in the server. RAID 0, 1, 5 are supported. In addition, you can choose advanced volume settings, such as stripe size, policies, and number of hot spare drives.

ThinkSystem servers with XCC version 2.1 and later (ThinkSystem SR950 requires XCC version 1.4 or later), you can also specify the RAID adapter slot number and drive bay numbers to create a single volume using the available array capacity. In this case, RAID level 0, 1, 5, 6, 10, 50, 60, and 00 are supported. In addition, you can choose advanced volume settings, such as stripe size, policies, and hot spare drives.

Note: On the target server, ensure that there are enough available drives of the specified type, and ensure that the RAID state of the drives is "Unconfigured Good," as reported in the **Drives** section on the servers Inventory Details page (see Viewing the details of a managed server).

- **Lenovo SD Media Adapter**. Choose the where to create the volume and the volume size. You can also choose advanced volume settings, such as media type and access policy.
- **ThinkSystem M.2 with Mirroring**. Choose the PCI slot, RAID level, volume name, and stripe size to create a single volume using the available array capacity.
  - You can define multiple ThinkSystem M.2 with Mirroring storage adapters, each in a different PCI slot.
  - For ThinkSystem Edge Servers, you must specify a specific PCI slot number. For other ThinkSystem servers that have only one M.2 RAID adapter installed, you can choose First Matched (the default value) or specify a specific PCI slot number.
- **Intel Optane DC Persistent Memory**. Choose the type of persistent memory, warning threshold for the percentage of remaining capacity, and percentage of total capacity to be used as memory. (The remaining memory is used as persistent storage).

  Attention:
  - To configure Intel Optane DC Persistent Memory DIMMs, security must be disabled and a namespace must not be created.
  - Enable Security is supported only when the security state is “Disabled” for all Intel Optane DC Persistent Memory DIMMs in the server.
  - Disable Security and Secure Erase are supported only when the security state is “Locked” and the passphrase is the same for all Intel Optane DC Persistent Memory DIMMs in the server.
  - The Intel Optane DC PMEM security state is not included in the XClarity Administrator inventory. You can manually check the security state in UEFi.

- **Keep existing storage configuration on target**. The existing storage configuration is not changed during deployment. Choose this option to use the storage configuration that is already in place on the target server.
- **Disable local disk**. (Flex System x240 Compute Node only) The on-board storage controller and storage option ROM (both UEFI and Legacy) are disabled during deployment. Disabling the local disk drive decreases the overall boot time when booting from SAN.

Defining I/O adapters

You can define I/O port settings and addressing mode to be applied to target servers when this pattern is deployed.

About this task

If you intend to virtualize or reassign your I/O adapter addresses, you can configure this pattern to use virtual I/O adapter addressing.

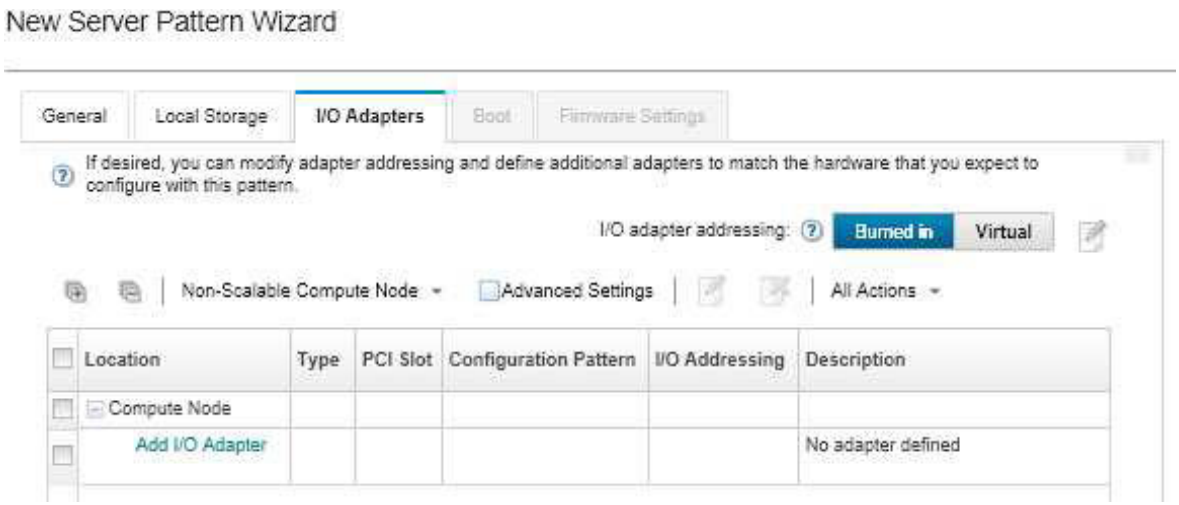
If you are creating a pattern from an existing server, some adapter information might be automatically learned. You can define additional I/O adapter patterns to match the hardware that you expect to have in the servers when this pattern is deployed. By defining I/O adapter patterns, you can configure adapter-port

settings for your supported adapter. If using virtual I/O adapter addresses, you can also define SAN boot targets for Fibre Channel adapters that you add (see Defining boot options).

Procedure

To define I/O adapter settings, complete the following steps.

Step 1. From the New Server Pattern Wizard, click the **I/O Adapters** tab.



Note: You can display additional information about the I/O adapters by clicking **Advanced Settings**.

Step 2. If you are creating a server pattern for a server in a Flex System chassis, choose the type of I/O-adapter addressing mode:

- **Burned in**. Use existing World Wide Name (WWN) and Media Access Control (MAC) addresses that are provided with the adapter from manufacturing.
- **Virtual**. Use virtual I/O adapter addressing to simplify the management of LAN and SAN connections. Virtualizing I/O-addresses reassigns the burned-in hardware addresses with virtualized Fibre WWN and Ethernet MAC addresses. This can speed deployment by pre-configuring SAN zone membership and facilitate failover by eliminating the need to reconfigure SAN-zoning and LUN-masking assignments when replacing hardware.

  When virtual addressing is enabled, both Ethernet and Fibre Channel addresses are allocated by default regardless of defined adapters. You can choose the pool from which Ethernet and Fibre Channel addresses are allocated.

  You can also edit virtual-address settings by clicking the **Edit** icon ( ) next to the address modes.

  Restriction: Virtual addressing is supported for only servers in Flex System chassis. Rack and tower servers are not supported.

Step 3. If you are creating a server pattern for a server in a Flex System chassis, select one of the following scalability options. The rows in the table change based on what is selected.
- Non-scalable Flex system
- 2 node scalable Flex system
- 4 node scalable Flex system

Step 4. Choose the I/O adapters that you expect to be installed in the servers to which the pattern is to be deployed. To add an adapter:

a. Click the **Add I/O Adapter** link in the table to display the Add I/O Adapter 1 or LOM dialog.

b. Select the PCI slot for the adapter.

c. Select the adapter type from the table.

Note: By default, the table lists only I/O adapters that are currently installed in the managed servers. To list all supported I/O adapters, click **All Supported Adapters**.

d. Select the initial port pattern to be assigned to all ports in the port group when the pattern is deployed.

Port patterns are used to modify port settings that are learned from the server. These initial port patterns are assigned when the adapter is first added. After the adapter is added, you can assign different patterns to individual ports from the I/O Adapter page.

You can create a port pattern by clicking the **Create** icon ( ). You can create a port pattern based on an existing pattern by clicking the **Edit** icon ( ).

For more information about port patterns, see Defining port settings.

e. Click **Add** to add the port pattern to the table on the I/O Adapter page.

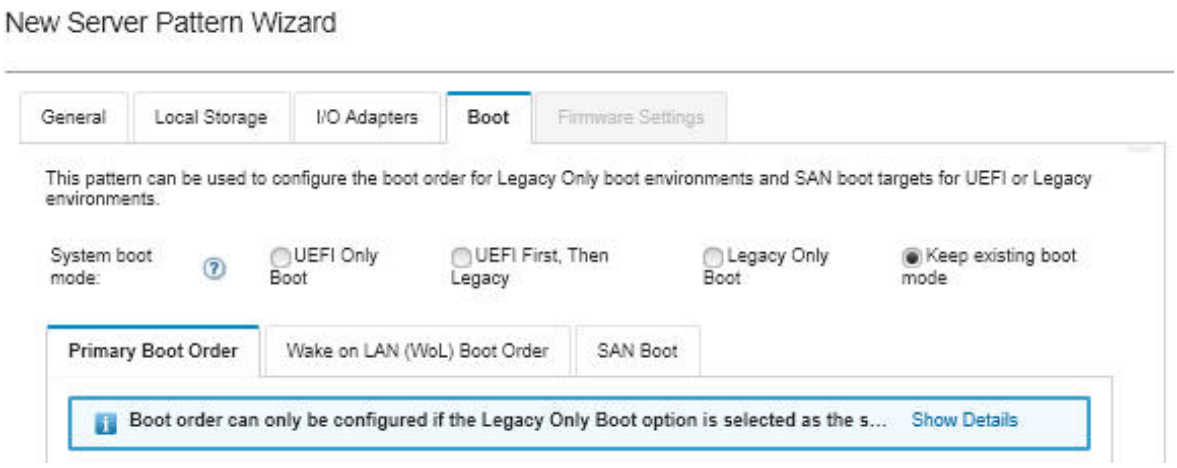
Defining boot options

You can define the boot order to be applied to the target servers when this pattern is deployed.

Procedure

Complete the following steps to create a boot-options pattern.

Step 1. From the New Server Pattern Wizard, click the **Boot** tab.



Step 2. Select one of the following system-boot modes:

- **UEFI Only Boot**. Select this option to configure a server that supports Unified Extensible Firmware Interface (UEFI). If you are booting UEFI-enabled operating systems, this option might shorten boot time by disabling legacy option ROMs.

  If the pattern is learned from a Thinksystem server, you can click the **Primary Boot Order** tab to specify the boot order. You can keep the boot order that is specified on the server to which the pattern is to be deployed or configure the boot order to specify the order in which boot options are to be applied. However, boot priority of boot devices in a device group (boot option) is not supported.

- **UEFI First, Then Legacy**. Select this option to configure a server to attempt to boot using UEFI first. If there is an issue, the server attempts to boot in legacy mode.

If the pattern is learned from a Thinksystem server, you can click the **Primary Boot Order** tab to specify the boot order. You can keep the boot order that is specified on the server to which the pattern is to be deployed or configure the boot order to specify the order in which boot options are to be applied. However, boot priority of boot devices in a device group (boot option) is not supported.

- **Legacy Only Boot**. Select this option if you are configuring a server to boot an operating system that requires legacy (BIOS) firmware. Select this option only if you are booting non-UEFI enabled operating systems.

  Tip: If you select the legacy-only boot mode (which makes boot time much faster), you cannot activate any Features on Demand (FoD) keys.

  If you choose this option, you can specify:

  – **Primary Boot Order**. Choose to keep the boot order specified on the server to which the pattern is to be deployed. You can also choose to configure the Legacy Only boot order to specify the order in which boot options are to be applied.

  – **Wake on LAN (WoL) Boot Order**. Choose to keep the current WoL boot order specified on the server to which the pattern is to be deployed. You can also choose to configure the Legacy Only boot order to specify the order in which WoL boot options are to be applied.

- **Keep existing boot mode**. Select this option to keep the existing settings on the target server. No changes to the boot order are made when the pattern is deployed.

Step 3. Select the **SAN Boot** tab to choose a boot target pattern and specify boot device targets.

Note: If you defined Fibre Channel adapters and enabled virtual addressing when you defined the I/O adapters, you can set SAN primary and secondary boot targets for the Fibre Channel adapters. You can specify multiple worldwide port name (WWPN) and logical unit number (LUN) identifiers for the storage targets.

Defining firmware settings

You can specify the baseboard management controller and UEFI firmware settings that are to be applied to target servers when this pattern is deployed.

About this task

The firmware settings are organized into categories that group together related settings. For each category, you can create a *category pattern* that contains common firmware settings and can be reused by multiple server patterns. Most of the firmware settings that you can configure directly on the baseboard management controller and UEFI can also be configured through category patterns. The firmware settings that are available depend on the server type, your Flex System environment, and the scope of the server pattern.

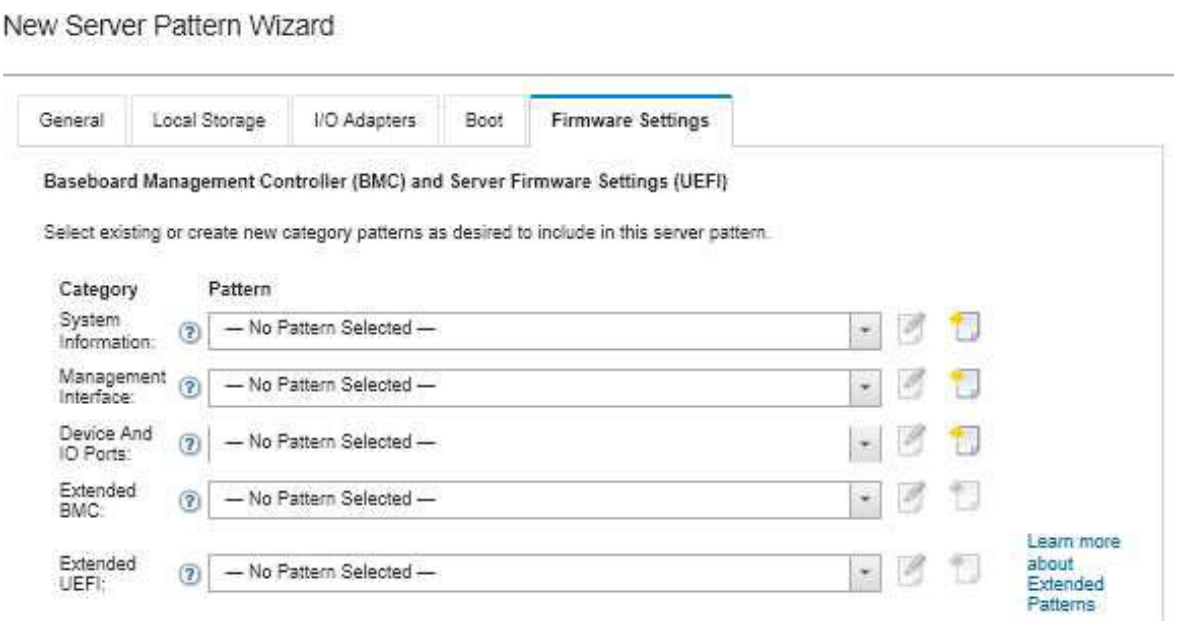
Category patterns can be predefined, user-defined, or learned from existing servers:

- *Extended category patterns* are patterns for some I/O adapter ports, advanced Unified Extensible Firmware Interface (UEFI), and baseboard management-controller (BMC) settings that are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended category patterns; however, you can edit the patterns after they are created.
- *User-defined category patterns* are patterns that you can create, including system information, management interfaces, devices and I/O ports, Fibre Channel boot targets, and I/O adapter ports.

Procedure

Complete the following steps to define firmware settings.

Step 1. From the New Server Pattern Wizard, click the **Firmware Settings** tab.



Step 2. Choose the category-pattern type that includes the settings that you want to define.

- **System information**. Use this category pattern to define automatic system-name generation, contact names, and locations. For more information about system-information patterns, see Defining system-information settings.
- **Management interfaces**. Use this category pattern to define automatic host-name generation, management IP-address assignments, domain name system (DNS) settings, and internet speed settings. For more information about management-interfaces patterns, see Defining management-interface settings).
- **Devices and I/O ports**. Use this category pattern to define console redirection and COM ports, PCIe speed, onboard devices, adapter option ROM, and option ROM execution order. For more information about device and I/O port patterns, see Defining devices and I/O ports settings.
- **Extended BMC**. Use this category pattern to define other baseboard management-controller settings. The extended management-controller patterns are automatically created when you create a server pattern from an existing server. You cannot manually create an extended management-controller pattern. For more information about management-interfaces patterns, see Defining extended management-controller settings.).
- **Extended UEFI**. Use this category pattern to define other Unified Extensible Firmware Interface (UEFI) settings. The extended UEFI patterns are automatically created when you create a server pattern from an existing server. You cannot manually create an extended UEFI pattern. For more information about management-interfaces patterns, see Defining extended UEFI settings).

Step 3. Create new category patterns by clicking the **Create** icon ( ) next to that category-pattern type.

You can also edit an existing category pattern by selecting a specific pattern from the drop-down list and clicking the **Edit** icon ( ) next to that category-pattern type. You can also copy an existing category pattern by editing the pattern and clicking **Save As** to save it with a new name.

Defining system-information settings

You can define system name, contact, and location information by creating a system information pattern.

Procedure

Complete the following steps to create a system-information pattern.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **System Information Patterns** vertical tab, and then click the **Create** icon ( ).

Tip: You can also create a new system-information pattern from the Firmware Settings page of the New Server Pattern wizard by clicking the **Create** icon next to the **System Information** selection.

Step 4. In the New System Information Pattern dialog, specify the following information.

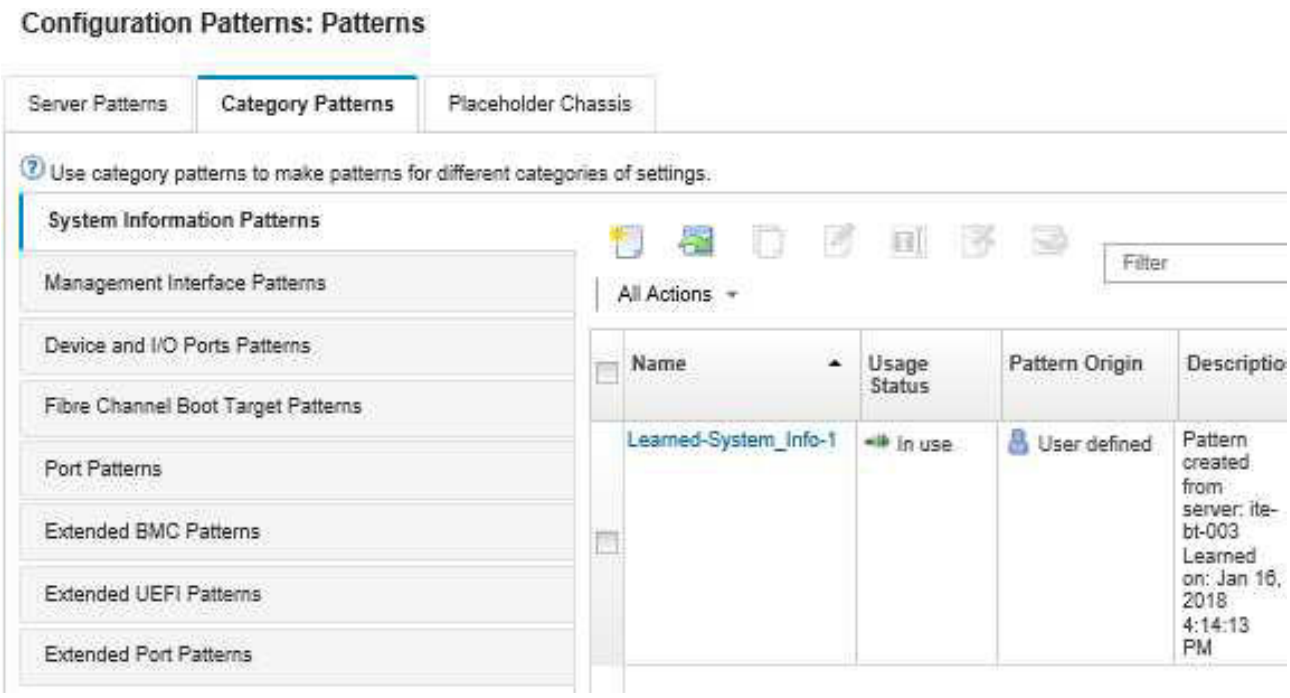
- Enter a name and description for the pattern.
- Choose whether to automatically generate system names. If you click **Custom**, you can specify how names are to be generated when the pattern is deployed. If you click **Disable**, the system name remains unchanged on each server when the pattern is deployed. For most devices, the name is limited to 256 English characters by the baseboard management controller. Automatically generated names are truncated to 256 characters.
- Specify the person to be contacted for this server and the location of the server.

  Note: If SNMP is enabled, you must specify a contact and system location.

Step 5. Click **Create**.

Results

The new pattern is listed on the **System Information Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).

- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining management-interface settings

You can define hostnames, IP address, domain name system (DNS), interface speed, and port assignments for the management interface by creating a management interface pattern.

Procedure

Complete the following steps to create a management-interface pattern.

Note: Duplex settings are not supported by server patterns.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Management Interface Patterns** vertical tab, and then click the **Create** icon ( ).

Tip: You can also create a new management-interface pattern from the Firmware settings page of the New Server Pattern wizard by clicking the **Create** icon ( ) next to the **Management Interface** selection.

Step 4. In the New Management Interface Pattern dialog, specify the following information.

- Enter a name and description for the pattern.
- Click the **Hostname** tab, and choose whether to automatically generate hostnames. If you click **Custom**, you can specify how names are to be generated when the pattern is deployed. If you click **Disable**, the hostname remains unchanged on each server when the pattern is deployed.

  Hostnames are limited to 63 English characters by the baseboard management controller. Automatically generated names are truncated to 63 characters.
- Click the **Management IP Addresses** tab, and configure IPv4 and IPv6 addresses settings.

  For **IPv4** addresses, you can choose one of the following options:
  - **Obtain dynamic IP address from DHCP server**.
  - **First by DHCP**. If it is not successful, obtain a static IP address from the address pool.
  - **Obtain a static IP address from the address pool.**

  For **IPv6** addresses, you can choose to:
  - **Use the stateless address auto configuration**.
  - **Obtain a dynamic IP address from a DHCP server**.
  - **Obtain a static IP address from the address pool**.

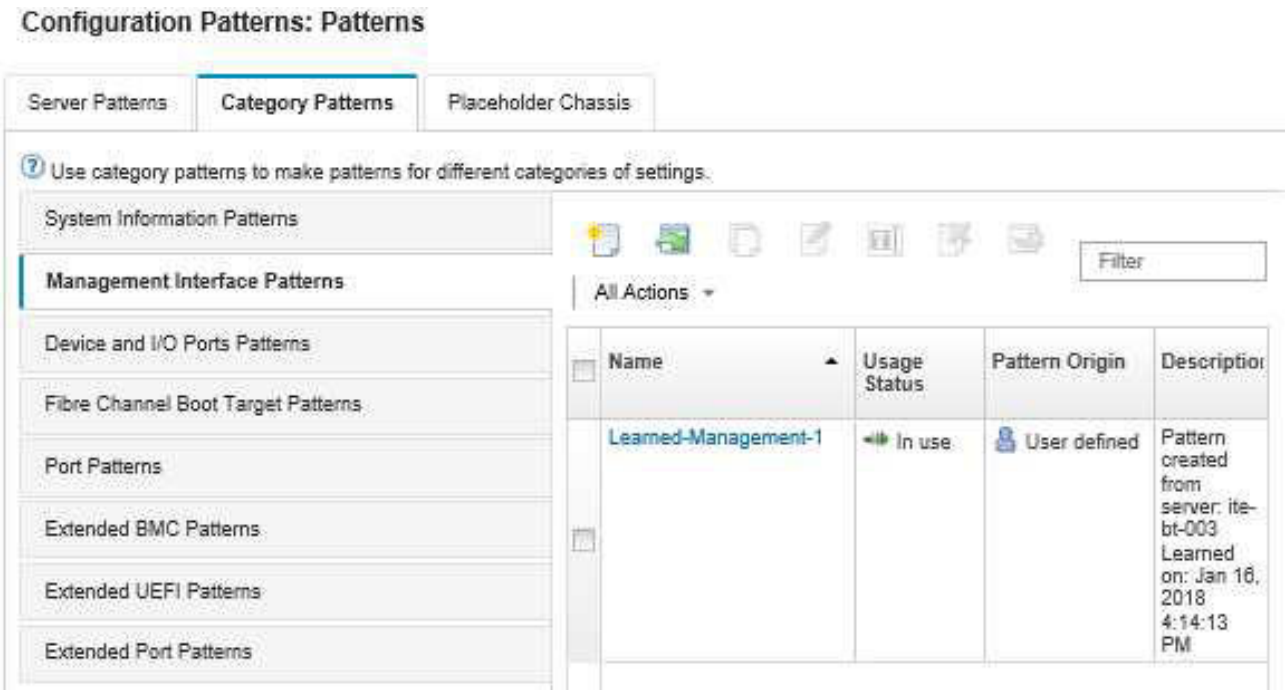
  In the **Domain Name System (DNS)** tab, choose to enable or disable the Dynamic Domain Name Service (DDNS). If you enable DDNS, you can choose one of the following options:
  - Obtain domain name from DHCP server.
  - Specify a domain name.
- Click the **Interface Settings** tab, and specify the maximum transmission unit (MTU). The default is 1500.
- Click the **Port Assignments** tab, and specify the numbers to use for the following ports:
  - HTTP
  - HTTPS
  - Telnet CLI
  - SSH CLI

- SNMP agent
- SNMP traps
- Remote control console
- CIM over HTTP
- CIM over HTTPS

Step 5. Click **Create**.

Results

The new pattern is listed on the **Management Interface Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining devices and I/O ports settings

You can enable console redirection and enable and define the characteristics of the COM 1 port by creating a device and I/O ports pattern.

Procedure

To create a device and I/O ports pattern, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Devices and I/O Ports Patterns** vertical tab, and then click the **Create** icon ( ).

Tip: You can also create a devices and I/O ports pattern from the Firmware Settings page of the New Server Pattern wizard by clicking the **Create** icon ( ) next to the **Devices and I/O Ports** selection.

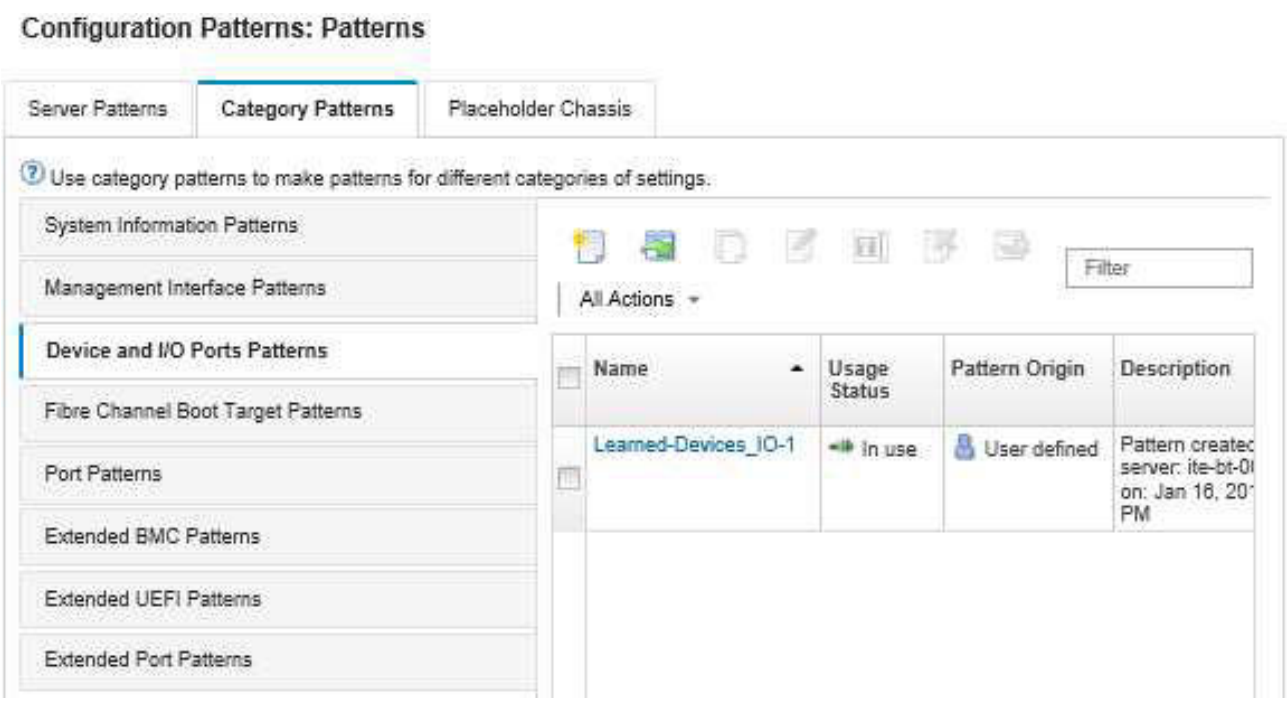
Step 4. In the New Devices and I/O Ports Pattern dialog, specify the following information.

- Enter a name and description for the pattern.
- Choose to enable or disable console redirection. If you enable console redirection, you can choose to enable or disable the following:
  - **Serial over LAN**.
  - **Service processor redirection**. If you enable service processor redirection, you can choose to use COM port 1 or 2 for the Legacy optional serial data port. Note that if disabled, COM port 1 is always used.You can also choose one of the following CLI modes:
    - Disable
    - Enable with user-defined keystroke sequence
    - Enable with EMS compatible keystroke sequence
- Choose to enable or disable COM ports 1 and 2. If you choose to enable COM ports, specify the following settings:
  - Baud rate
  - Data bits
  - Parity
  - Stop bits
  - Text emulation
  - Active after boot
  - Flow control

Step 5. Click **Create**.

Results

The new pattern is listed on the **Devices and I/O Ports Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining Fibre Channel boot-target settings

You can configure the server to boot from a storage area network (SAN) device instead of from local disk drive by creating a Fibre Channel boot-target pattern.

Procedure

Complete the following steps to create a Fibre Channel boot-target pattern.

Restriction: Fibre Channel boot targets are supported for only Flex compute nodes. Standalone rack and tower servers are not supported.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Fibre Channel Boot Target Pattern** vertical tab, and then click the **Create** icon ( ).

Step 4. In the New Fibre Channel Boot Target Pattern dialog, specify the following information.

- Enter a name and description for the pattern.
- Specify one or more WWPN addresses and LUN identifiers to use as primary boot targets. In addition, you can optionally specify one or more WWPN addresses and LUN identifiers to use as secondary boot targets.

  For example, you can add the storage primary paths as primary targets, and the storage secondary paths as secondary targets. By using different target groups in different server

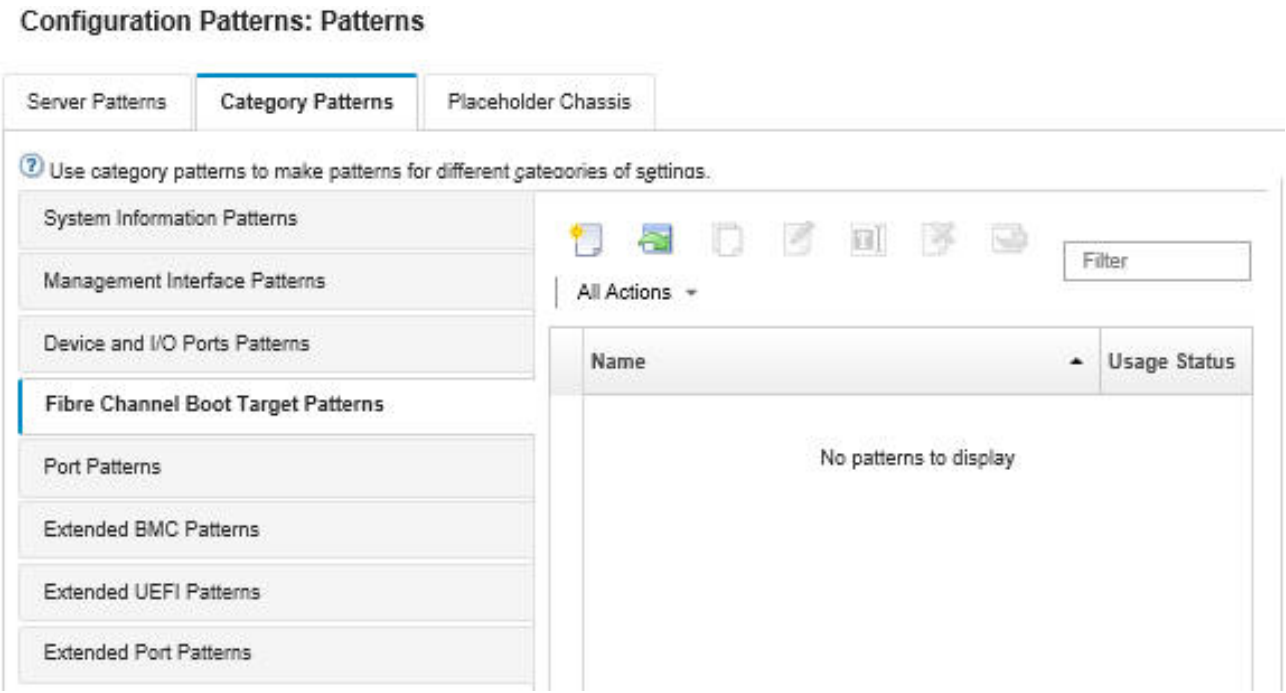
patterns, you can balance the storage load during simultaneous boot requests from multiple hosts.

Tip: If you specify `00:00:00:00:00:00:00:00` for the WWPN, XClarity Administrator attempts to boot from the first discovered target.

Step 5. Click **Create**.

Results

The new pattern is listed on the **Fibre Channel Boot Target Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining port settings

You can define typical port settings for a specific I/O adapter type by creating a port pattern.

About this task

You can use network settings in port patterns to configure switch internal ports. However, you cannot use port patterns to configure the switch global settings, such as VLAN IDs, global UFP mode, global CEE mode, and global FIPs. You must manually configure the global settings using the following rules that are compatible with the internal port settings that you intend to deploy before you deploy the port patterns. You

also cannot use port patterns to configure the PVID tagging. See the documentation that came with your switch to determine the compatibility checks between the global settings and internal port settings and how to configure these settings for that switch.

- Ensure that **globalCEEState** is “On” when PFC is configured.
- Ensure that **globalCEEState** is “On” when vport is set to “FCoE” mode.
- Ensure that **globalCEEState** is “On” and **globalFIPsState** is “On” when FIPs are configured.
- Ensure that **globalUFPMode** is “Enable” when the switch internal port mode is set to “UFP” mode.
- Ensure that the VLAN ID is created before adding a port to a specific VLAN.

Procedure

Complete the following steps to create an I/O adapter port pattern.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Port Pattern** vertical tab, and then click the **Create** icon ( ).

Tip: You can also create a new port pattern from the Add I/O Adapter page by clicking the **Create** icon ( ) next to the **Initial port pattern** selection.

Step 4. In the New Port Pattern dialog, specify the following information.

- Enter a name and description for the pattern.
- Specify the following adapter and port compatibility settings. When assigning patterns to adapters and ports, pattern settings are filtered based on compatibility with the target adapter or port.
  - Target adapter type
  - Target port operational mode, including:
    - pNIC mode
    - vNIC virtual fabric mode
    - vNIC switch independent mode
    - vNIC unified fabric protocol mode

    These settings enable NIC virtualization. For more information, see NIC Virtualization in Flex System Fabric Solutions.
  - Target port protocols, including:
    - Ethernet only
    - Ethernet and FCoE
    - Ethernet and iSCSI
  - Port extended settings pattern, which is used to configure additional port settings that are learned from the server
- If you set the target port operational mode to **pNIC mode**, choose to apply corresponding settings to the Flex switch internal ports, where applicable. If selected, you can configure additional VLAN and advanced settings:
  - Specify the target port protocol.
  - If you set the target port protocol to **Ethernet and FCoE**, optionally select and specify the priority 2 ID.
- If you set the target port operational mode to **vNIC virtual fabric mode**, configure the physical function settings, including the type and VLAN tag for each function.

- If you set the target port operational mode to **vNIC switch independent mode**, specify the type, minimum bandwidth and VLAN tag for each enabled function. You can also choose to apply corresponding settings to the Flex switch internal ports, where applicable. If selected, you can configure additional switch internal port and advanced settings:
  - Specify the default LAN, which is used only by the operating system when the operating system sends untagged packets.
  - Specify a comma separated list of VLANs.
  - Choose to configure manual control and specify the triggers.
  - Choose to configure flow control type, including
    - Keep existing flow control
    - Priority-based flow control
    - Link-level flow control

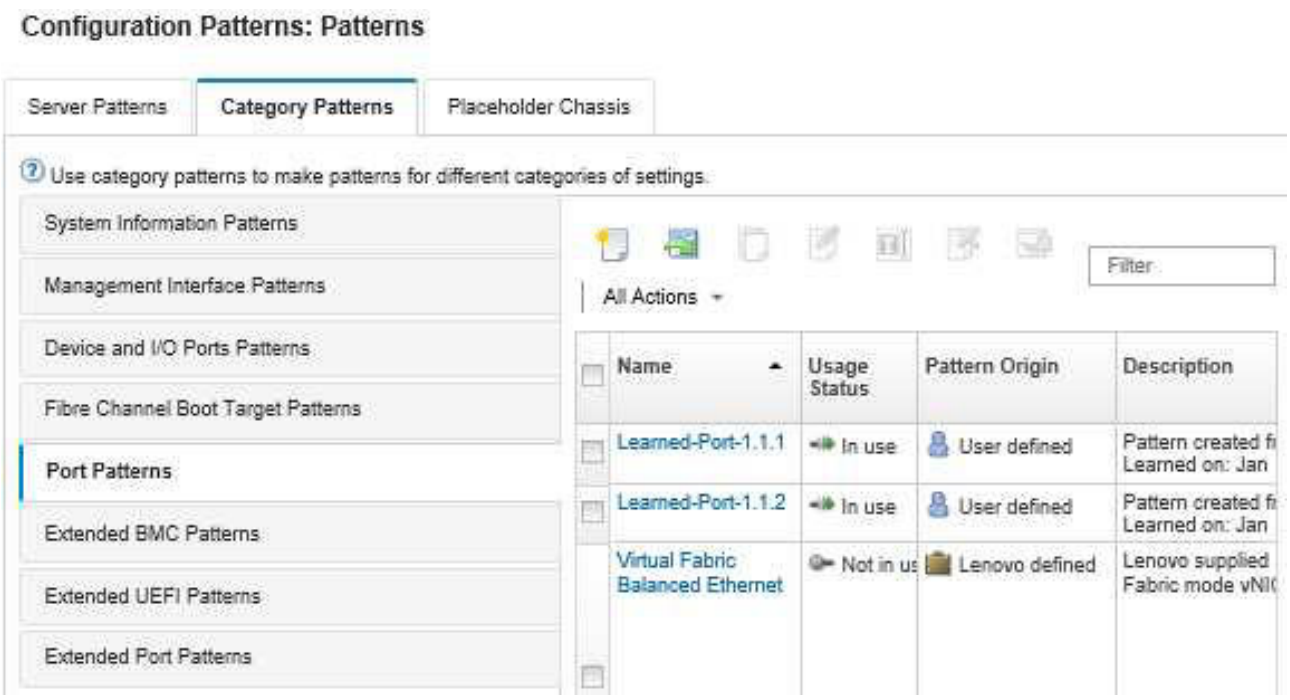
    For more information about these flow-control types, see the documentation that came with your Flex switch.
- If you set the target port operational mode to **vNIC unified fabric protocol mode**, choose to apply corresponding settings to the Flex switch internal ports, where applicable. If selected, you can configure additional UFP function and advanced settings:
  - Specify the QoS Mode (bandwidth or priority).
  - Choose to enable default VLAN ID tagging and specify the mode, minimum bandwidth and VLAN tag for each enabled function.
  - Choose to configure layer 2 failure and specify the number of triggers for each function.
  - For bandwidth QoS mode, specify the flow control type (priority based, link-level, or existing flow control).
  - For bandwidth QoS mode, choose to whether priority 4 is enabled when iSCSI is selected.

  Note: Ensure that global failover is “On” when defining failover triggers.

Step 5. Click **Create**.

Results

The new pattern is listed on the **Port Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended management-controller settings

The extended baseboard management-controller settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended management-controller patterns; however, you can copy and modify the patterns that have already been created.

Before you begin

Note: IMM thermal setting might conflict with the UEFI operating-mode setting. If they do conflict, the UEFI settings overwrites the IMM setting when the device is rebooted, and any thermal settings that you define in an extended baseboard management-controller pattern will be out of compliance. To resolve the non-compliance issue, either remove the setting from the extended baseboard management-controller pattern or select a setting that does not conflict with the current UEFI operating-mode setting.

Procedure

Complete the following steps to modify extended management-controller patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended BMC Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ( ).

Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

- To configure DNS settings, click **Network Settings Interface → DNS Configuration**. You can enable DNS, select the IP protocol, and specify up to three IPv4 or IPv6 addresses, and enable the discovery of XClarity Administrator IP addresses.

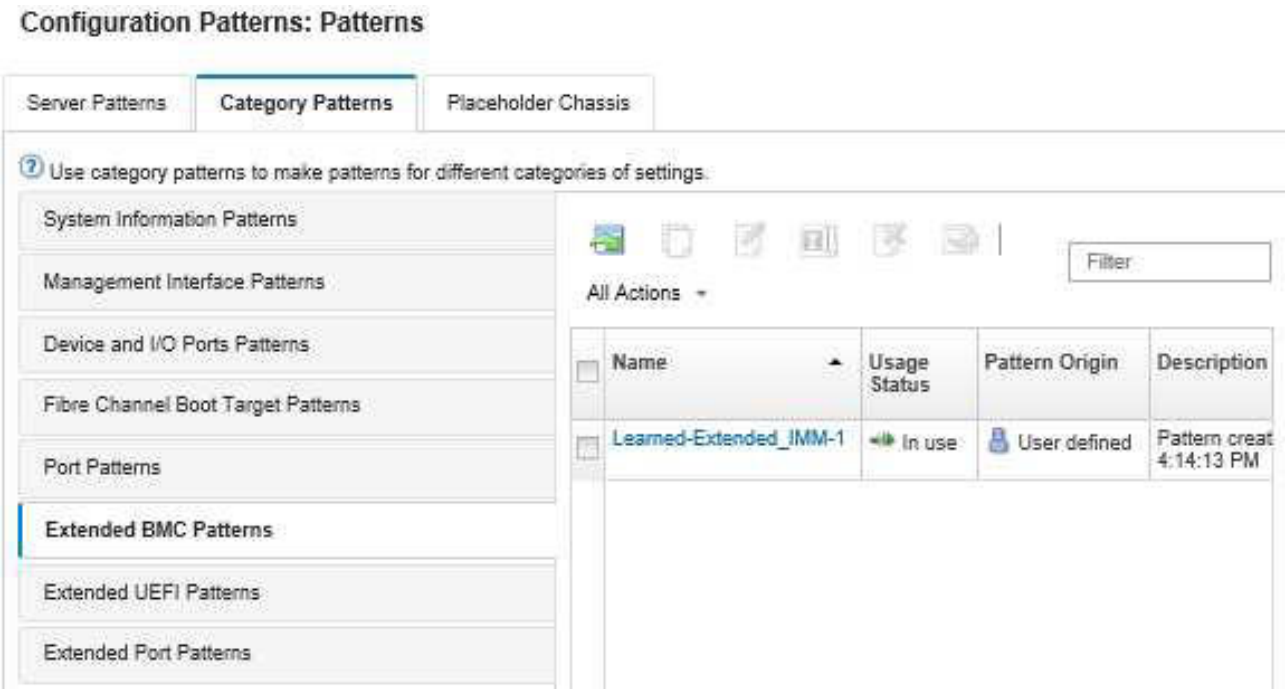
  Note: For Flex System devices, you can configure only the IP address to use to discover the XClarity Administrator server.
- To configure NTP settings, click **Network Settings Interface → Integrated Module NTP Setting**. You can specify the host name for up to 4 NTP servers and the frequency.

  Note: For Flex System devices, you cannot configure NTP settings.
- (Rack servers only) To data and time settings, click **General Settings → Integrated Module Clock Settings**. You can specify the time zone (UTC offset), enable or disable daylight savings time (DST), and choose whether to use UTC or the local time on the host.
- To change user account security settings, click **Account Security Configuration**.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended BMC Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).

- Rename a pattern by clicking the **Rename** icon ().
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended UEFI settings

The extended Unified Extensible Firmware Interface (UEFI) settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended UEFI patterns; however, you can copy and modify the patterns that have already been created.

About this task

The following Extended UEFI patterns are predefined by Lenovo XClarity Administrator to optimize your servers for specific environments.

- **ESXi Install Options**
- **Efficiency – Favor Performance**
- **Efficiency – Favor Power**
- **Maximum Performance**
- **Minimal Power**

Notes:

- Modification of UEFI security settings (including secure boot, trusted platform module (TPM), and physical presence policy configuration) are not supported using Extended UEFI Patterns.
- You can modify the UEFI administrator password for selected ThinkSystem and ThinkAgile servers from the Servers page by clicking **All Actions → Security → UEFI Administrator Password**. Lenovo XClarity Controller firmware level 20A is required.

Procedure

Complete the following steps to modify extended UEFI patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended UEFI Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ().

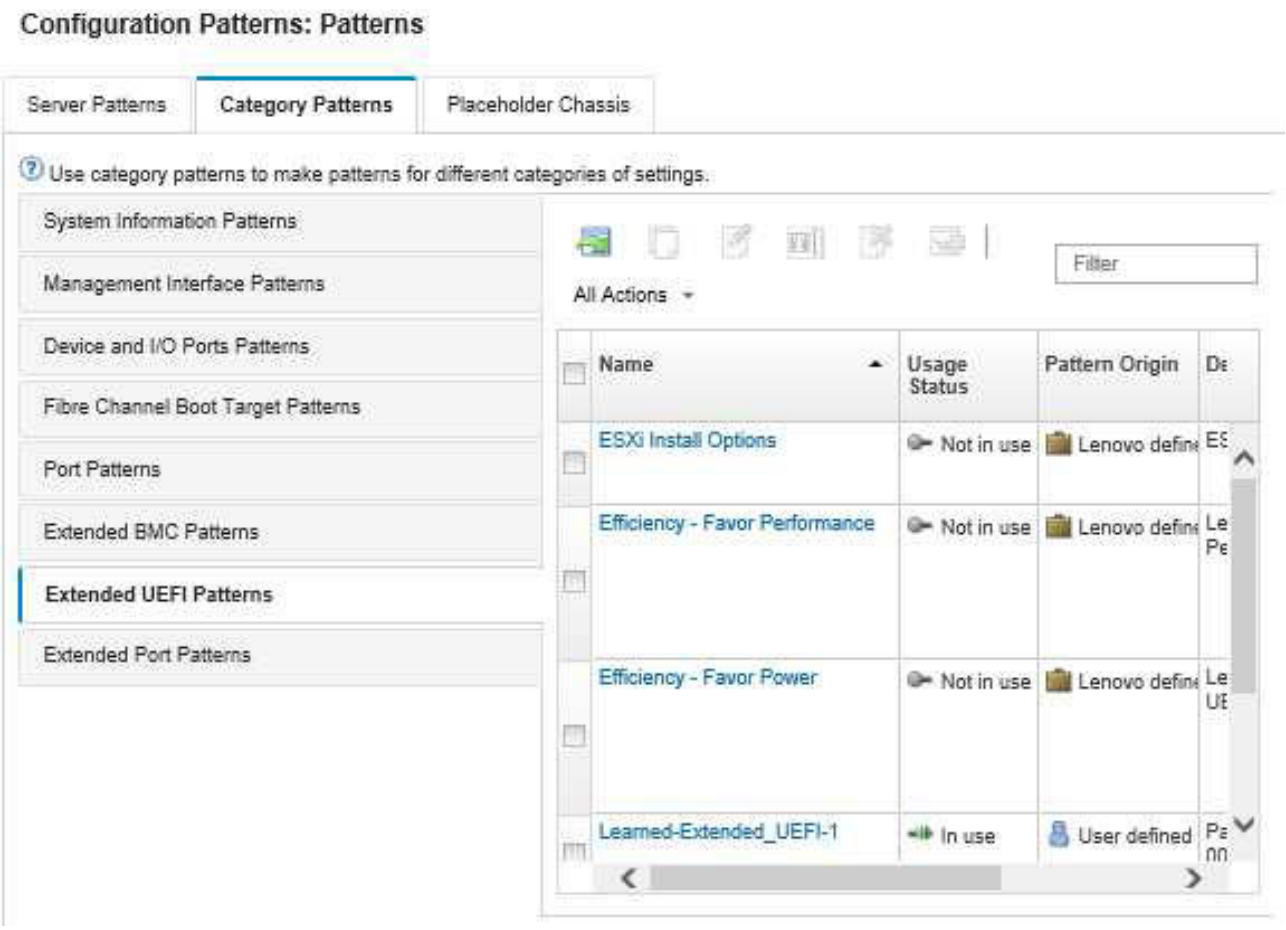
Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended UEFI Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended port settings

Extended port settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended port patterns; however, you can copy and modify the patterns that have already been created.

About this task

XClarity Administrator provides the following predefined extended port pattern:

- **Virtual fabric balanced Ethernet**. Lenovo supplied port pattern for Virtual Fabric mode vNIC mode, Ethernet only

Some device-level settings on Mellanox and Broadcom I/O adapters must be set to the same value on all ports. If the settings are set to different values on different ports, the settings for one port will be used, and the settings for other ports will be out of compliance. To resolve the non-compliance issue, select the same value for those device level settings.

For Mellanox I/O adapters, the following settings must be set to the same value on all ports.
- Advanced power settings
- PCI Virtual Functions Advertised
- Slot power limiter
- Virtualization Mode

For Broadcom I/O adapters, the following settings must be set to the same value on all ports.
- Banner Message Timeout
- BW Limit
- BW Limit Valid
- BW Reservation
- BW Reservation Valid
- Enable PME Capability
- Maximum Number of PF MSI-X Vectors
- Multi-Function Mode
- Number of MSI-X Vectors per VF
- Number of VFs Per PF
- Option ROM
- SR-IOV
- Support RDMA

Procedure

Complete the following steps to modify extended port patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended Port Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ( ).

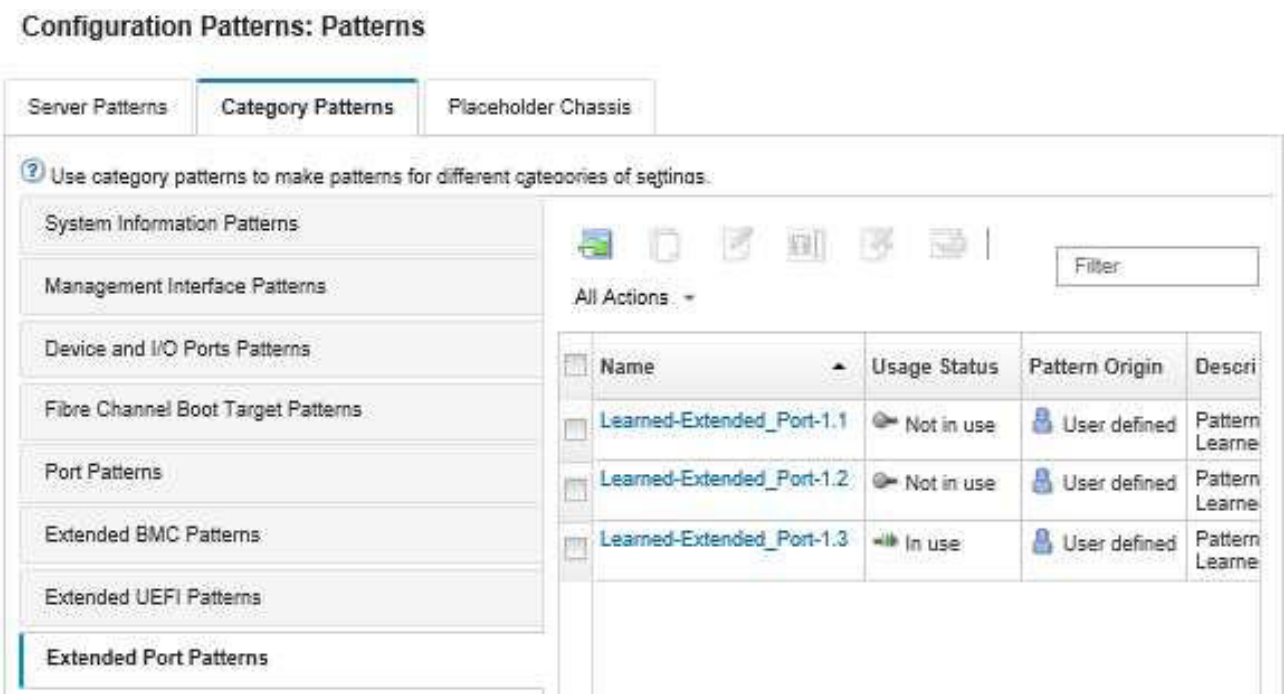
Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended Port Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended SR635/SR655 BIOS settings

The extended SR635/SR655 BIOS settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing ThinkSystem SR635 or SR655 server. You cannot manually create extended SR635/SR655 BIOS patterns; however, you can copy and modify the patterns that have already been created.

Procedure

Complete the following steps to modify extended SR635/SR655 BIOS patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended SR635/SR655 BIOS Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ( ).

Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended SR635/SR655 BIOS Patterns** tab in the Configuration Patterns: Category Patterns page:

From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Deploying a server pattern to a server

You can deploy a server pattern to one or more managed servers. You can also deploy a server pattern to one or more empty bays in a chassis that is managed by Lenovo XClarity Administrator or in a placeholder chassis. Deploying a server pattern before the server is installed reserves management IP addresses, reserves virtual Ethernet or Fibre Channel addresses, and pushes the network setting to the relative switch internal ports.

Procedure

To deploy a server pattern to a managed server, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

Step 3. Select the server pattern to deploy, and click the **Deploy** icon ( ).

The Deploy Server Pattern dialog is displayed with the selected server pattern listed in the **Pattern to Deploy** list.

Step 4. Choose when to activate the configurations:

- **Full**. Immediately powers on or restarts the server to activate server, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) configurations.
- **Partial**. (default) Immediately activates management-controller configurations, but defers the activation of server and UEFI configurations until the next server restart. The server must be manually powered on or restarted before the profile is fully activated.

  Note: When deploying server patterns that included only IMM settings (including system information, management interface, and extended BMC category patterns), the server does not need to be restarted.
- **Deferred**. Generates a profile for the server, management controller, and UEFI configurations but does not activate the configuration settings on the server. You must manually activate the server profile by restarting the server before the profile is fully activated.

Note: The network settings on the relative switch internal ports are pushed to the switch immediately after the deployment, regardless of activation configuration.

Step 5. Choose one or more servers or empty chassis bays to which you want to deploy the server pattern.

Note: To display a list of empty chassis bays, select **Show Empty Bays**.

Step 6. Click **Deploy**. A dialog is displayed that lists the deployment status of each selected bay.

Step 7. Click **Deploy** again to start the deployment process.

Note: Deployment might take several minutes to complete. During deployment, a server profile is created and assigned to each selected server or chassis bay.

Step 8. Click **Close**.

What to do next

You can monitor the deployment progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar. You can also monitor the server-profile creation by clicking **Provisioning → Server Profiles**. After the deployment is complete, review the generated server profiles, and record the management IP address and any virtualized Ethernet or Fibre-Channel addresses.

If you deployed a server pattern to an existing server and selected:

- **Full** activation, a server profile is created for each server, the configuration is propagated to each server, and each server is rebooted to activate the configuration changes.
- **Partial** activation, a server profile is created for each server, and the configuration is propagated to each server. To fully activate the configuration changes, you must manually power on or restart each server (see Powering on and off a server).
- **Deferred** activation, a server profile is created for each server. You must manually activate the server profile on the server (see Activating a server profile).

If you deployed a server pattern to an empty bay in a managed chassis or placeholder chassis, after the compute nodes are physically installed in appropriate chassis bays and then discovered and managed by Lenovo XClarity Administrator, you must deploy and activate the server profile to the newly installed compute nodes (see Activating a server profile).

If one or more servers do not start after you deployed a new server pattern to those servers, the problem might be that the boot settings were overwritten with the default boot settings that are in the server pattern. For operating systems that are installed in UEFI mode, restoring the default settings might require additional configuration steps to restore the boot configuration. For examples for recovering boot settings on servers that are running on Windows or Linux, see Recovering boot settings after server pattern deployment.

Modifying a server pattern

You can make subsequent configuration changes to an existing server pattern. If the original server pattern is deployed to servers (if it is in use), you can redeploy the changed server pattern to all or a sub-set of those servers.

About this task

Note: If you choose not to redeploy the changed server pattern to a set of servers, those servers remain associated with the original unchanged server pattern.

By editing the server pattern, you can control a common configuration from a single place and retain the original set of virtual address assignments.

Procedure

Complete the following steps to modify a server pattern.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

Step 3. Select the server pattern to edit, and click the **Edit** icon (). The Edit Server Patterns Wizard is displayed.

Step 4. Enter the name of the pattern and a description.

Step 5. Choose the local storage configuration to be applied when this pattern is deployed to a server, and click **Next**.

For information about local storage settings, see Defining local storage.

Step 6. Optional: **Optional:** Modify the I/O adapter addressing, and define additional I/O adapters to match the hardware that you expect to configure with this pattern, and click **Next**.

For information about I/O adapter settings, see Defining I/O adapters.

Step 7. Define the boot order to be applied when this pattern is deployed to a server, and click **Next**.

For information about SAN boot targets settings, see Defining boot options.

Step 8. Select firmware settings from the list of existing category patterns.

You can create new category patterns by clicking the **Create** icon ( ).

For information about firmware settings, see Defining firmware settings.

Step 9. Click **Save** to save the changes to save configuration changes to the current server pattern, or click **Save As** to save the configuration changes to a new server pattern.

Step 10. Choose to save the changes to the current server pattern or to a new server pattern.

- Click **Save** to save the changes to the current server pattern. From the Save and Redeploy Pattern dialog, perform these steps:
  1. Choose when to activate the configurations.
     - **Full**. Immediately powers on or restarts the server to activate server, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) configurations.
     - **Partial**. (default) Immediately activates management-controller configurations, but defers the activation of server and UEFI configurations until the next server restart. The server must be manually powered on or restarted before the profile is fully activated.

       Note: When deploying server patterns that included only IMM settings (including system information, management interface, and extended BMC category patterns), the server does not need to be restarted.

     Note: The network settings on the relative switch internal ports are pushed to the switch immediately after the deployment, regardless of activation configuration.
  2. Select the target servers to which you want to redeploy the configuration changes. You can choose all of the servers to which the original server pattern was deployed or a subset of those server.
  3. Click **Redeploy**
- Click **Save As** to save changes to a new server pattern. To deploy the new pattern, see Deploying a server pattern to a server.

Exporting and importing server and category patterns

If you have multiple Lenovo XClarity Administrator instances, you can export server and category patterns from one XClarity Administrator instance and import them in another XClarity Administrator instance.

About this task

You can export only server and category patterns. Policies, address pools, and profiles cannot be exported. Exported patterns are dissociated with any reference address pools. To leverage the address pools in an

imported pattern, edit the pattern and re-associate the pattern with the pools in XClarity Administrator in which they are imported.

Note: When you export a server patterns, the associated category patterns are also exported.

Procedure

- To export one or more patterns:
  1. From the XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.
  2. Click the **Server Patterns** or **Category Patterns** tab.
  3. Select one or more patterns to be exported.
  4. Click the **Export** icon ().
  5. Click **Export** to export the patterns.
  6. Save the pattern-data file to your local system.

     Note: If an exported pattern references address pools, these references are removed from the exported pattern to avoid conflicts when the pattern is imported into another XClarity Administrator instance. When the pattern is imported again, you can edit the imported pattern and assign the desired address pools.
- To import one or more patterns:
  1. From the XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.
  2. Click the **Import** icon () to import the patterns. The Import Patterns dialog is displayed.
  3. Click **Select File**, and select a pattern-data file to be imported. Repeat for additional pattern-data files.
  4. Click **Import** to import the selected files.

     A summary report is displayed with a list of patterns that were imported, patterns that were renamed to naming conflicts, and patterns that were skipped because they already exist.

Working with server profiles

A *server profile* is an instance of a server pattern that is applied to a specific server. Server profiles are generated and assigned automatically when a server pattern is deployed to one or more servers. One server profile is created for each target server. Each server profile contains the specific configuration for a single server and contains information (such as assigned name, IP addresses, and MAC addresses) that is unique for that specific server.

About this task

The server profile is activated during the baseboard-management-controller startup process. You can choose to:
- Reboot the server when the pattern is deployed to activate the server profile immediately
- Defer activation until the next reboot.
- Defer activation until you manually activate the server profile.

Multiple server profiles can inherit from a single server pattern. After a server pattern is deployed to one or more servers, you can quickly deploy configuration changes to multiple servers by editing the parent server pattern and category patterns. The dependant server profiles are automatically updated and redeployed to their associated servers. By editing the server pattern, you can control a common configuration from a single place.

If you replace an existing server or if you install a pre-provisioned server in an empty bay in a chassis, you must activate the server profile for that new server to provision the configuration changes on the new server.

Note: You can deploy a server pattern to multiple servers; however, multiple patterns cannot be deployed to a single server.

You can change the server profile that is associated with a server in several ways, depending on the reason for the change.

- If you want to move or repurpose a server:
  1. Deactivate the current server profile on the current server (see Deactivating a server profile).
  2. Deploy the new server pattern to the new server (see Deploying a server pattern to a server).
- If a server failed and you want to use a spare server in its place:
  1. Deactivate the current server profile on the failed server (see Deactivating a server profile).
  2. Activate the same server profile on the spare server (see Activating a server profile).
  3. When the failed server is fixed, you can repeat these steps to switch the profile again.
- If a server failed and you want to replace the hardware:
  1. Deactivate the current server profile on the failed server (see Deactivating a server profile).
  2. Replace the failed server.
  3. Activate the same server profile on the new server (see Activating a server profile).

Important:

- When using address virtualization, a server retains its assigned virtual MAC or WWN address until it is powered down. When deactivating a profile that has address virtualization enabled, the **Power off the server** checkbox is selected by default. Ensure that the original server is powered off before you activate the inactive profile on a different server to avoid address conflicts.
- If you delete a profile that is not the most recently created, the virtual MAC and WWN addresses *are not* released from the address pool. For more information, see Deleting a server profile.
- The settings on a server can become out of compliance with its server profile if settings are changed without using Configuration Patterns or if an issue occurred during deployment, such a firmware issue or an invalid setting. You can determine the compliance status of each server from the Configuration Patterns: Server Profiles page.

Activating a server profile

You can activate a server profile on a replaced, reassigned, or newly installed and managed server.

About this task

If you replace an existing server or if you install a pre-provisioned server in an empty bay in a chassis, you must activate the server profile for that new server to provision the configuration changes on the new server.

Important:

- When using address virtualization, a server retains its assigned virtual MAC or WWN address until it is powered down. When deactivating a profile that has address virtualization enabled, the **Power off the server** checkbox is selected by default. Ensure that the original server is powered off before you activate the inactive profile on a different server to avoid address conflicts.
- If you delete a profile that is not the most recently created, the virtual MAC and WWN addresses *are not* released from the address pool. For more information, see Deleting a server profile.

- The settings on a server can become out of compliance with its server profile if settings are changed without using Configuration Patterns or if an issue occurred during deployment, such a firmware issue or an invalid setting. You can determine the compliance status of each server from the Configuration Patterns: Server Profiles page.

Procedure

To activate a server profile, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Profiles**. The Configuration Patterns: Server Profiles page is displayed.

Step 2. Select the server profile to activate.

Tips: The current state of the server profiles is listed in the **Profile Status** column. You can activate server profile that is in the Inactive or Pending activate state.

Step 3. Click the **Activate server profile** icon ( ).

Step 4. Click **Activate**.

If the profile is in the pending, active, or active failed state, you can choose when to activate the deployment:

- **Full**. Immediately powers on or restarts the server to activate server, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) configurations.
- **Partial**. (default) Immediately activates management-controller configurations, but defers the activation of server and UEFI configurations until the next server restart. The server must be manually powered on or restarted before the profile is fully activated.

  Note: When deploying server patterns that included only IMM settings (including system information, management interface, and extended BMC category patterns), the server does not need to be restarted.

When the server profile is first activated, the profile status changes to “Active.” After compliance is verified, the status changes to “Compliance” or “Non-Compliant.”

Results

The state of the server profile on the Configuration Pattern: Server Profiles page changes to Active.



Deactivating a server profile

You can remove a server profile from a server or chassis bay by deactivating the profile.

Procedure

To deactivate a server profile, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Profiles**. The Configuration Patterns: Server Profiles page is displayed.

Step 2. Select the server profile to deactivate.

Tip: The current state of the server profile is listed in the **Profile Status** column.

Step 3. Click the **Deactivate server profile** icon ().

Step 4. Choose one of the following deactivation options:

- **Reset IMM Identity Settings**. Resets the profile-configured identity settings (including the baseboard-management-controller hostname, device name, or management interface assigned static IP addresses). Only the settings that are configured through the associated server pattern are reset.

  Note: For servers with statically assigned IP addresses, this option enables DHCP mode. If there is not a DHCP server enabled on the network, the server must be manually reconfigured with a valid static IP address. Converged, NeXtScale, and System x rack and tower servers must then be remanaged using XClarity Administrator.
- **Power off the server**. Powers off the server. When the server is powered back on, virtual address assignments revert to the burned-in defaults.
- **Force deactivation**. Deactivates the server profile even if the server has been removed or is not reachable.
- **Reset switch internal port settings**. Resets the profile-configured switch internal port settings to default values, including disabling UFP mode and removing associated member vports from VLAN definitions. Only the settings that are configured through the associated server pattern are reset.

  Choose this option to leave the switch ports in a state where the server profile can then be deployed to another server without settings that would conflict with the previous switch port configuration.

Step 5. Click **Deactivate**.

Results

The state of the server profile on the Configuration Pattern: Server Profiles page changes to Inactive.



Note: If XClarity Administrator cannot communication with the management controller (for example if the management controller is in an error state or is restarting), deactivation of the server profile fails and the server profile is not deactivated. If this occurs, reattempt the deactivation, and select the force deactivation option to deactivate the profile. The previously assigned server is still configured with the profile assigned identity and address assignments. The server must be manually powered down and removed from the infrastructure to avoid address conflicts.

Deleting a server profile

You can delete only server profiles that have been deactivated.

Before you begin

Ensure that the server profiles to be deleted are deactivated (see Deactivating a server profile).

Procedure

To delete a server profile, complete the following steps

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Profiles**. The Configuration Patterns: Server Profiles page is displayed.

Step 2. Select the server profile that is in the Deactivated state.

Tip: The current state of the server profile is listed in the **Profile Status** column.

Step 3. Click the **Delete** icon ( ).

Note: When you delete the most recently created profile, any virtual MAC or WWN address is released from the address pool. If you delete a profile that is not the most recently created, the virtual MAC and WWN addresses *are not* released from the address pool.

Working with placeholder chassis

You can pre-provision servers that will be installed in a Flex System chassis at a later time by defining a *placeholder chassis* to act as a target for the server pattern until the physical hardware arrives.

About this task

When you deploy a server pattern to a placeholder chassis, Lenovo XClarity Administrator creates a server profile for all 14 server bays in the Flex System chassis and reserves the management IP addresses and virtual Ethernet or Fibre Channel addresses for the servers.

The placeholder chassis bundles all of the server profiles, so that when the hardware arrives, you can deploy the placeholder chassis to activate the server profiles on the physical servers instead of deploying all 14 server profiles individually. Each server must be rebooted to fully activate the server profile.

Creating a placeholder chassis

You can create a placeholder chassis that can be pre-provisioned before the hardware is installed. Provisioning compute nodes in the chassis reserves management IP addresses and virtual Ethernet or Fibre Channel addresses.

Procedure

Complete the following steps to create a placeholder chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Placeholder Chassis** tab.

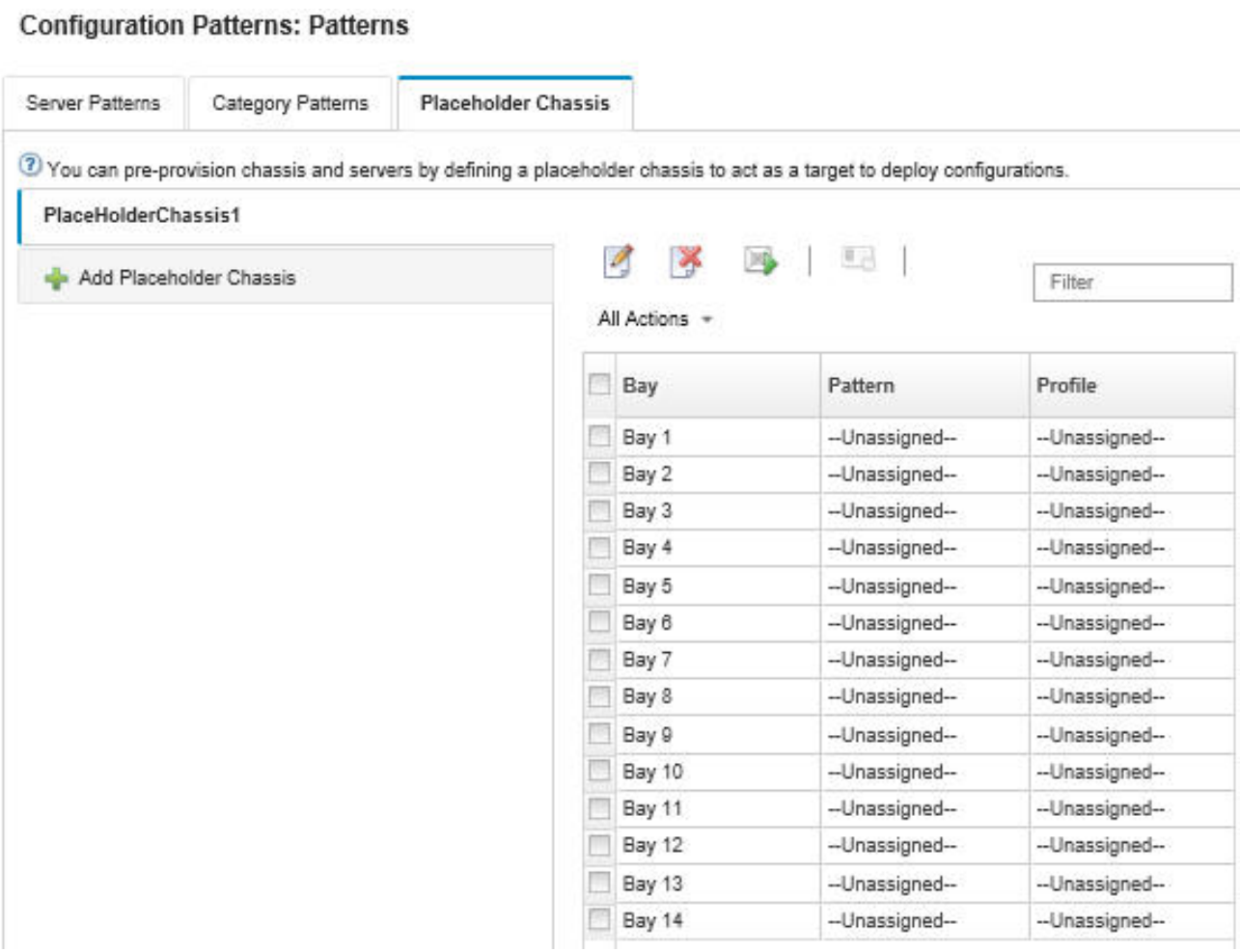
Step 3. Click the **Add Placeholder Chassis** vertical tab.

Step 4. Enter a name and description for the placeholder chassis.

Step 5. Click **Add**.

What to do next

A vertical tab is added for the new placeholder chassis on the Configuration Patterns: Placeholder Chassis page.



From this page, you can perform the following actions on a selected placeholder chassis:

- Deploy the placeholder chassis by clicking the **Deploy** icon ( ).
- Modify the placeholder chassis name and description by clicking the **Edit** icon ( ).
- Deploy a server pattern to the placeholder chassis (see Deploying a server pattern to a placeholder chassis).
- Deactivate the server profile from a placeholder chassis (see Deactivating a server profile).
- Delete the placeholder chassis by clicking the **Delete** icon ( ).

Deploying a server pattern to a placeholder chassis

You can deploy a server pattern to each bay in a placeholder chassis. Deploying a server pattern before the servers are installed in the Flex System chassis creates a server profile for each server bay in the chassis and reserves management IP addresses and virtual Ethernet or Fibre Channel addresses.

Procedure

Complete the following steps to deploy a server pattern to a placeholder chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

Step 3. Select the server pattern that you want to deploy to the placeholder chassis.

Step 4. Click the **Deploy** icon (). The Deploy Server Pattern dialog is displayed with a list of available chassis and placeholder chassis.

Step 5. Select **Deferred** from the **Activation** list.

Step 6. Click **Show Empty Bays**.

Step 7. Choose one or more placeholder chassis bays to which you want to deploy the server pattern.

Step 8. Click **Deploy**. A dialog is displayed that lists the deployment status of each selected bay.

Step 9. Click **Deploy** again to start the deployment process.

A server profile is created and assigned for each selected bay in the placeholder chassis.

Note: Deployment can take several minutes to complete

Step 10. Click **Close**.

What to do next

You can monitor the deployment progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar. You can also monitor the server-profile creation by clicking **Provisioning → Server Profiles**. After the deployment is complete, review the generated server profiles, and record the management IP address and any virtualized Ethernet or Fibre-Channel addresses.

After the Flex System chassis is physically installed in the rack and then discovered and managed by XClarity Administrator, you can deploy the placeholder chassis to provision all servers in the chassis (see Deploying a server pattern to a placeholder chassis).

Deploying a placeholder chassis

After you pre-configure a placeholder chassis by deploying a server pattern to that placeholder chassis, and then discover and manage the actual chassis, you can deploy the placeholder chassis to configure the actual compute nodes.

Procedure

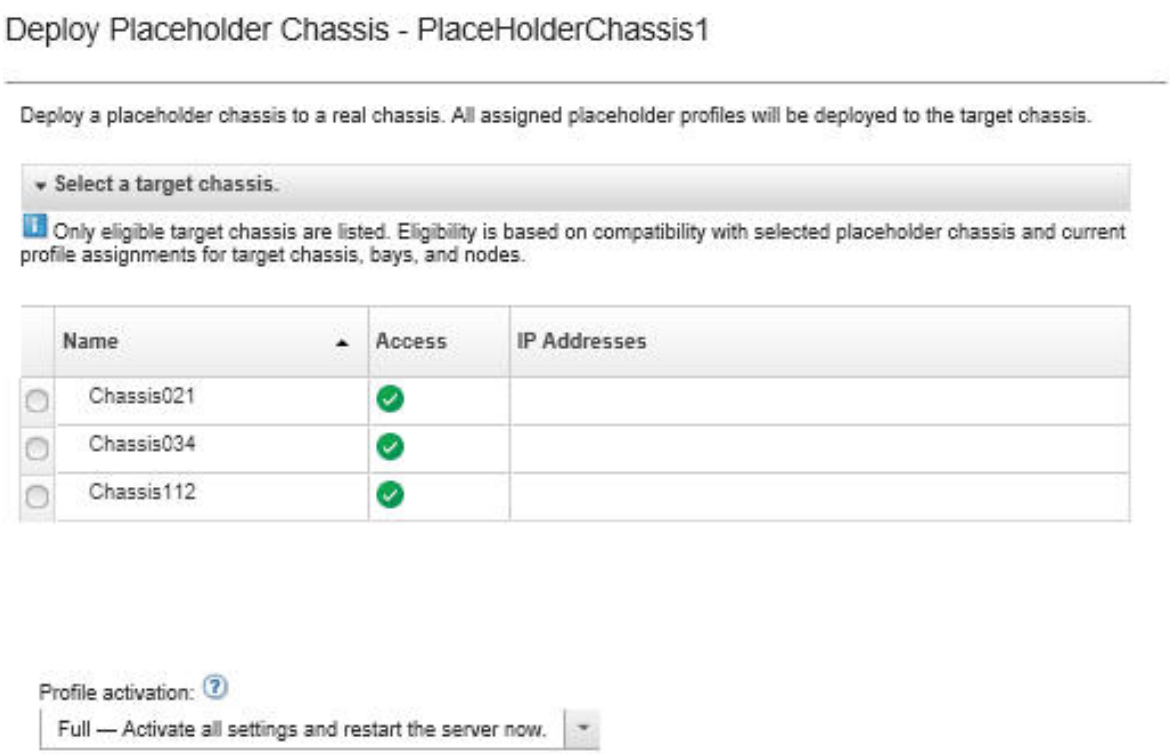
Complete the following steps to deploy a placeholder chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Placeholder Chassis** tab.

Step 3. Select the vertical tab for the placeholder chassis that you want to deploy.

Step 4. Click the **Deploy placeholder chassis** icon () to display the Deploy Placeholder Chassis dialog.



Step 5. Choose when to activate the configurations:

Note: The network settings on the relative switch internal ports are pushed to the switch immediately after the deployment, regardless of activation configuration.

- **Full**. Immediately powers on or restarts the server to activate server, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) configurations.
- **Partial**. (default) Immediately activates management-controller configurations, but defers the activation of server and UEFI configurations until the next server restart. The server must be manually powered on or restarted before the profile is fully activated.

  Note: When deploying server patterns that included only IMM settings (including system information, management interface, and extended BMC category patterns), the server does not need to be restarted.

Step 6. Click **Activate**.

Resetting storage adapters to default values

You can reset the local storage adapters to their default manufacturing settings for one or more servers.

About this task

Attention: This action clears all data on the local storage adapters.

If the server is powered off and RAID link is supported, the server is booted to system setup to reset local HDD and SSD adapters.

Procedure

Complete these steps to clear the RAID configuration for one or more servers.

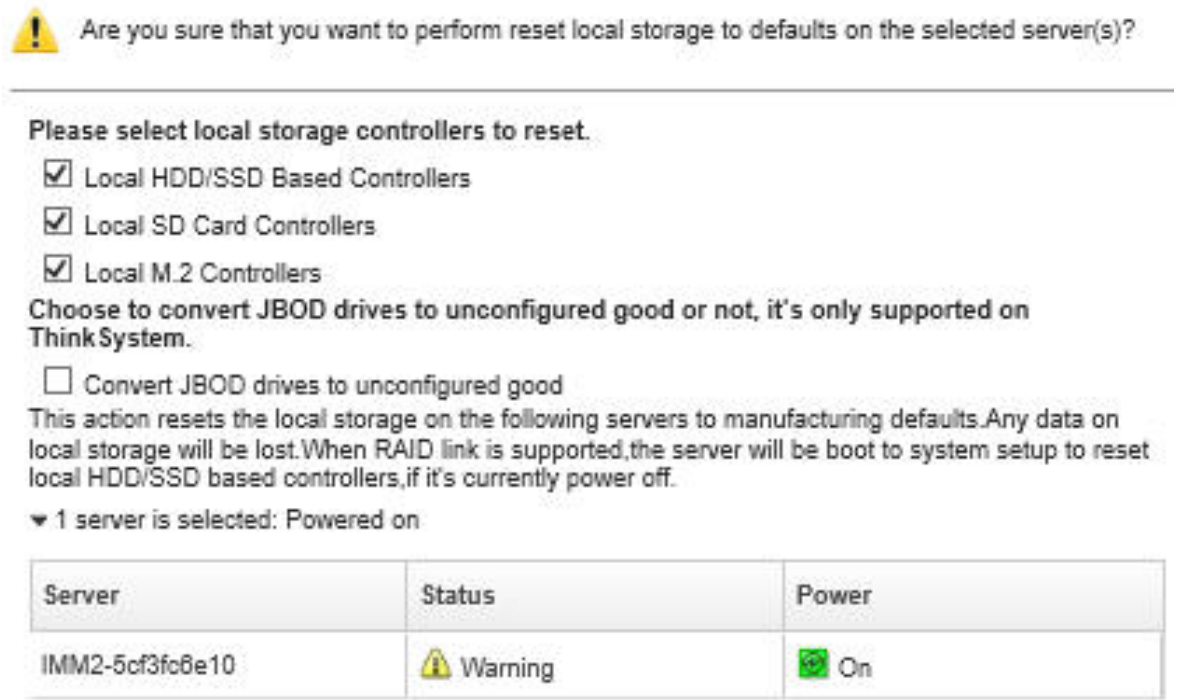
Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find the server that you want to manage. In addition, you can select a server type from the **All Systems** drop down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.



Step 2. Select one or more servers

Step 3. Select **All Actions → Service → Reset Local Storage to Defaults**. A dialog is displayed that asks for additional information.



Step 4. Select the local storage adapters to reset.

Step 5. Optional: : (ThinkSystem servers only) Chose to convert JBOD drives to unconfigured good.

Step 6. Click **Reset Storage**.

Configuring memory

You can encrypt and decrypt persistent memory for Intel® Optane™ DC Persistent Memory DIMMs.

Procedure

Complete the following procedure to encrypt and decrypt persistent memory.

Step 1. From the XClarity Administrator menu, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

Step 2. Select one or more servers that you want to configure.

Step 3. Click **All Actions → Security → Intel Optane PMEM Operation** to display the Intel Optane PMEM Operation dialog.

Step 4. Select the security operation that you want to perform.

- **Enable security**. Data that is written to the persistent memory region is encrypted using the specified passphrase.

  Important: Record the encryption passphrase. The passphrase is required to authorize disabling security or erasing the encryption passphrase.

- **Disable security**. Data that is written to the persistent memory region is not encrypted.

  Data that is already stored in the persistent memory region remains encrypted and is still accessible.

  Note: This action is available only when security is enabled, and the passphrase set. You must authorize this operation using the current passphrase. You can disable security for multiple DIMMs in the device only if all DIMMs share the same passphrase.

- **Secure erase**. Erases the encryption passphrase that is used to encrypt the data that is stored in the persistent memory region to ensure that data is unrecoverable.

  Note: This action is available only when security is enabled, and the passphrase set. You must authorize this operation using the current passphrase.

- **Secure erase without passphrase**. Securely erases all the data that is stored in the persistent memory of the specified DIMMs in the device. After the secure erase, all data is unrecoverable.

  Note: This action is available only when security is disabled and passphrase is not required.

Step 5. If required, specify and confirm the passphrase.

Step 6. Click **OK**.

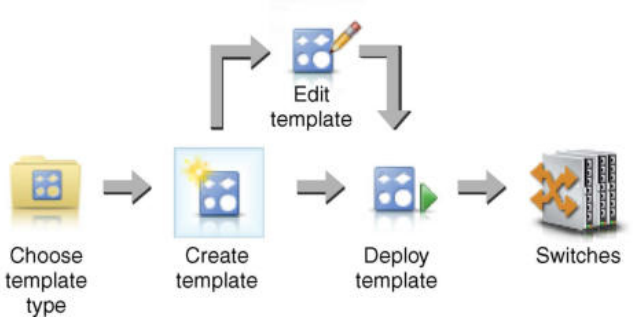
Chapter 12. Configuring switches using configuration templates

You can use templates to quickly provision multiple CNOS rack switches from a single set of defined configuration settings.

About this task

You can use switch-configuration templates in XClarity Administrator to configure global settings, port channels, virtual LANs, Virtual link aggregation groups, and spine-leaf topologies on managed switches. Currently, only rack switches running CNOS are supported.

The following figure illustrates the workflow for configuring managed rack switches.



1. **Choose a template type.**

   A *switch-configuration template* groups together related switch settings. You can create the following types of switch-configuration templates.
   - **Global**. Configures global settings, including system propriety, native VLAN tags, and L2 interfaces.
   - **Port channel**. Configures basic and advanced port-channel settings, and removes ports from and deletes a port channel.
   - **Spine-leaf**. Deploys a spine-leaf configuration to an existing topology.
   - **Virtual LAN (VLAN)**. Configures VLAN settings and properties, and deletes a V LAN.
   - **Virtual link aggregation group (VLAG)**. Configures basic, advanced, and peer VLAG settings, and creates and deletes a VLAG instance.
2. **Create a template.**

   You can create multiple switch-configuration templates to represent different configurations that are used in your data center. You use switch-configuration templates to control a common switch configuration from a single place.

   For more information about creating switch configuration templates, see Creating a switch-configuration template.
3. **Deploy the template to one or more switches.**

   You can deploy a server pattern to one or more individual rack switches running CNOS.

   For more information about deploying a switch configuration, see Deploying switch-configuration templates to a target switch.
4. **Edit a template.**

© Copyright Lenovo 2015, 2021

Editing a switch-configuration template does not automatically deploy the updated settings to all switches to which the initial template was deployed. You must manually redeploy changed templates. The history page keeps track of the settings for each deployment.

Setting default server-configuration preferences

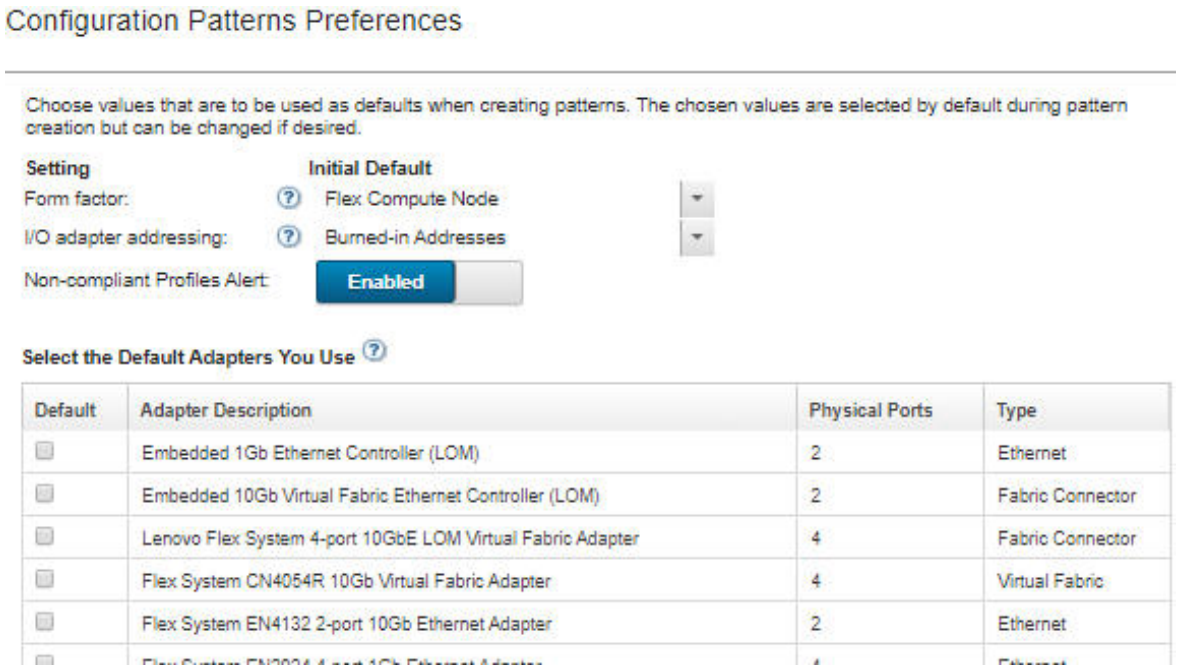
You can define values to be selected by default when creating server configuration patterns. The values can be changed during server pattern creation.

Procedure

To set default server-configuration settings, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning**, and then click the help icon ( ) after **Configuration Patterns** to display the Configuration Patterns: Getting Started page.

Step 2. Click **Set Configuration Pattern Preference** to display the Configuration Pattern Preference dialog.



Step 3. Select the default server form factor.

Step 4. Select the default I/O adapter addressing mode.

- **Burned in**. Use existing World Wide Name (WWN) and Media Access Control (MAC) addresses that are provided with the adapter from manufacturing.
- **Virtual**. Use virtual I/O adapter addressing to simplify the management of LAN and SAN connections. Virtualizing I/O-addresses reassigns the burned-in hardware addresses with virtualized Fibre WWN and Ethernet MAC addresses. This can speed deployment by pre-configuring SAN zone membership and facilitate failover by eliminating the need to reconfigure SAN-zoning and LUN-masking assignments when replacing hardware.

  When virtual addressing is enabled, both Ethernet and Fibre Channel addresses are allocated by default regardless of defined adapters. You can choose the pool from which Ethernet and Fibre Channel addresses are allocated.

  You can also edit virtual-address settings by clicking the **Edit** icon ( ) next to the address modes.

Restriction: Virtual addressing is supported for only servers in Flex System chassis. Rack and tower servers are not supported.

Step 5. Choose whether to enable or disable raising an alert when a server's configuration settings do not match the assigned server-configuration profile

Alerts are raised only for non-compliance with an active profile (in the ASSIGNED or ERROR_ ACTIVATING state).

When the server's configuration becomes compliant or if the server profile is unassigned, the non-compliant profile alert is deleted.

Step 6. Select one or more default I/O adapters that you want to use as preferred adapters in the selection lists.

Step 7. Click **Save**.

Creating a switch-configuration template

When you create a switch-configuration template, you define the settings for a specific type of configuration.

Before you begin

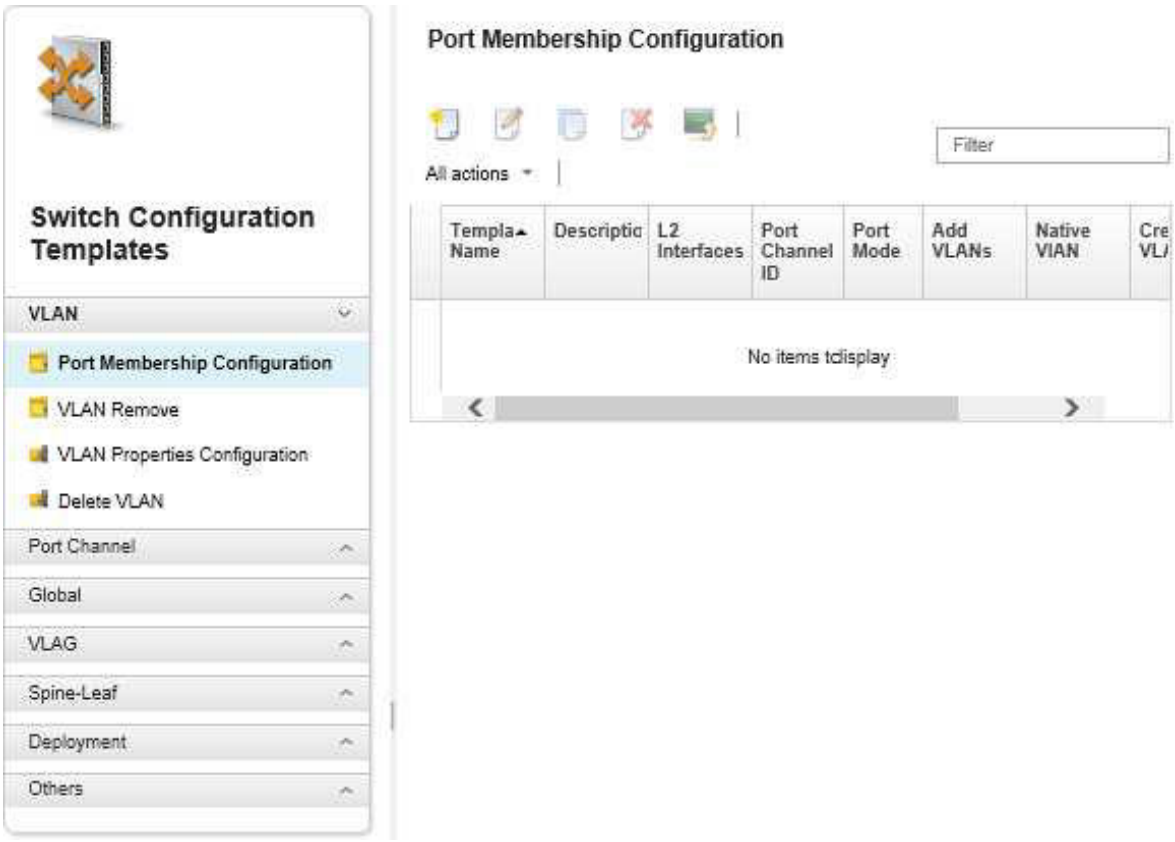
Before you create a switch-configuration template, consider the following suggestions:

- Identify groups of switches that have the same hardware options and that you want to configure the same way. You can use a switch-configuration template to apply the same configuration settings to multiple switches, thereby controlling a common configuration from one place.
- Identify the aspects of configuration that you want to customize (for example, global, port-channel, or VLAN settings).

Procedure

Complete the following steps to create a switch-configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.



Step 2. Select the type of template that you want to create from the left navigation.

Step 3. Click the **Create** icon ( ) to display the Create New Template dialog.

The fields that are listed on this dialog vary depending on the type of template.

Step 4. Click **Save** to save the template, or click **Save and Deploy** to save and immediately deploy the template to one or more managed rack switches

For information about deploying a template, see Deploying switch-configuration templates to a target switch .

What to do next

If you clicked **Save and Deploy**, the Deploy Switch Template page is displayed. From this page, you can deploy the switch-configuration template to specific switches.

If you clicked **Save**, the switch-configuration template is saved to the Switch Configuration Templates page. From this page, you can perform the following actions on selected server patterns:

- View details about the template by clicking the template name in the Name column.
- View an aggregated list of all templates, click **Others → All templates**.
- Deploy the template (see Deploying switch-configuration templates to a target switch).
- Copy and then modify a template by clicking the **Copy** icon ( ).
- Edit the template by clicking the **Edit** icon ( ).

Note: Changes to the template are *not automatically* redeployed to switches on which the original template was deployed.

- Rename the pattern by clicking the **Rename** icon ().
- Delete the pattern by clicking the **Delete** icon ().

Defining VLAN port-membership settings

You can add physical ports and port channels to one or more (for trunk) VLANs using the VLAN Port Membership Configuration template.

Procedure

Complete the following steps to create a Port Membership Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAN → Port Membership Configuration** in the left navigation, and then click the **Create** icon ().

Step 3. In the Create New Template dialog, specify the following information.

Important: You must specify one or more physical L2 interfaces or port channel IDs.

- Enter a name and description for the template.
- Specify one or more valid physical L2 interfaces. You can specify a list of interfaces separated by a comma, a range of IDs separated by a dash, or a combination of both, for example:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Specify one or more valid port channel IDs (port aggregator interfaces). You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- Choose whether the port accepts tagged or untagged traffic. This can be one of the following values.
  - **access**. The port carries traffic for a single VLAN.
  - **trunk**. (default) The port carries traffic for all VLANs that are accessible by the switch.
- Specify one or more VLAN IDs to add to the port's VLAN membership list. You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Notes:

- If the port mode is set to “access,” only the first VLAN ID is used. For example, in the range `2-4,5,10-20`, only `2` is used.
- CNOS reserves VLAN IDs 4000-4095 by default. Using reserved VLAN IDs (either by CNOS or another user) might cause the switch-configuration deployment to fail.

- Specify a native VLAN ID with which untagged traffic is tagged. This can be a number from 1-4096.

  Notes:
  – This field is valid only when the port mode is set to “trunk.”
  – If it is not specified, or if the ID is outside the end-state VLANs on a port, the port will effectively not allow untagged traffic.
- Select **Create VLANs** to create VLAN IDs that are currently missing on the target switch.

  If a port belongs in a VLAN that is not created, the port continues to be a member of that VLAN, but any traffic that is tagged with that VLAN ID and reaches the port is not allowed to pass.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining VLAN properties

You can configure advanced VLAN properties using the VLAN Properties Configuration template.

Procedure

Complete the following steps to create a VLAN Properties Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAN → VLAN Properties Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify a VLAN ID on which to apply the changes. This can be a number from 1-4095.

  Note: CNOS reserves VLAN IDs 4000-4095 by default. Using reserved VLAN IDs (either by CNOS or another user) might cause the switch-configuration deployment to fail.
- Specify a custom name for the VLAN.
- Choose whether the VLAN is active (enabled) or suspended (disabled).
- Choose whether IP multicast (IPMC) flood on the target VLAN is controlled (enabled) on IPv4 or IPv6 interfaces. This can be one of the following values.
  – **Disable**. IPv4 and IPv6 are disabled.
  – **Enable**. IPv4 and IPv6 are enabled.
  – **IPv4 Disable**.
  – **IPv4 Enable**
  – **IPv6 Disable**
  – **IPv6 Enable**

  This action is additive, meaning that “IPv4 Enable” deployed on top of “Disable” results in “IPv4 Enable,” but deploy on top of “IPv6 Enable” results in ""Enable.” The reverse is true for the disable options.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Removing VLAN settings

You can remove interfaces from VLANs using the VLAN Remove template.

Procedure

Complete the following steps to create a VLAN Remove template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAN → VLAN Remove** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

Important: You must specify one or more physical L2 interfaces or port channel IDs.

- Enter a name and description for the template.
- Specify one or more valid physical L2 interfaces. You can specify a list of interfaces separated by a comma, a range of IDs separated by a dash, or a combination of both, for example:
  - Ethernet1/10
  - Ethernet1/1,3,5,7
  - Ethernet1/1-10,21-30
  - Ethernet2/1-5,7,9,11-13
- Specify one or more valid port channel IDs (port aggregator interfaces). You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13
- Specify one or more VLAN IDs to remove from the port's VLAN membership list. You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13

Note: If the port mode is set to “access,” removing the VLAN causes the port to go in VLAN 1.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Deleting VLANs

You can remove VLAN configurations from the switch using the Delete VLAN template.

Procedure

Complete the following steps to create a Delete VLAN template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAN → Delete VLAN** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify one ore more VLAN IDs to remove from the port's VLAN membership list. You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  – 10
  – 3,5,7,9
  – 5-10,21-32
  – 2-5,7,9,11-13

  Note: You cannot delete reserved VLAN IDs.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining port-channel basic settings

You can create port aggregators and add ports to the aggregators using a port-channel Basic Configuration template.

If the port channel has ports in it, and some of those ports are part of the template, their properties (port priority, mode, and timeout) are updated with the template's settings when the template is deployed.

Procedure

Complete the following steps to create a port-channel Basic Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Port Channel → Basic Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify one or more valid physical L2 interfaces. You can specify a list of interfaces separated by a comma, a range of IDs separated by a dash, or a combination of both, for example:
  – Ethernet1/10
  – Ethernet1/3,5,7,9
  – Ethernet1/5-10,21-32
  – Ethernet2/2-5,7,9,11-13
- Specify the port channel ID (port aggregator interface) to create or update. This can be a number from 1-4095.
- Specify the Link Aggregation Control Protocol (LACP) port mode. This can be one of the following values.
  – **Active**. (default) Enables LACP unconditionally
  – **Passive**. Enables LACP only when an LCAP device is detected.
  – **Static**. Disables LCAP.

Note: Active and Passive can be mixed in the same aggregator, but Static cannot.

- Specify the LACP port priority. This can be a number from 1 - 65535.

  Note: The LACP port priority is used with the port number to form the LACP Port ID.
- Specify the LACP timeout mode before LCAP goes into individual mode. This can be one of the following values.
  - **Long**. (default) 90 seconds
  - **Short**. 3 seconds

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining port-channel advanced settings

You can configure advanced port-channel properties using the port-channel Advanced Configuration template.

Procedure

Complete the following steps to create a port-channel Advanced Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Port Channel → Advanced Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify a port channel ID (port aggregator interface) to update. This can be a number from 1-4095.
- Choose whether individual ports remain active when LACP fails. This can be one of the following values.
  - **Active**. (default) Enables LACP unconditionally.
  - **Suspend**. Disables LACP .
- Specify the minimum number of links that must be up for the port channel to be considered up. This can be a number from 1 – 32.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Deleting port channels

You can remove port channels from the switch using the Delete Port Channel template.

Procedure

Complete the following steps to create a Delete Port Channel template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Port Channel → Delete Port Channel** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify one ore more port channel IDs (port aggregator interfaces) to delete. You can specify a list of numbers separated by a comma, a range of numbers separated by a comma, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining general switch settings

You can configure general switch properties using the global Generic Configuration template.

Procedure

Complete the following steps to create a switch global Generic Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Global → Generic Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the LACP system priority that is used to generate the LACP system ID. This can be a number from 1 – 65535.
- Choose where to enable native VLAN tagging. This can be one of the following values.
  - **Ingress and Egress**
  - **Egress only**

  Note: This property is supported by CNOS 10.10.1 and later.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining global L2 interface settings

You can configure VLAN tagging properties on L2 Interfaces using the L2 Interface Configuration template.

Procedure

Complete the following steps to create an L2 Interface Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Global → L2 Interface Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify one or more valid physical L2 interfaces. You can specify a list of interfaces separated by a comma, a range of IDs separated by a dash, or a combination of both, for example:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Choose where to enable native VLAN tagging. This can be one of the following values.
  - **Ingress and Egress**
  - **Egress only**

  Note: This property is supported by CNOS 10.10.1 and later.
- Choose whether to enable or disable tunnelling (QinQ) support.

  Note: This property is supported by CNOS 10.10.1 and later.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining peer VLAG settings

You can configure a VLAG peers using the VLAG Peers Configuration template.

Procedure

Complete the following steps to create a VLAG Peers Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAG → Peers Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Choose whether to enable or disable the VLAG.
- For Peer 1 and Peer 2, complete the following fields. Fields for both peers must be populated.
  - Specify the IIPv4 or IPv6 address of the VLAG peer to use for health check.
  - Specify the ID of the port channel that is used between the two peers. This can be a number from 1 – 4095.
  - Specify the VRF that is used for health check (for example, management, default, or customVRF).

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining VLAG instance settings

You can create or update a VLAG instance using the VLAG Instance Configuration template. A VLAG instance is a device that is connected to both switches (usually through a port aggregation) to which the VLAG appears as a single device.

Procedure

Complete the following steps to create a VLAG Instance Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAG → Instance Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the VLAG ID. This can be a number from 1 – 64.
- Specify the ID of the port-channel that is connected to the Peer 1 and Peer 2. This can be a number from 1 – 4095.
- Choose whether to enable or disable the VLAG instance.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining VLAG advanced settings

You can configure advanced VLAG properties using the VLAG Advanced Configuration template.

Procedure

Complete the following steps to create a VLAG Advanced Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAG → Advanced Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the priority that is used to control which peer is primary. This can be a number from 1 – 65535.

  If not specified, the switch's default priority is used. For CNOS, the default is 0.
- Specify the grace period, in seconds, for the VLAG to come online after a simultaneous reboot. This can be a number from 240 – 3600.

  If not specified, the switch's default is used. For CNOS, the default is 300.
- Specify the tier ID that is used to differentiate VLAG setups in the same network. This can be a number from 1 – 512.
- Specify the vLAG startup delay interval, in seconds, that is used to delay bringing up ports after a peer reloads. This can be a number from 0 – 3600.

  If not specified, the switch's default is used. For CNOS, the default is 120.

- Specify the number of VLAG keep-alive attempts (unanswered hello messages) before the VLAG fails. This can be a number from 1 – 24.

  If not specified, the switch's default is used. For CNOS, the default is 3.
- Specify the interval, in seconds, between VLAG keep-alive attempts. This can be a number from 2 – 300.

  If not specified, the switch's default is used. For CNOS, the default is 5.
- Specify the interval, in seconds, between VLAG keep-alive retry attempts. This can be a number from 1 – 300.

  If not specified, the switch's default is used. For CNOS, the default is 30.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Deleting a VLAG instance

You can delete a VLAG instance using the VLAG Instance Delete template.

Procedure

Complete the following steps to create a VLAG Instance Delete template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAG → Instance Delete** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the unique ID of the VLAG instance. This can be a number from 1 – 64.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining a spine-leaf topology

You can verify the physical topology and deploy a SpineLeaf (L3 fabric) setup on managed switches using the spine-leaf Topology Wizard template.

Procedure

Complete the following steps to create a spine-leaf Topology Wizard template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Spine-Leaf → Topology Wizard** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.

- Specify the autonomous system (AS) number for the Border Gateway Protocol (BGP) protocol that is running on the switch. This can be a number from 1 – 4294967295.

  Note: This is supported by CNOS 10.9.3 and later.
- Choose whether to allow single links between switches.

  Typically, deployment fails if there are not at least two links between any spine and leaf switch.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Deploying switch-configuration templates to a target switch

You can define VLAN port settings by creating a VLAN port-configuration template.

About this task

There are three types of deployments:

- **Normal**. Deploys switch-configuration settings to one or more rack switches in a basic layered architecture.
- **VLAG**. Deploys switch-configuration settings to exactly two switches that support a virtual link aggregation group (VLAG) architecture. The switches must be of the same model and software version.
- **Spine-Leaf**. Deployment templates to one or more spine switches and leaf switches.

Procedure

To deploy a switch-configuration template to one or more managed switches, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Select one or more switch-configuration templates that you want to deploy.

Step 3. Click the **Deploy** icon ( ) to display the Deploy Template dialog.

Step 4. Select one or more switches to which you want to deploy the templates.

Only switches that are compatible with the selected templates are listed.

Step 5. Click **Deploy**. A dialog is displayed that lists the deployment status of each selected switch.

Step 6. Click **Deploy** again to start the deployment process.

Note: Deployment might take several minutes to complete.

What to do next

You can view the deployment history (see Viewing switch-configuration deployment history).

Viewing switch-configuration deployment history

You can view information about switch-configuration templates that have been deployed to managed switches, including the template name, template type, timestamp, and the switches to which they were deployed. Each deployment contains a snapshot of the template as it was when it was deployed.

Procedure

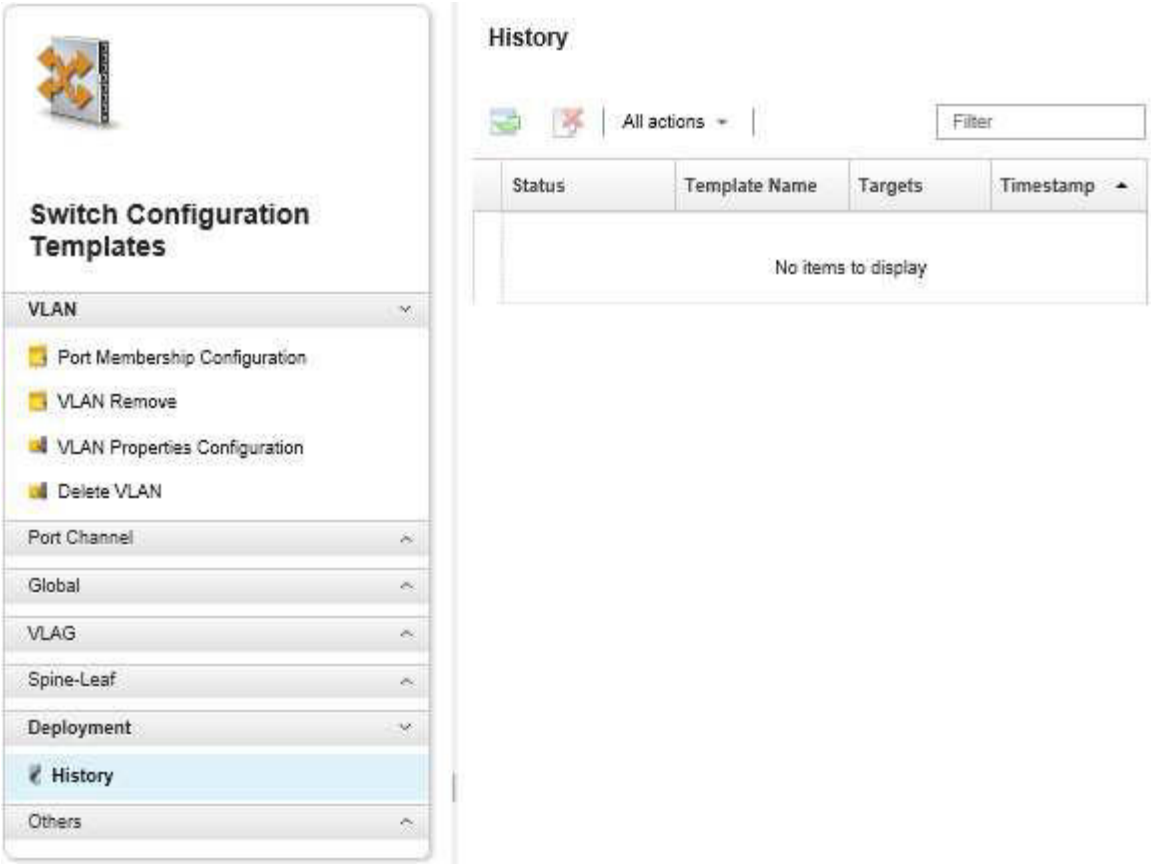
Complete the following steps to view switch-configuration deployment history.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Expand **Deployment**, and click **History** in the left navigation to display a table of deployed templates.

The **Status** column indicates whether the configuration deployment was successful. It can be one of the following states:

- **Succeeded**. Configuration deployment to all target switches completed successfully.
- **Warning**. Configuration deployment to one or more target switches completed with warnings.
- **Failed**. Configuration deployment to one or more target switches failed.



What to do next

- View the information about each deployed template, including what was deployed and what succeeded or failed, by clicking the template name in the table.
- Clear the deployment history by selecting a deployment and clicking the **Delete** icon ( ).

Chapter 13. Updating firmware and Windows device drivers

You can use Lenovo XClarity Administrator to update firmware and Windows device drivers on supported devices.

Updating firmware and updating device drivers are separate processes; there is no connection between these processes. XClarity Administrator does not maintain compliance between firmware and devices drivers on managed devices, even though it is recommended that you update device drivers at the same time as the firmware.

XClarity Administrator provides the following support for managed devices.

- Download and install repository packs, which are collections of the latest firmware that is available at the same time as the XClarity Administrator release
- Download and install any version of Update Express System Packs (UXSPs)
- Download and install the latest available individual firmware-update packages

Notes:

- When you import UXSPs from the Firmware Updates Repository page, only firmware updates are downloaded and stored in the repository. Device drivers are discarded.
- When you import UXSPs from the Windows Driver Updates Repository page, only device drivers are downloaded and stored in the repository. Firmware updates are discarded.
- XClarity Administrator does not support updating devices drivers in Linux or VMWare.

Updating firmware on managed devices

From the Lenovo XClarity Administrator web interface, you can download, install, and manage firmware updates for managed devices, including chassis, servers, storage systems, and switches. You can assign firmware-compliance policies to the managed devices to ensure that firmware on those devices remains compliant. You can also create and edit firmware-compliance policies when validated firmware levels do not match the suggested predefined policies.

Learn more:

- Lenovo ThinkSystem Firmware and Driver Update Best Practices
- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Firmware updates
- XClarity Administrator: Provisioning firmware security updates

About this task

Note: An operating system is not required to update firmware. For bare metal servers, ensure that the server is powered off before updating firmware.

You can manage and apply firmware updates to the following managed devices:

- **Chassis**. CMM updates
- **Converged, Flex System, NeXtScale, System x, ThinkAgile, and ThinkSystem servers**. Baseboard management controller, UEFI, DSA, mezzanine, and adapter updates
- **Lenovo Storage** and ThinkSystem DM storage **devices**
- **RackSwitch and Flex System switches**

Firmware for the following devices cannot be updated through XClarity Administrator:

© Copyright Lenovo 2015, 2021

- **ThinkServer servers**. See the documentation that was provided with the server to find information about how to update the firmware.
- **Flex Power Systems compute nodes**. Several methods are available to update firmware for Flex Power Systems compute nodes. For more information, see IBM Flex System p260/p460 Compute Nodes online documentation. The process for other Flex Power Systems compute nodes is similar.
- **Flex System v7000 Storage Node**. Use the Flex System v7000 Storage Node user interface to update the firmware. For more information, see FlexSystem v7000 Storage Node online documentation.
- **Flex switches that are in stacked mode or protected mode**. You *cannot* update firmware on stacked switches. Updating firmware is disabled for all switches that are stacked.
- **Flex switches**. If you are using the following switch, see the documentation that was provided with the switch to find information about how to update the firmware.
  - Cisco Nexus B22 Fabric Extender

For information about installing operating systems using XClarity Administrator (see Installing operating systems on bare-metal servers).

Procedure

The following figure illustrates the workflow for updating firmware on managed devices.



Step 1. **Manage the firmware-updates repository**

The *firmware-updates repository* contains a catalog of available updates and the update packages that can be applied to the managed devices.

The *catalog* contains information about firmware updates that are currently available for all devices that XClarity Administrator supports. The catalog organizes the firmware updates by device type. When you refresh the catalog, XClarity Administrator retrieves information about the latest available firmware updates from the Lenovo website and stores the information in the firmware-updates repository.

If new firmware updates are available, you must first download the update packages before you can update that firmware on the managed devices. Refreshing the catalog does not automatically download update packages. The Product Catalog table on the Firmware Updates Repository page identifies which update packages are downloaded and which are available for download.

You can download firmware updates in a few different ways:

- **Firmware-update repository packs**

  Firmware-update repository packs contains the latest available firmware updates at a specific point in time for all supported devices and a refreshed default firmware-compliance policy. These repository packs are imported and then applied from the Update Management Server page. When you apply a firmware-update repository pack, each update package in the pack is added to the firmware-updates repository, and a default firmware-compliance policy is automatically created for all manageable devices. You can copy this predefined policy, but you cannot change it.

  The following repository packs are available:

- **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all CMMs and Flex System switches.
- **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all RackSwitch switches and Lenovo Storage devices.
- **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all Converged HX Series, Flex System, NeXtScale, and System x servers.
- **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all ThinkAgile and ThinkSystem servers.
- **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all ThinkAgile and ThinkSystem V2 servers.

You can determine whether firmware-update repository packs are stored in the repository from the **Download Status** column on Update Management Server page. This column contains the following values:

- **Downloaded**. The firmware-update repository pack is stored in the repository.
- **Not Downloaded**. The firmware-update repository pack is available but not stored in the repository.

- **UpdateXpress System Packs (UXSPs)**

  UXSPs contains the latest available firmware and device driver updates, organized by operating system. When you download UXSPs, XClarity Administrator downloads the UXSP, based on the version that is listed in the catalog, and stores the update packages in the firmware-updates repository. When you download a UXSP, each firmware update in the UXSP is added to the firmware-updates repository and listed on the **Individual Updates** tab, and a default firmware-compliance policy is automatically created for all manageable devices using the name *<uxsp-version>-<date>-<server-short-name>*`-UXSP` (for example, `v1.50-2017-11-22- SD530-UXSP`). You can copy this predefined policy, but you cannot change it.

  Note: When you download UXSPs from the Firmware Updates: Repository page, only firmware updates are downloaded and stored in the repository. Device driver updates are excluded. For information about downloading Windows device driver updates using UXSPs, see Managing the OS device-drivers repository.

  You can determine whether UXSPs are stored in the firmware-updates repository from the **Download Status** column on the **Individual Updates** tab of the Firmware Updates: Repository page. This column contains the following values:

  - **Downloaded**. The entire update package or the individual firmware update is stored in the repository.
  - *x* **of** *y* **Downloaded**. Some but not all firmware updates in the update package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
  - **Not Downloaded**. The entire update package or the individual firmware update is available but not stored in the repository.

- **Individual firmware updates**

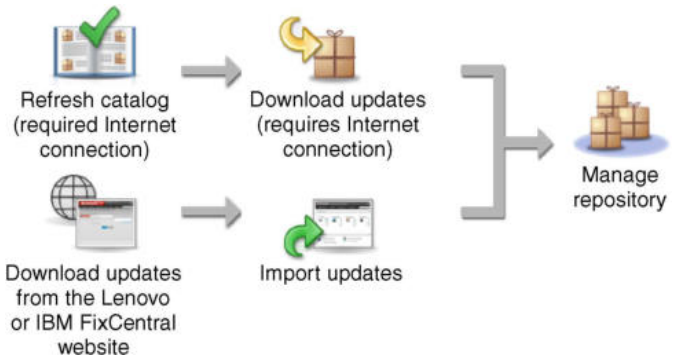
  You can download individual firmware-update packages, at one time. When you download firmware-update packages, XClarity Administrator downloads the update, based on the version that is listed in the catalog, and stores the update packages in the firmware-updates repository. You can then create firmware-compliance policies using those update packages for each of your managed devices.

Note: The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

You can determine whether specific *firmware updates* are stored in the firmware-updates repository from the **Download Status** column on the **Individual Updates** tab on the Firmware Updates: Repository page. This column contains the following values:

- **Downloaded**. The entire update package or the individual firmware update is stored in the repository.
- *x* **of** *y* **Downloaded**. Some but not all firmware updates in the update package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
- **Not Downloaded**. The entire update package or the individual firmware update is available but not stored in the repository.

XClarity Administrator must be connected to the Internet to refresh the catalog and download firmware-update. If it is not connected to the Internet, you can manually download the files to a workstation that has network access to the XClarity Administrator host using a web browser and then import the files into the firmware-updates repository.



When you manually import firmware updates into XClarity Administrator, you must include the following required files: payload (image and MIB), metadata XML, change history, and readme. For example:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Attention:

- Only import these required files. Do not import other files that might be found on the firmware download websites.
- If you do not include the XML file in the update package, the update is not imported.
- If you do not include all required files that are associated with the update, the repository shows that the update is not downloaded, which means that it is partially imported. You can then import the missing files by selecting and importing them.
- The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which

firmware-update packages to use for your managed servers, see Downloading firmware updates.

For more information about the firmware updates, see Managing the firmware-updates repository.

Step 2. **(Optional) Create and assigning firmware-compliance policies**

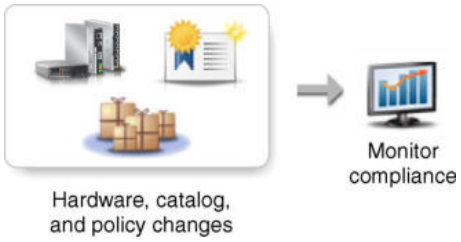
Firmware-compliance policies ensure that the firmware on certain devices is at the current or specific level by flagging the devices that need attention. Each firmware-compliance policy identifies which devices are monitored and which firmware level must be installed to keep the devices in compliance. You can set compliance at the device or firmware component level. XClarity Administrator then uses these policies to check the status of managed devices and to identify devices that are out of compliance.

When you create a firmware-compliance policy, you can choose to have XClarity Administrator flag a device when:

- The firmware on the device is down level
- The firmware on the device does not exactly match the compliance target version

XClarity Administrator comes with a predefined firmware-compliance policy named **Latest firmware in repository**. When new firmware is downloaded or imported into the repository and when XClarity Administrator is restarted, this policy is updated to include latest available versions of firmware in the repository.

After a firmware-compliance policy is assigned to a device, XClarity Administrator checks the compliance status of each device when the device inventory changes or firmware-updates repository changes. When the firmware on a device is not compliant with the assigned policy, XClarity Administrator identifies that device as not compliant on the Firmware Updates: Apply / Activate page, based on the rule that you specified in the firmware-compliance policy



For example, you can create a firmware-compliance policy that defines the baseline level for firmware that is installed in all ThinkSystem SR850 devices and then assign that firmware-compliance policy to all managed ThinkSystem SR850 devices. When the firmware-updates repository is refreshed and a new firmware update is added, those compute nodes might become out of compliance. When that happens, XClarity Administrator updates the Firmware Updates: Apply / Activate page to show that the devices are not compliant and generates an alert.

Note: You can choose to show or hide alerts for devices that do not meet the requirements of their assigned firmware-compliance policies (see Configuring global firmware-update settings). Alerts are hidden by default.

For more information about the firmware-compliance policies, see Creating firmware-compliance policies.

Step 3. **Applying and activating updates**

XClarity Administrator does not automatically apply firmware updates to managed devices. To update firmware, you must manually apply and active the update on selected devices. You can apply the firmware in one of the following ways:

- **Apply bundled firmware updates using compliance policies**

  You can apply firmware updates to *all* components in the selected devices according to the assigned firmware-compliance policy using a bundle image that contain the applicable firmware update packages.

  The bundled-update process first updates the baseboard management controller and UEFI out of band. When these updates are complete, the process creates a bundled image of remaining firmware in the compliance policy based on the machine type. Then, the process mounts the image to the selected device and restarts the device to boot the image. The image automatically runs to perform the remaining updates.

  Attention: The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.

  Notes:

  – Applying bundled firmware updates is supported only for ThinkSystem SR635 and SR655 servers.

  – Ensure that each target device was booted to the OS at least once to retrieve the full inventory information.

  – Baseboard management controller firmware v2.94 or later is required to use the bundled-update function.

  – Only firmware updates from repository packs or individual firmware updates are used. UpdateXpress System Packs (UXSPs) are not supported.

  – Only downloaded firmware updates are applied. Refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

    Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.

  – Compliance check is supported only for the baseboard management controller and UEFI in ThinkSystem SR635 and SR655 servers; however, XClarity Administrator attempts to apply firmware updates to all available hardware components.

  – Updates are applied according to the assigned firmware-compliance policy. You cannot choose to update a subset of components.

  – XClarity Administrator v3.2 or later is required to apply firmware updates for Lenovo XClarity Provisioning Manager (LXPM), LXPM windows drivers, or LXPM Linux drivers to ThinkSystem SR635 and SR655 servers.

  – The baseboard management controller and UEFI updates are skipped if the currently installed version is higher than the assigned compliance policy.

  – Firmware-compliance policies must be created and assigned to the devices on which you intend to apply firmware updates. For more information, see Creating firmware-compliance policies and Assigning firmware-compliance policies.

  – The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

- **Apply selected firmware updates with or without compliance policies**

  You can apply firmware updates on selected components and devices according to the assigned firmware-compliance policy using applicable firmware-update packages. You can also choose to apply firmware updates that are later than the currently installed firmware on selected components and devices without using compliance policies.

  You can choose to apply updates for all components in a specific device. You can also choose to update only a subset of components in the selected devices, such as the baseboard management controller or UEFI.

  To activate the firmware updates, the devices must be restarted. (Note that restarting a device is disruptive.) You can choose to restart the devices as part of the update process (called *immediate activation*), or wait until a maintenance window is available to restart the devices (called *delayed activation*). In this case, you must manually restart the device for the update to take effect.

  When you choose to update the firmware for a managed device, the following steps occur:

  1. XClarity Administrator sends the firmware updates (for example, for the management controller, UEFI, and DSA) to the device.
  2. When the device is restarted, the firmware updates are activated on the device.
  3. For servers, XClarity Administrator sends updates for optional devices, such as network adapter and hard drive updates. XClarity Administrator applies these updates, and the server is restarted
  4. When you restart the device or choose immediate activation, the updates for the optional devices are activated.

  Notes:

  – When applying updates using compliance policies, a firmware-compliance policy must be created and assigned to each target devices. For more information, see Creating firmware-compliance policies and Assigning firmware-compliance policies.

  – If you choose to install a firmware-update package that contains updates for multiple components, all components to which the update package applies are updated.

  – Updates to CMMs and Flex switches are always activated immediately, even if you select delayed activation.

When you perform updates on a set of devices, XClarity Administrator performs the updates in the following order:
- Chassis CMM
- RackSwitch and Flex System switches
- Flex compute nodes, and rack and tower servers
- Lenovo Storage devices

Attention: Before you attempt to apply firmware updates on managed devices, ensure that you have completed the following actions:

- Read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).
- Initially, devices that are not supported for updates are hidden from the view. Devices that are not supported cannot be selected for updates.
- By default, all detected components are listed as available for applying updates; however, down-level firmware might prevent a component from appearing in inventory or reporting full-version information. To list all policy-based packages that are available for you to apply updates, click **All Actions → Global Settings**, and selecting **Enhanced Support for Down-Level**

Devices. When this option is selected, “Other Available Software” is listed in the Installed Version column for undetected devices. For more information, see Configuring global firmware-update settings.

Notes:

- The global settings cannot be changed when updates to managed devices are in progress.
- It takes a few minutes to generate the additional options. After a few moments, you might need to click the **Refresh** icon ( ) to refresh the table.

- Ensure that no jobs are currently running on the target server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.
- Ensure that the firmware-updates repository contains the firmware packages that you intend to deploy. If not, refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.

  If you intend to install prerequisite firmware, ensure that the prerequisite firmware is downloaded in the repository as well.

  In some cases, multiple versions might be needed to update firmware, and all versions would need to be downloaded to the repository. For example, to upgrade the IBM FC5022 SAN scalable switch from v7.4.0a to v8.2.0a, you must first install v8.0.1-pha, then v8.1.1, and then v8.2.0a. All three versions must be in repository to update the switch to v8.2.0a.
- Typically, devices must be restarted to activate the firmware update. If you choose to restart the device during the update process (*immediate activation*), ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

For more information about installing updates, see Applying and activating firmware updates.

Firmware-update considerations

Before you begin updating firmware for managed devices by using Lenovo XClarity Administrator, review the following important considerations.

General considerations

- **Minimum required levels of firmware.**

  Ensure that the firmware that is installed on each managed device is at the minimum required level before using XClarity Administrator to update firmware on those devices. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.

  Note: For information about I/O device support and known limitations, see the XClarity Administrator Support – Compatibility webpage.
- **Update all components to the level that is included in the firmware-updates repository.**

  Because firmware updates for Flex System components are tested and released together, it is recommended that you maintain the same firmware level on all components in a Flex System chassis. Therefore, it is important to update firmware on all components in the chassis in the same maintenance window. XClarity Administrator applies the selected updates in the correct sequence automatically.
- **LXPM Linux Drivers and LXPM Windows Drivers are not included when downloading UXSPs**

Lenovo XClarity Provisioning Manager (LXPM) Linux and Windows drivers are not included in UpdateXpress System Packs (UXSPs). To apply these update packages to your devices, either download the latest firmware-update repository packs or manually download the individual packages and create a firmware compliance policy to include those packages.

- **Some firmware updates are codependent on a minimum level of device driver.**

  Before applying adapter and I/O firmware updates on a server, you might be required to update the device driver to a minimum level. In general, firmware updates are not dependent on specific levels of device drivers. Refer to the firmware update readme for such co-dependencies, and update the device drivers in your operating system before updating the firmware. XClarity Administrator does not update device drivers in your operating system.

- **Reboot XClarity Administrator before updating firmware**

  If previous attempts to update firmware fails, reboot XClarity Administrator before updating firmware. Rebooting the management sever ensures that the system reserved account that is used to update firmware is synchronized on the managed devices.

- **Firmware updates are disruptive and require workloads to be quiesced on devices.**

  Performing firmware updates on managed devices is disruptive if you choose to immediately activate the update. You must quiesce the devices before updating firmware using immediate activation.

  When updating firmware on servers, the servers are shut down and placed in a maintenance operating system to update device drivers for adapters, disk drives, and solid-state drives.

  Flex switches in a given chassis are updated sequentially and are restarted during the firmware update process. Implementing redundant data paths lessens the disruption, but there might still be a brief interruption in network connectivity during the firmware update.

- **Do not use XClarity Administrator to update the firmware on the server on which XClarity Administrator is running.**

  If XClarity Administrator is running on a hypervisor host that runs on a server that it is managing, do not use XClarity Administrator to update firmware on that server. When firmware updates are applied with immediate activation, XClarity Administrator forces the target server to restart, which would restart the hypervisor host and XClarity Administrator as well. When applied with deferred activation, only some firmware is applied until the target system is restarted

CMM considerations

- **Virtually reseat CMMs before updating firmware .**

  If you are updating CMMs that are running firmware level stack release 1.3.2.1 2PET12K through 2PET12Q, that have been running for more than three weeks, and are in a dual-CMM configuration, you must virtually reseat both the primary and standby CMMs before updating firmware (see Virtually reseating a CMM.

Baseboard-management controller considerations

- **IPMI over KCS Access must be enabled in the baseboard management controller to ensure that the management controller can communicate with XClarity Administrator.**

  To enable this option from the Lenovo XClarity Controller user interface, click **BMC Configuration → Security → IPMI over KCS Access**.

- **Minimum required BMC levels for Pending-Activation status**

  To see the pending-activation status, the following firmware version must be installed on the primary baseboard management controller in the server.
  - **IMM2**: TCOO46F, TCOO46E, or later (depending on the platform)
  - **XCC**: CDI328M, PSI316N, TEI334I, or later (depending on the platform)

- **Updates applied to the primary management controller and UEFI firmware partitions.**

  Baseboard management-controller (BMC) and UEFI updates can be applied to the primary and backup firmware partitions for the management controller and UEFI independently.

  You can also apply management controller and UEFI updates to only the primary firmware partitions on the server. By default, the management controller is configured to synchronize the backup management controller partition with the primary management controller partition after the primary management controller has been running satisfactorily and the new level is ready to promote to backup. However, the management controller is not configured to synchronize the UEFI backup partition by default. Therefore, consider one of the following options on the management controller:

  – Enable the automatic synchronization of the UEFI backup partition.

    This ensures that both the primary and backup partitions are running the same level of firmware (and that the backup UEFI firmware is compatible with the management controller firmware).

  – Disable the automatic synchronization of the management-controller backup partition.

    Although not recommended, this gives you complete control over the firmware levels for the management controller and the UEFI. However, you must manually update the management controller and UEFI firmware for both partitions.

  You use firmware-compliance policies to determine which updates are applied to each device. For more information about firmware-compliance policies, see Creating firmware-compliance policies.

  Note: If the management controller and UEFI are configured to automatically synchronize the backup firmware from the primary, it is not necessary for XClarity Administrator to update the backup banks. In that case, you can clear the backup bank updates when applying updates to a server or remove the backup banks from the firmware-compliance policy.

- **Possibility of VMware vSphere ESXi system failure (host purple diagnostic screen) when a management controller is reset.**

  If you are running VMware vSphere ESXi on any server, ensure that the following minimum VMware ESXi levels are installed before updating the firmware on the server:

  – If you are running VMware vSphere ESXi 5.0, install a minimum level of 5.0u2 (update 2)

  – If you are running VMware vSphere ESXi 5.1, install a minimum level of 5.1u1 (update 1)

  If you do not install these minimum levels, a VMware vSphere ESXi system failure (host purple diagnostic screen) might occur whenever the management controller is reset, including when management-controller firmware is applied and activated.

  Note: This issue does not affect ESXi v5.5.

ThinkSystem device considerations

- For ThinkSystem SR635 and SR655 servers, the following limitations apply.

  – Only Immediate activation is supported. Delayed activation and Prioritized activation are not supported.

  – For XClarity Administrator v3.1.1 and later, you can use the bundled update function to update all components on ThinkSystem SR635 and SR655 servers, including baseboard management controller, UEFI, disk drives, and IO options.

    Attention: The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.

    Notes:

- Applying bundled firmware updates is supported only for ThinkSystem SR635 and SR655 servers.
- Ensure that each target device was booted to the OS at least once to retrieve the full inventory information.
- Baseboard management controller firmware v2.94 or later is required to use the bundled-update function.
- Only firmware updates from repository packs or individual firmware updates are used. UpdateXpress System Packs (UXSPs) are not supported.
- Only downloaded firmware updates are applied. Refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.
- Compliance check is supported only for the baseboard management controller and UEFI in ThinkSystem SR635 and SR655 servers; however, XClarity Administrator attempts to apply firmware updates to all available hardware components.
- Updates are applied according to the assigned firmware-compliance policy. You cannot choose to update a subset of components.
- XClarity Administrator v3.2 or later is required to apply firmware updates for Lenovo XClarity Provisioning Manager (LXPM), LXPM windows drivers, or LXPM Linux drivers to ThinkSystem SR635 and SR655 servers.
- The baseboard management controller and UEFI updates are skipped if the currently installed version is higher than the assigned compliance policy.
- Firmware-compliance policies must be created and assigned to the devices on which you intend to apply firmware updates. For more information, see Creating firmware-compliance policies and Assigning firmware-compliance policies.
- The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

You can also use the traditional update function to apply firmware updates to only the baseboard management controller and UEFI.

- For XClarity Administrator v3.0:
  - Management data is not correctly updated when updating firmware from 20A to 20B or 20C. To work around this issue, either unmanage and then manage the device again, or restart XClarity Administrator.
  - Downgrading firmware updates is not supported.
- For XClarity Administrator v2.8 and later
  - You can update baseboard management controller and UEFI firmware using the traditional update process. Baseboard management controller firmware version AMBT10M or later is required, and UEFI firmware version CFE114L or later is required.
  - Firmware updates are not supported in the following situations.
    - If XClarity Administrator v2.7 manages ThinkSystem SR635 and SR655 servers running 20A firmware, and you upgrade to 20B firmware using the baseboard management controller before upgrading to XClarity Administrator v2.8.
    - If XClarity Administrator v2.7 manages ThinkSystem SR635 and SR655 servers running 20B firmware before upgrading to XClarity Administrator v2.8.
    - If XClarity Administrator v2.8 manages ThinkSystem SR635 and SR655 servers running 20A firmware, and you upgrade to 20B firmware using the baseboard management controller.

- **XClarity Administrator v2.1, v2.2, and v2.3 require a cumulative patch to manage ThinkSystem servers running BMC firmware TEI342s-2.40, CDI334v-2.50, or PSI322k-1.50.**

  For XClarity Administrator v2.1, v2.2, and v2.3, before updating BMC firmware on ThinkSystem servers to version TEI342s-2.40, CDI334v-2.50, or PSI322k-1.50, you must either apply the latest XClarity Administrator Virtual Appliance Cumulative Patch or update to XClarity Administrator v2.4. XClarity Administrator v2.0 or earlier does not require the cumulative patches.

- **Firmware updates is not supported on ThinkSystem servers using DHCPv6 or statically assigned IPv6 addresses**

  When using IPv6 addressing on ThinkSystem servers, firmware updates is supported on only IPv6 Link-Local Address(LLA) and stateless addresses.

- **When updating firmware to version 20D, you must update both UEFI and XCC together.**

  UEFI and Lenovo XClarity Controller (XCC) must be updated together for version 20D. Updating XCC and not UEFI, and vice versa, will cause issues.

Flex System device considerations

- **Ensure that the Flex switches that are being updated are powered on,**
- **Select Immediate Activation when updating compute nodes that are at management-controller firmware levels earlier than Flex System 1.3.2.**

  When you apply the Flex System 1.3.2, 2nd Quarter lifecycle release to a compute node, you must choose *immediate activation* to update the compute node. Immediate activate forces the compute node to restart during the update process.

- **Flex switches must be configured with an IP address that is reachable from XClarity Administrator.**

  The target Flex switch must be assigned an IP address that can communicate with XClarity Administrator so that XClarity Administrator can download and apply the firmware update.

- **Update support on scalable complexes, such as x480 X6 and x880 X6 nodes.**

  Update support on scalable nodes such as the Flex System x480 X6 and x880 X6 compute nodes is limited to configurations where the complex is configured as a *single partition* that includes all compute nodes that are part of the multi-node complex. You cannot use XClarity Administrator to update a complex that consists of multiple partitions.

  If you assign a firmware-compliance policy to a partition that includes multiple servers in a scalable complex (such as Flex System x480 X6 and x880 X6 compute nodes), XClarity Administrator updates firmware on all management controllers and UEFIs for each server in the partition by default. However, if you select a subset of components within the partition, XClarity Administrator updates the firmware on only the selected components in the partition.

- **Before updating the CMM2 to v1.30 (1AON06C) or later, Flex switches must be running Level 3 version of Enhanced Configuration and Management (EHCM L3)**

  CMM2 and the Flex switches communicate using the EHCM protocol. This protocol is required for XClarity Administrator to update the Flex switches. When you update a CMM2 to v1.30 (1AON06C) or later, XClarity Administrator verifies that the Flex switches are running EHCM L3 and if not, cancels the CMM update with a warning that the Flex switches must be first updated to a version that supports EHCM-L3. You can override this verification by selecting **Attempt to update components already in compliance** when updating the CMM firmware.

  Attention: There is currently no firmware version for Flex System EN6131 Ethernet switches and IB6131 InfiniBand switches that support EHCM L3. This means that after you update the CMM2 to firmware v1.30 (1AON06C) or later, you can no longer use XClarity Administrator to update those switches. The work-around is to use the management controller web interface or command-line interface for the chassis to update the switch.

Flex System switch	Version	Release date
CN4093	7.8.4.0	June 2014
EN4023	6.0.0	April 2015
EN4093	7.8.4.0	June 2014
EN4093R	7.8.4.0	June 2014
EN6132	Not available	Not available
FC3171	9.1.3.02.00	June 2014
FC5022	7.4.0b1	March 2016
IB6132	Not available	Not available
SI4091	7.8.4.0	June 2014
SI4093	7.8.4.0	June 2014

Note: The EN2092 1-Gb Ethernet Scalable Switch does not require EHCM L3 and does not have this restriction.

Storage considerations

- **ThinkSystem DM storage devices be at v9.7 or later**

  To update firmware on ThinkSystem DM storage devices, the devices must be running v9.7 or later.

  Downgrading is supported for only minor versions. For example, you can downgrade 9.7P11 to 9.7P9; however you cannot downgrade 9.8 to 9.7.

- **Disk drives must be in the JBOD, Online, Ready, or Unconfigured (good) state.**

  To update firmware on disk drives, the RAID state must be JBOD, Online, Ready, or Unconfigured (good). Other states are not supported. To determine the RAID state for a disk drive, go to the Inventory page for the device, expand the **Drives** section, and check the **RAID State** column for that disk drive (see Viewing the details of a managed server).

- **Firmware version does not detect disk drives and solid state drives.**

  XClarity Administrator detects only the installed-firmware version and performs a compliance check for disk drives and solid-state drives (SSDs) that are attached to a MegaRAID or an NVME adapter. Other attached drives might have a level of firmware that is not supported or might not support firmware-version reporting. However, firmware updates are applied to those drives when selected.

- **NVMe firmware is applied even if it is not identified with a target component**

  On the Apply/Activate page, the NVMe firmware version is listed for solid state drives (SSDs). Because no target firmware update is identified for discovered NVMe devices, a warning message is displayed when you attempt to update the target system. However, the HDD/SSD update is applied even if it is not identified with a target component, so the NVMe firmware is still updated.

- **Applying the ServeRAID M5115 PSoC3 update package from XClarity Administrator requires a minimum installed level of 68.**

  The ServeRAID M5115 PSoC3 (Programmable System-on-Chip) update from earlier than version 68 must be done in a controlled manner.

  Tip: You can view the code version for the ServeRAID M5115 PSoC3 by logging in to the CMM web interface and selecting the **Firmware** tab for the target compute node. Then, select the expansion card for the ServeRAID M5115 adapter. The PSoc3 code version is the GENERIC firmware type.

For installed versions earlier than 68, you cannot update using XClarity Administrator. Instead you must perform the following steps from either the Chassis Management Module (CMM) web interface or the command-line interface (CLI):

- **Using the CMM web interface:**
  1. Log in to the Chassis Management Module (CMM) web interface.
  2. From the main menu, click **Service and Support → Advanced**.
  3. Click the **Service Reset** tab.
  4. Select the appropriate compute node by clicking its radio button.
  5. From the **Reset** pull down button, click **Virtual Reseat**.
  6. Click **OK** to confirm.
- **Using the CMM CLI**:
  - Log in to the CMM Secure Shell (SSH) interface.
  - Enter the following command to perform a virtual reseat:
    `'service -vr -T blade[x]`

    where *x* is the bay number of the compute node to be reseated.

After the system is powered back on, boot to the operating system and update the ServeRAID M5115 PSoC3 using the extracted embedded update package. Complete the following steps to extract the embedded package.

- **Using Microsoft Windows:**

  Open the update package (lnvgy_fw_psoc3_m5115-70_windows_32-64.exe), and select Extract to Hard Drive. Then, select the path where the embedded package is to be extracted.
- **Using Linux:**

  Run the following command:

  `lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x`

  where *x* is the location where the embedded package is to be extracted.

Managing the firmware-updates repository

The *firmware-updates repository* contains a catalog of available updates and the update packages that can be applied to the managed devices.

About this task

The *catalog* contains information about firmware updates that are currently available for all devices that XClarity Administrator supports. The catalog organizes the firmware updates by device type. When you refresh the catalog, XClarity Administrator retrieves information about the latest available firmware updates from the Lenovo website and stores the information in the firmware-updates repository.

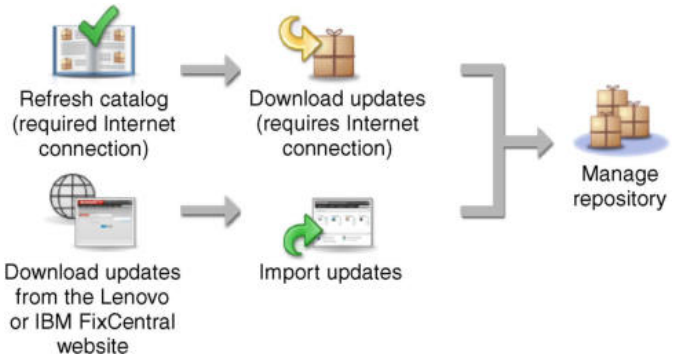
If new firmware updates are available, you must first download the update packages before you can update that firmware on the managed devices. Refreshing the catalog does not automatically download update packages. The Product Catalog table on the Firmware Updates Repository page identifies which update packages are downloaded and which are available for download.

You can download firmware updates in a few different ways:

- **Individual firmware updates**. You can download individual firmware-update packages, at one time, based on the version that is listed in the catalog.

- **UpdateXpress System Packs (UXSPs)**. UXSPs contains the latest available firmware and device driver updates, organized by operating system. When you download UXSPs from the Firmware Updates: Repository page, only firmware updates are downloaded and stored in the repository. Device driver updates are excluded.
- **Firmware-update repository packs**. Repository packs contains the latest available firmware updates for all supported devices and a refreshed default firmware-compliance policy. These repository packs are imported and then applied from the Update Management Server page.

XClarity Administrator must be connected to the Internet to refresh the catalog and download firmware-update. If it is not connected to the Internet, you can manually download the files to a workstation that has network access to the XClarity Administrator host using a web browser and then import the files into the firmware-updates repository.



When you manually import firmware updates into XClarity Administrator, you must include the following required files: payload (image and MIB), metadata XML, change history, and readme. For example:
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Attention:

- Only import these required files. Do not import other files that might be found on the firmware download websites.
- If you do not include the XML file in the update package, the update is not imported.
- If you do not include all required files that are associated with the update, the repository shows that the update is not downloaded, which means that it is partially imported. You can then import the missing files by selecting and importing them.
- The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

After the firmware-updates are downloaded in the repository, information is provided about each update, including the release date, size, policy usage, and severity. The severity indicates the impact and the need to apply the update to help you to assess how your environment might be affected.
- **Initial Release**. This is the first release of the firmware.
- **Critical**. The firmware release contains urgent fixes for data corruption, security, or stability issue.
- **Suggested**. The firmware release contains significant fixes for problems that you are likely to encounter.
- **Non-Critical**. The firmware release contains minor fixes, performance enhancements, and textual changes.

Notes:

- The severity is relative to the previously released version of the update. For example, if the installed firmware is v1.01, and update v1.02 is Critical and update v1.03 is Recommended, this means that the update from 1.02 to 1.03 is recommended, but the update from v1.01 to v1.03 is critical because it is cumulative (v1.03 includes v1.02 critical issues).
- Special cases might arise where an update is only critical or recommended for a specific machine type or operating system. Refer to the Release Notes for additional information.

Procedure

To view firmware updates that are available in the product catalog, complete the following steps.

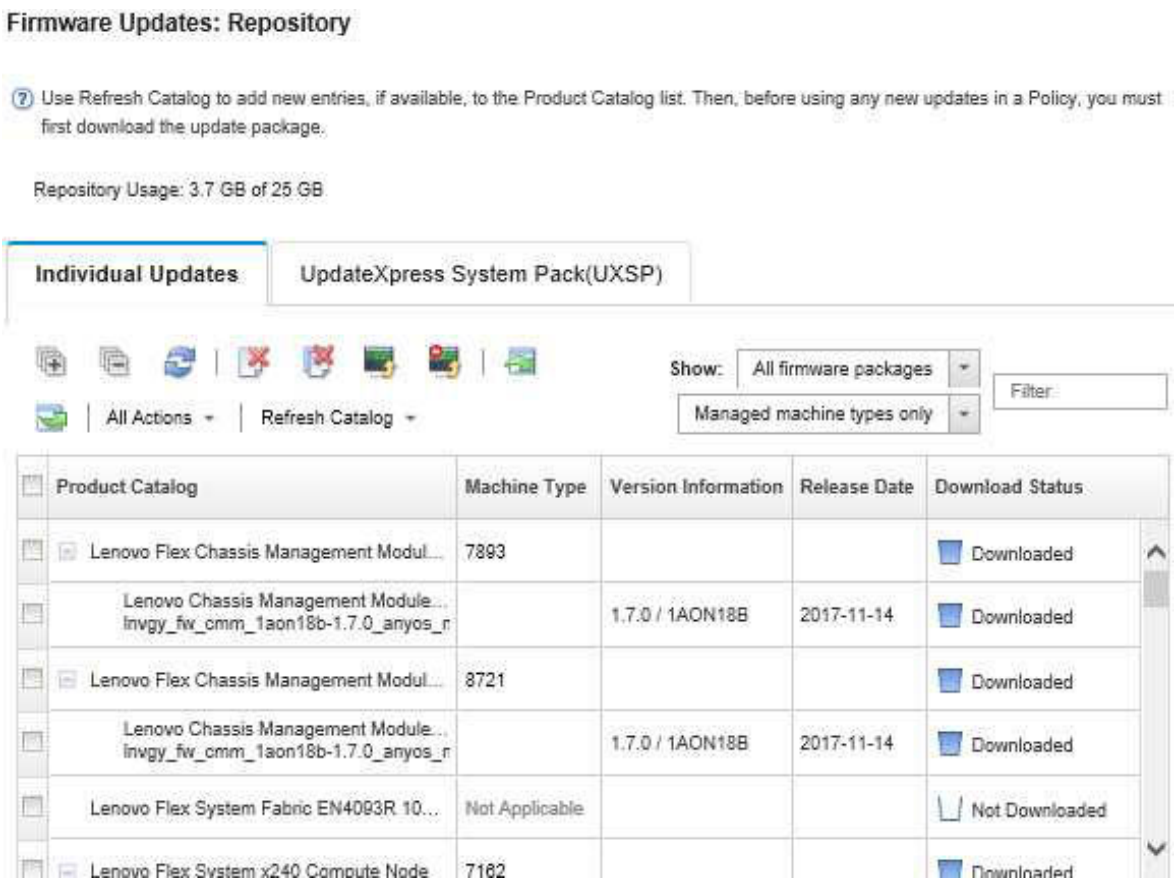
Step 1. From the XClarity Administrator menu bar, click **Provisioning → Repository**. The Firmware Updates Repository page is displayed with a list of available firmware-update packages, organized by device type.

Step 2. Click the **Individual Updates** tab to view information about available firmware update packages, or click the **UpdateXpress System Packs (UXSPs)** tab to view information about available UXSPs

Step 3. Expand a device and device components to list the update packages and firmware updates for that device.

You can sort the table columns and click the **Expand all** icon () and **Collapse all** icon () to make it easier to find specific firmware updates. In addition, you can filter the list of displayed devices and firmware updates by selecting an option in the **Show** menu to list only firmware updates of a specific age, firmware updates for all server types or only managed-server types or by entering text in the **Filter** field. Note that if you search for specific devices, only the devices are listed; firmware updates are not listed under the device name.

Note: For servers, specific update packages are available based on the type of server. For example, if you expand a server, such as the Flex System x240 Compute Node, update packages that are available specifically for that compute node are displayed.



Results

From this page, you can perform the following actions:

- Refresh this page with the current firmware-update information in the catalog by clicking the **Refresh** icon ( ).
- Retrieve the latest information about available updates by clicking **Refresh Catalog**.Retrieving this information might take several minutes to complete. For more information, see Refreshing the product catalog.
- Add the firmware updates to the repository by selecting one or more update packages or updates in the product catalog and then clicking the **Download** icon ( ). When the firmware updates are downloaded and added to the repository, the status changes to “Downloaded.”

  Note: The XClarity Administrator must be connected to the Internet to acquire updates through the XClarity Administrator user interface. If it is not connected to the Internet, you can import updates that you previously downloaded.

  For more information about downloading updates, see Downloading firmware updates.
- Import firmware updates that you manually downloaded to a workstation that has network access to XClarity Administrator by selecting one or more updates and then clicking the **Import** icon ( ).For more information about importing updates, see Downloading firmware updates.
- Stop firmware downloads that are currently in progress by selecting one or more updates and then clicking the **Cancel Downloads** icon ( ).Canceling downloads cancels *all* firmware downloads that are in progress. You can monitor the detailed progress of and stop a specific firmware download from the jobs log (see Monitoring jobs).

- Delete update packages or individual updates from the repository (see Deleting firmware updates).
- Export firmware updates that exist in the firmware-updates repository to a local system (see Exporting and importing firmware updates).

Refreshing the product catalog

The product catalog contains information about all firmware updates that are available for all devices that Lenovo XClarity Administrator supports, including chassis, servers, and Flex switches.

Before you begin

An Internet connection is required to refresh the product catalog.

Refreshing the catalog might take several minutes to complete.

About this task

When you refresh the catalog, XClarity Administrator retrieves information about the latest available firmware updates from the Lenovo XClarity Support website and stores the information to the firmware-updates repository.

Refreshing the catalog only adds information about available firmware updates to the repository. It does not download the update packages. You must download the firmware updates to make the updates available for installation. For more information about downloading updates, see Downloading firmware updates.

Procedure

To refresh the product catalog, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.

Step 2. Click the **Individual Updates** tab to retrieve information about individual firmware-update packages, or click the **UpdateXpress System Pack (UXSP)** tab to retrieve information about UXSPs.

Step 3. Click **Refresh Catalog**, and then click one of the following options to obtain information about the latest available firmware updates.

- **Refresh Selected - Latest Only**. Retrieves information about the most current version of firmware updates that are available for only the selected devices.
- **Refresh All - Latest Only**. Retrieves information about the most current version of all firmware updates for all supported devices.
- **Refresh Selected**. Retrieves information about all versions of firmware updates that are available for only the selected devices.
- **Refresh All**. Retrieves information about all versions of all firmware updates that are available for all supported devices.

Tip: You can refresh the product catalog and download the latest firmware in one step by clicking **All Actions → Refresh and download the latest for all managed devices** or **All Actions → Refresh and download the latest for selected devices**.

Downloading firmware updates

You can download or import firmware updates in the firmware-updates repository, depending on your access to the Internet. Firmware updates must be available in the firmware-updates repository before you can update firmware on management devices.

Before you begin

Ensure that all ports and Internet address that Lenovo XClarity Administrator requires are available before you attempt to download firmware. For more information about ports, see Port availability and Firewalls and proxy servers in the XClarity Administrator online documentation.

If a device type is not listed in the firmware-updates repository, you must first manage a device of that type before downloading or importing individual firmware updates for that device type.

Important:

- For XClarity Administrator v1.1.1 and earlier, you must manually download and import the firmware updates for Lenovo hardware from Lenovo Data Center Support website.
- XClarity Administrator cannot download updates for RackSwitch switches and Lenovo storage devices from the Lenovo website to the firmware-updates repository; instead, you must manually download and import the RackSwitch and Lenovo Storage updates from the Lenovo website to a workstation that has network access to the XClarity Administrator host, or download and apply the *firmware-update repository packs*, which contain all available firmware updates.
- Internet Explorer and Microsoft Edge web browsers have an upload limit of 4 GB. If the file that you are importing is greater than 4 GB, consider using another web browser (such as Chrome or Firefox).

About this task

You can download firmware updates in a few different ways:

- **Firmware-update repository packs**

  Firmware-update repository packs contains the latest available firmware updates at a specific point in time for all supported devices and a refreshed default firmware-compliance policy. These repository packs are imported and then applied from the Update Management Server page. When you apply a firmware-update repository pack, each update package in the pack is added to the firmware-updates repository, and a default firmware-compliance policy is automatically created for all manageable devices. You can copy this predefined policy, but you cannot change it.

  The following repository packs are available:

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all CMMs and Flex System switches.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all RackSwitch switches and Lenovo Storage devices.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all Converged HX Series, Flex System, NeXtScale, and System x servers.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all ThinkAgile and ThinkSystem servers.
  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all ThinkAgile and ThinkSystem V2 servers.

  You can determine whether firmware-update repository packs are stored in the repository from the **Download Status** column on Update Management Server page. This column contains the following values:

  - **Downloaded**. The firmware-update repository pack is stored in the repository.
  - **Not Downloaded**. The firmware-update repository pack is available but not stored in the repository.
- **UpdateXpress System Packs (UXSPs)**

UXSPs contains the latest available firmware and device driver updates, organized by operating system. When you download UXSPs, XClarity Administrator downloads the UXSP, based on the version that is listed in the catalog, and stores the update packages in the firmware-updates repository. When you download a UXSP, each firmware update in the UXSP is added to the firmware-updates repository and listed on the **Individual Updates** tab, and a default firmware-compliance policy is automatically created for all manageable devices using the name *<uxsp-version>-<date>-<server-short-name>*`-UXSP` (for example, `v1.50-2017-11-22- SD530-UXSP`). You can copy this predefined policy, but you cannot change it.

Note: When you download UXSPs from the Firmware Updates: Repository page, only firmware updates are downloaded and stored in the repository. Device driver updates are excluded. For information about downloading Windows device driver updates using UXSPs, see Managing the OS device-drivers repository.

You can determine whether UXSPs are stored in the firmware-updates repository from the **Download Status** column on the **Individual Updates** tab of the Firmware Updates: Repository page. This column contains the following values:

- **Downloaded**. The entire update package or the individual firmware update is stored in the repository.
- *x* **of** *y* **Downloaded**. Some but not all firmware updates in the update package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
- **Not Downloaded**. The entire update package or the individual firmware update is available but not stored in the repository.

- **Individual firmware updates**

  You can download individual firmware-update packages, at one time. When you download firmware-update packages, XClarity Administrator downloads the update, based on the version that is listed in the catalog, and stores the update packages in the firmware-updates repository. You can then create firmware-compliance policies using those update packages for each of your managed devices.

  Note: The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

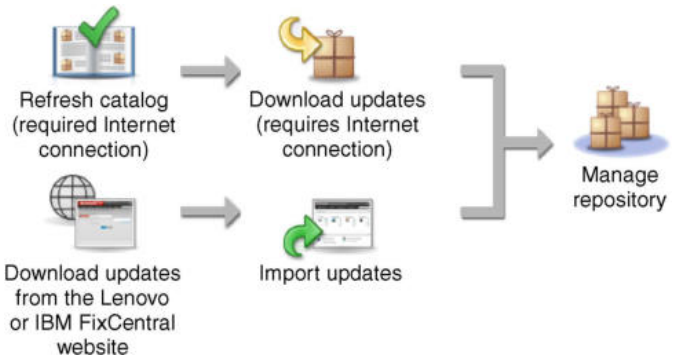
  You can determine whether specific *firmware updates* are stored in the firmware-updates repository from the **Download Status** column on the **Individual Updates** tab on the Firmware Updates: Repository page. This column contains the following values:

  - **Downloaded**. The entire update package or the individual firmware update is stored in the repository.
  - *x* **of** *y* **Downloaded**. Some but not all firmware updates in the update package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
  - **Not Downloaded**. The entire update package or the individual firmware update is available but not stored in the repository.

When you install XClarity Administrator or update to a new release, it is a best practice to download the latest repository pack to ensure you have the latest firmware updates. Then, you can schedule a recurring job to refresh the catalog to find individual updates that were posted on the web since the last repository pack and then electronically download those updates, one at a time.

XClarity Administrator must be connected to the Internet to refresh the catalog and download firmware-update. If it is not connected to the Internet, you can manually download the files to a workstation that has

network access to the XClarity Administrator host using a web browser and then import the files into the firmware-updates repository.



When you manually import firmware updates into XClarity Administrator, you must include the following required files: payload (image and MIB), metadata XML, change history, and readme. For example:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Note: The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers.

A message is displayed on the page when the repository is more than 50% full. Another message is displayed on the page when the repository is more than 85% full. To reduce the space used in the repository, you can remove unused images files and policies. You can remove unused firmware-compliance policies and associated firmware packages by clicking **Provisioning → Compliance policies**, selecting one or more policies to delete, and then clicking **Actions → Delete any policy and firmware packages**.

The following table summarizes the differences between acquiring firmware-update repository packs, UXSPs, and individual firmware-update packages.

Update package	UI page for downloading and importing files	Webpage to download files manually	Is the firmware updates repository refreshed?	Is the firmware-compliance policy refreshed automatically?
Firmware-update repository packs	Update Management Server page **Note:** You must import and then apply the repository pack.	XClarity Administrator download webpage	Yes	Yes
UpdateXpress System Packs	Firmware Updates: Repository page, **UpdateXpress System Packs (UXSPs)** tab	Lenovo XClarity Essentials UpdateXpress webpage	Yes	Yes
Firmware-updates	Firmware Updates: Repository page, **Individual Updates** tab	Lenovo Data Center Support website **Notes:** Use the Fix Central website for the following devices: • Flex System x220 Type 2585, 7906 • Flex System x222 Compute Nod Type 2589, 7916 • Flex System x240 Type 7863, 8737, 8738, 8956 • Flex System x280 / x480 / x880 X6 Type 4259, 7903 • Flex System x440 Type 2584, 7917	Yes	No

Procedure

To download one or more firmware updates, complete the following steps.

- To import one or more *firmware-update repository packs*:
  1. From the XClarity Administrator menu bar, click **Administration → Update Management Server** to display the Management Server Update page.
  2. Download the latest repository packs:
     - If XClarity Administrator is connected to the Internet:
       a. Retrieve information about the latest updates by clicking the **Refresh Catalog → Refresh All Managed – Latest only**). New management-server updates and firmware-update repository packs are listed in the table on the “Management Server Update” page.

          Refreshing the repository might take several minutes to complete.

          Note: Refreshing the repository does not automatically download payload files. Only the XML and readme files are downloaded.
       b. Select the firmware-update repository packs that you want to download.

          Tip: Ensure that the packages that you select have “Supplemental Pack” in the **Type** column.

c. Click the **Download Selected** icon (). When the download is complete, the **Download Status** for that software update changes to “Downloaded”.

– If XClarity Administrator is not connected to the Internet:

a. Download the firmware-update repository packs from the XClarity Administrator download webpage to a workstation that has a network connection to the XClarity Administrator host.

b. From the Management Server Update page, click the **Import** icon ().

c. Click **Select Files**, and browse to the location of the firmware-update repository packs on the workstation.

d. Select all package files, and then, click **Open**.

You must import the metadata file (.xml) as well as the image or payload file (.zip, .bin, .uxz, or .tgz), change history file (.chg), and readme file (.txt) for the update. Any files that are selected but are not specified in the .xml file are discarded. If you do not include the .xml file, the update is not imported.

e. Click **Import**.

When the import is complete, the firmware-update repository packs are listed in the table on the Management Server Update page, and the **Download Status** for each update is “Downloaded”.

3. Select the firmware-update repository packs that you want to install to the firmware-updates repository.

Note: Ensure that **Download Status** is “Downloaded” and that the **Type** is “Patch.”

4. Click the **Perform Update** icon () add the firmware-update packages to the repository.
5. Wait a few minutes for the update to complete and XClarity Administrator to be restarted.
6. Determine if the update is complete by refreshing the web browser.

When completed, the Management Server Update page is displayed, and the **Applied Status** column changes to “Applied.”

7. Clear the web browser cache.

- To download one or more *UXSPs*.

1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository** to display the Firmware Updates Repository page.
2. Click the **UpdateXpress System Packs (UXSPs)** tab.
3. Download the latest UXSPs:

– If XClarity Administrator is connected to the Internet:

To refresh the catalog and download the latest UXSPs for all managed devices, click **All Actions → Refresh and download the latest for all managed devices**.

To refresh the catalog and download the latest UXSPs for only selected devices:

a. Expand the device to display the list of available UXSPs.

b. Select one or more UXSPs that you want to download.

c. Click **All Actions → Refresh and download the latest for selected devices**.

When the download is complete, the **Download Status** for the selected UXSPs changes to “Downloaded.”

– If XClarity Administrator is not connected to the Internet:

a. Download the UXSPs from the Lenovo XClarity Essentials UpdateXpress webpage to a workstation that has a network connection to the XClarity Administrator host

b. From XClarity Administrator, click the **Import** icon ().

c. Click **Select Files**, and browse to the location of the UXSPs on the workstation.

d. Select all package files, and then, click **Open**.

You must import the metadata file (.xml) as well as the image or payload file (.zip, .bin, .uxz, or .tgz), change history file (.chg), and readme file (.txt) for the update. Any files that are selected but are not specified in the .xml file are discarded. If you do not include the .xml file, the update is not imported.

e. Click **Import**.

When the import is complete, the firmware-update repository packs are listed in the table on the Management Server Update page, and the Download Status for each update is ""“Downloaded.”

- To download one or more individual *firmware-update packages*.
  1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository** to display the Firmware Updates Repository page.
  2. Click the **Individual Updates** tab.
  3. Download the latest individual firmware-updates:
     - If XClarity Administrator is connected to the Internet:

       To refresh the catalog and download the latest firmware for all managed devices, click **All Actions → Refresh and download the latest for all managed devices**.

       To refresh the catalog and download the latest firmware for only selected devices:

       a. Expand the device to display the list of available firmware updates.

       b. Select one or more firmware updates that you want to download.

       Tip: An update package can consist of multiple firmware updates. When you download a firmware update, you can choose to download the entire update package or only specific updates. You can also choose to download multiple packages at one time.

       c. Click **All Actions → Refresh and download the latest for selected devices**.

       When the download is complete, the **Download Status** for the selected firmware updates changes to “Downloaded”.

     - If XClarity Administrator is not connected to the Internet:

       a. Download the firmware-update packages from the Lenovo Data Center Support website to a workstation that has network connection to the XClarity Administrator host.

       For the following servers, download firmware updates for the SLES 11 operating system from the Fix Central website:

       - Flex System x220 Type 2585, 7906
       - Flex System x222 Compute Nod Type 2589, 7916
       - Flex System x240 Type 7863, 8737, 8738, 8956
       - Flex System x280 / x480 / x880 X6 Type 4259, 7903
       - Flex System x440 Type 2584, 7917

       For all other servers, download firmware updates for the RHEL 6 operating system. from the Lenovo XClarity Support website.

b. From XClarity Administrator, click the **Import** icon ().

c. Click **Select Files**, and browse to the location of the firmware updates on the workstation.

d. Select all package files, and then click **Open**.

   You must import the metadata file (.xml) as well as the image or payload file (.zip, .bin, .uxz, or .tgz), change history file (.chg), and readme file (.txt) for the update. Any files that are selected but are not specified in the .xml file are discarded.

   Attention:

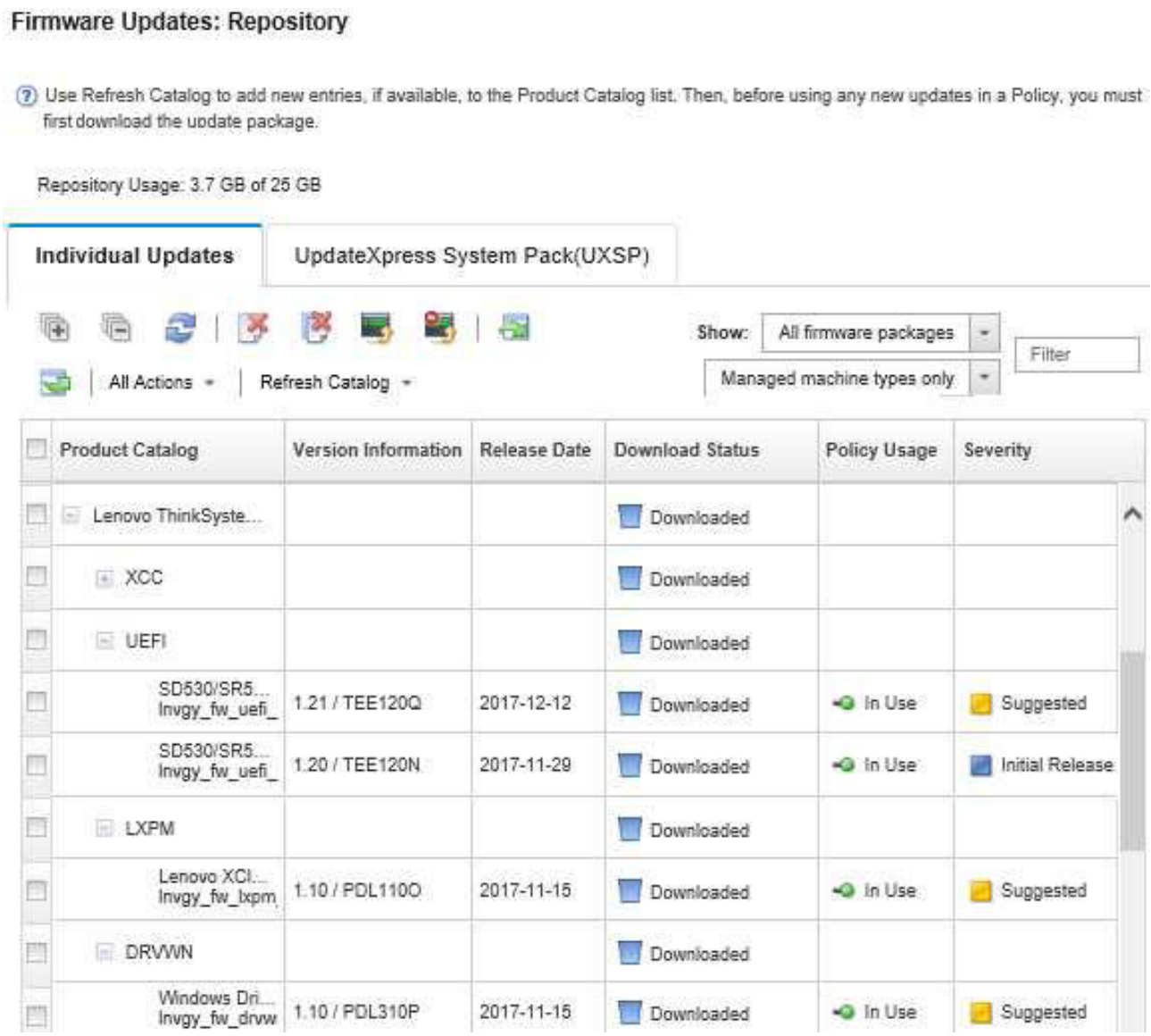
   - Only import these required files. Do not import other files that might be found on the firmware download websites.
   - If you do not include the XML file in the update package, the update is not imported.
   - If you do not include all required files that are associated with the update, the repository shows that the update is not downloaded, which means that it is partially imported. You can then import the missing files by selecting and importing them.
   - The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

e. Click **Import**.

Results

Refreshing the catalog and downloading the firmware updates might take a several minutes. When the updates have been downloaded and stored in the repository, the row in the product catalog is highlighted, and the **Download Status** column is changed to “Downloaded.”

Note: The machine type for some switches might show up as a hexadecimal number.



Exporting and importing firmware updates

You can export individual firmware updates and UpdateXpress System Packs (UXSPs) that exist in the repository to the local system.

About this task

Only firmware updates that exist in the repository are exported. Ensure that the download-status for the selected firmware updates is “Downloaded.”

All of the files that are associated with the firmware update are exported, including the update image or payload file (.zip, .bin, .uxz, or .tgz), metadata file (.xml), change history file (.chg), and readme file (.txt).

Attention: Do not change the name of the firmware update files.

Procedure

- To export firmware updates:
  1. Click the **Individual Updates** tab or **UpdateXpress System Packs (UXSPs)** tab.

2. Select one or more firmware updates.
3. Click the **Export** icon ().

- To import firmware updates:

  You can import files that you manually exported from Lenovo XClarity Administrator and files that you manually downloaded from the web. For more information, see Downloading firmware updates.

Deleting firmware updates

You can delete firmware updates and UpdateXpress System Packs (UXSPs) from the firmware-updates repository.

Before you begin

Ensure that all running or scheduled update jobs that use a firmware-compliance policy that contains the firmware updates to be deleted are completed or canceled (see Monitoring jobs).

Ensure that the update is not being used in a firmware-compliance policy before deleting the update. You cannot delete firmware-update packages that are currently used in one or more firmware-compliance policies.

Deleting a UXSP also deletes the firmware-compliance policy that was automatically created for that UXSP.

Procedure

To delete one or more firmware updates from the repository, complete the following steps.

Step 1. Unassign all firmware-compliance policies that contain the firmware updates to be deleted from all managed devices.

a. From the XClarity Administrator menu bar, click **Provisioning → Apply/Activate**. The Firmware Updates Apply/Activate page is displayed.

b. Select “No assignment” or select another firmware-compliance policy in the **Assigned Policy** column for the managed devices that use the firmware-compliance policy.

Step 2. Delete all user-defined firmware-compliance policies that contain the firmware updates to be deleted, or edited the firmware-compliance policies to remove the firmware updates to be deleted.

a. From the XClarity Administrator menu bar, click **Provisioning → Compliance Policies**. The Firmware Updates Compliance Policies page is displayed.

b. Select the firmware-compliance policy, and then select the **Delete** icon () to delete the policy, or click the **Edit** icon () to remove the firmware updates from the policy.

Step 3. Delete the firmware updates.

- **Individual firmware updates**
  1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.
  2. Click the **Individual Updates** tab.
  3. Select one or more firmware updates to be deleted.
  4. Click the **Delete only images** icon ( to delete only the image or payload file (.zip, .bin, .uxz, or .tgz). Information about the update, remains so that you can easily download the update again. Or click the **Delete full update packages** icon ( to delete the full update packages, including the image or payload file, change history file (.chg), readme file (.txt), and metadata file (.xml).

When you delete a firmware update, the payload files are removed; however, the XML file, which contains information about the update, remains so that you can easily download the update again, if needed, and the **Download Status** changes to "Not downloaded."

- **UXSPs**
  1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.
  2. Click the **UpdateXpress System Pack (UXSP)** tab.
  3. Select one or more UXSPs to be deleted.
  4. Click the **Delete UXSP and associated policy** icon ( ) to delete the full UXSPs, including the image or payload file, change history file (.chg), readme file (.txt), and metadata file (. xml),and all associated firmware-compliance policies.

  If selected UXSPs are associated with policies that are in use (assigned to devices), the Delete UXSP, Policy, and Update Packages dialog is displayed. Choose whether to delete the assigned policies in addition to the UXSP and unassigned policies, and click **OK**.

Creating firmware-compliance policies

Firmware-compliance policies ensure that the firmware on certain devices is at the current or specific level by flagging the devices that need attention. Each firmware-compliance policy identifies which devices are monitored and which firmware level must be installed to keep the devices in compliance. You can set compliance at the device or firmware component level. XClarity Administrator then uses these policies to check the status of managed devices and to identify devices that are out of compliance.

Before you begin

Refresh the product catalog in the firmware-updates repository, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

If a device type is not listed in the firmware-updates repository, you must first manage a device of that type and then download or import the complete set of firmware updates before creating compliance policies for devices of that type.

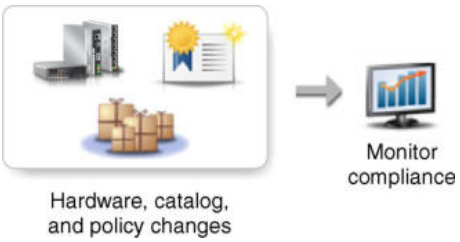
About this task

When you create a firmware-compliance policy, you can choose to have XClarity Administrator flag a device when:

- The firmware on the device is down level
- The firmware on the device does not exactly match the compliance target version

XClarity Administrator comes with a predefined firmware-compliance policy named **Latest firmware in repository**. When new firmware is downloaded or imported into the repository and when XClarity Administrator is restarted, this policy is updated to include latest available versions of firmware in the repository.

After a firmware-compliance policy is assigned to a device, XClarity Administrator checks the compliance status of each device when the device inventory changes or firmware-updates repository changes. When the firmware on a device is not compliant with the assigned policy, XClarity Administrator identifies that device as not compliant on the Firmware Updates: Apply / Activate page, based on the rule that you specified in the firmware-compliance policy



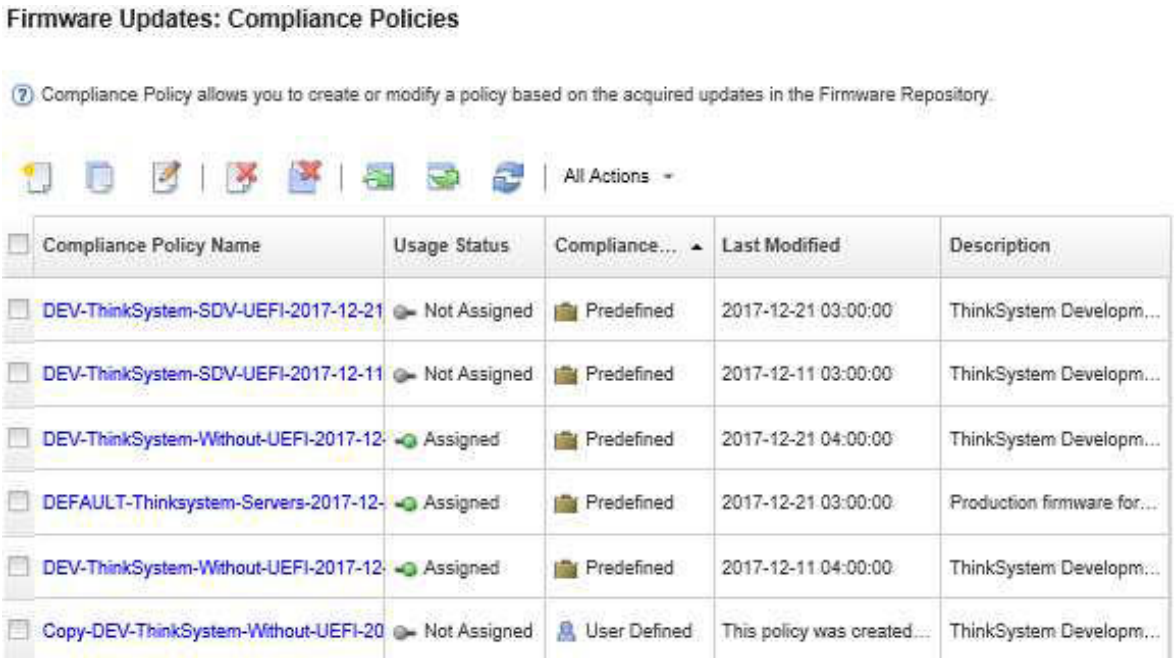
For example, you can create a firmware-compliance policy that defines the baseline level for firmware that is installed in all ThinkSystem SR850 devices and then assign that firmware-compliance policy to all managed ThinkSystem SR850 devices. When the firmware-updates repository is refreshed and a new firmware update is added, those compute nodes might become out of compliance. When that happens, XClarity Administrator updates the Firmware Updates: Apply / Activate page to show that the devices are not compliant and generates an alert.

Note: You can choose to show or hide alerts for devices that do not meet the requirements of their assigned firmware-compliance policies (see Configuring global firmware-update settings). Alerts are hidden by default.

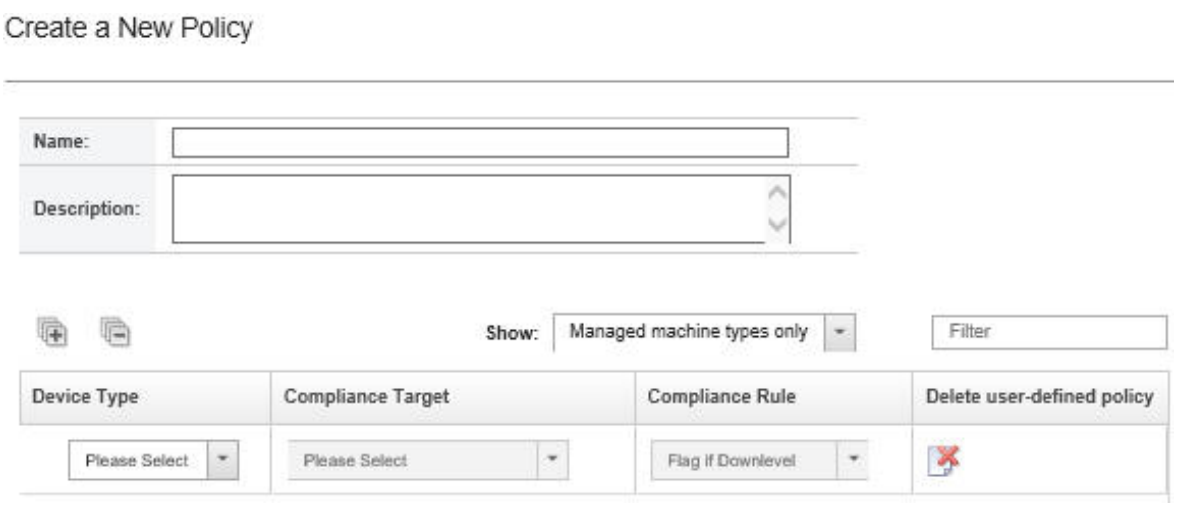
Procedure

To create a firmware-compliance policy, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning** → → **Firmware Updates: Compliance Policies**. The Compliance Policy page is displayed with a list of all existing firmware-compliance policies.



Step 2. Click the **Create** icon ( ) to display the Create a New Policy dialog.



Step 3. Fill in the name and description for the firmware-compliance policy.

Step 4. Fill in the table based on the following criteria for each device:

- **Device Type**. Choose a type of device or component for which this policy is to apply.

  Tip: If you choose a server, the compliance level is done at the UXSP level. However, you can also expand the server to specify specific firmware levels for each component, such as the baseboard management controller or UEFI.

- **Compliance Target**. Specify the compliance target for the applicable devices and subcomponents.

  For servers, you can choose one of the following values.

  – **Default**. Changes the compliance target for each subcomponent to the default value (such as the latest set of firmware in the repository for that device).

  – **Do not update**. Changes the compliance target for each subcomponent to “Do not update.”

  For devices without subcomponents (such as CMMs, switches, or storage devices) or for subcomponents in a server, you can choose one of the following values.

  – *<firmware_level>*. Specifies the baseline firmware level.

  – **Do not update**. Specifies that the firmware is not to be updated. Note that firmware on the backup management controller is not updated by default.

  Note: When you change default values for any subcomponent in a server, the compliance target for that server changes to **Custom**.

- **Compliance Rule**. Specify when a device is flagged as not compliant in the **Installed Version** column on the Firmware Updates: Apply/Activate.

  – **Flag if Downlevel**. If the firmware level that is installed on a device is earlier than the level that is specified in the firmware-compliance policy, the device is flagged as not compliant. For example, if you replace a network adapter in a compute node, and the firmware on that network adapter is earlier than the level identified in the firmware-compliance policy, the compute node is flagged as not compliance.

  – **Flag if Not Exact Match**. If the firmware level that is installed on a device is not an exact match with the firmware-compliance policy, the device is flagged as not compliant. For example, if you replace a network adapter in a compute node, and the firmware on that network adapter is different than the level identified in the firmware-compliance policy, then the compute node is flagged as not compliance.

  – **No Flag**. Devices that are out of compliance are not flagged.

Step 5. Optional: **Optional:** Expand the system type to display each update in the package, and select the firmware level to be used as the compliance target, or select “Do not update” to prevent firmware from being updated on that device.

Step 6. Click **Create**.

The firmware-compliance policy is listed on the Firmware Updates: Compliance Policy page.

What to do next

The firmware-compliance policy is added to the table on the page. The table shows the usage status, origin of the policy (whether user-defined or predefined), and the last modification date.

After you create a firmware-compliance policy, you perform the following actions on a selected firmware-compliance policy:

- Create a duplicate of an existing firmware-compliance policy by clicking the **Copy** icon ( ).
- Rename or edit a firmware-compliance policy by clicking the **Edit** icon ( ).
- Delete the selected firmware-compliance policy by clicking the **Delete policy** icon ( ) or delete the selected firmware-compliance policy and all associated firmware updates that are used only by that policy by clicking the **Delete any policy and firmware packages** icon ( ).You can choose to delete the policy even if it is assigned to a device.

  If the policy is assigned to a device, the policy is unassigned before it is deleted.

  You cannot delete the predefined **Latest Firmware** policy; however, you can disable the policy by clicking the **Global Settings** icon ( ), and then selecting **Disable Latest Firmware Policy**. When this option is selected, the Latest firmware policy is unassigned from managed devices, and the policy is no longer updated to include the latest available versions of firmware in the repository,
- Export firmware-compliance policy that exists in the firmware-updates repository to a local system by selecting the policies and clicking the **Export** icon ( ). You can then import the policies to another XClarity Administrator instance by clicking the **Import** icon ( ).

After you create a firmware-compliance policy, you can assign the policy to a specific device (see Creating firmware-compliance policies) and apply and activate updates for that device (see Applying and activating firmware updates).

Assigning firmware-compliance policies

You must assign a firmware-compliance policy to a device before you can apply and activate firmware updates on the device.

About this task

Lenovo XClarity Administrator supports the following policy assignments.

- **Updates Not Supported**. The device does not support firmware updates; therefore, you cannot assign a firmware-compliance policy
- **No assignment**. A policy is not currently assigned to the device. However, the next time that XClarity Administrator is restarted, the last-edited firmware-compliance policy that can be applied to the device is assigned to that device.
- *<policy_name>*. The specific policy is assigned to the device.

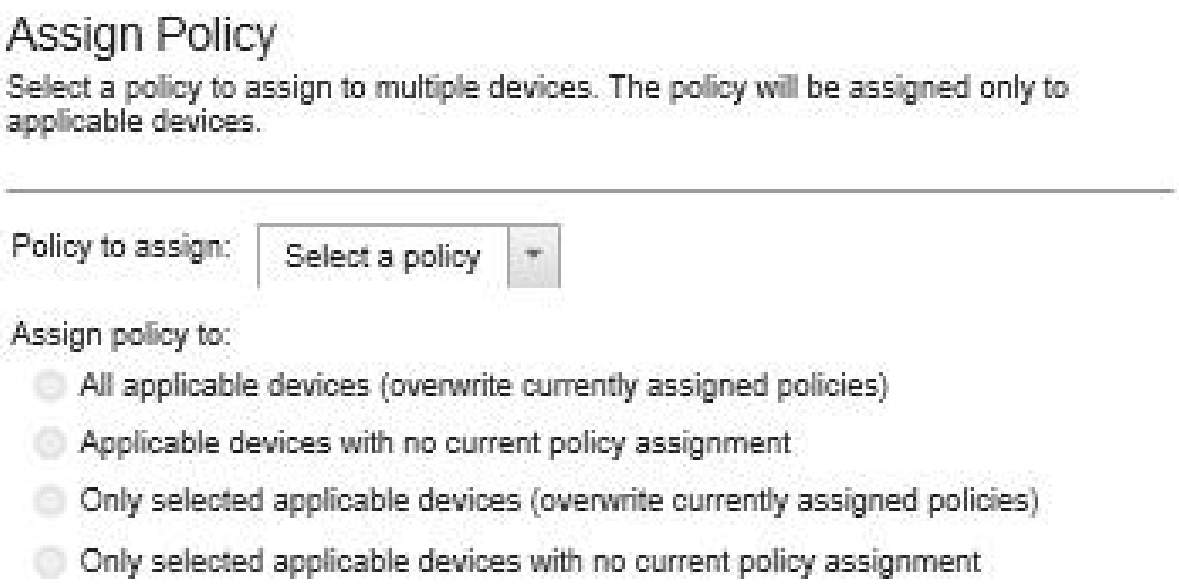
When a device is managed, XClarity Administrator automatically assigns the last-edited firmware-compliance policy that can be applied to that device. You can manually assign a different policy to a device.

Procedure

To assign a firmware-compliance policy to a device, complete the following steps.

- For a single device
  1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed with a list of managed devices.
  2. Select a policy from the drop-down menu in the **Assigned Compliance Policy** column.

     You can only select from a list of firmware-compliance policies that are applicable to each device. If a policy is not currently assigned to the device, the assigned policy is set to "No assignment." If no policies are applicable to the device, the assigned policy is set to "No applicable policies."
- For multiple devices
  1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed with a list of managed devices.
  2. **Optional:** Select one or more devices to which you want to assign a firmware-compliance policy.
  3. Click the **Assign policy** icon ( ) to display the Assign Policy dialog.



  4. Select a firmware-compliance policy from the **Policy to assign** drop-down menu.
  5. Select one of the following scopes for the policy assignment.
     - **All applicable devices**
     - **All applicable devices with no current policy assignment**
     - **Only selected applicable devices**
     - **Only selected applicable devices with no current policy assignment**
  6. Click **OK**. The policy that is listed in the **Assigned Policy** column on the Firmware Updates: Repository page changes to the name of the selected firmware-compliance policy.

Identifying devices that are not compliant

If a firmware-compliance policy has been assigned to a managed device, you can determine whether the firmware on that device is compliant with that policy.

Procedure

To determine whether the firmware on a device is compliant with its assigned firmware-compliance policy, click **Provisioning → Firmware Updates: Apply/Activate** from the Lenovo XClarity Administrator menu bar to display the Firmware Update: Compliance Policy page, and check the **Installed Versions** column for that device.

The **Installed Versions** column contains one of the following values:

- **Firmware version**. The firmware version that is installed on the device is compliant with the assigned policy.
- **Compliant**. The firmware that is installed on the device is compliant with the assigned policy.
- **Not Compliant**. The firmware that is installed on the device is not compliant with the assigned policy.
- **No Compliance Policy Set**. A firmware-compliance policy is not assigned to the device.

You can click the **Refresh** icon () to refresh the content in the **Installed Version** column.

Configuring global firmware-update settings

Global settings serve as defaults settings when firmware updates are applied.

About this task

From the Global Settings page, you can configure the following settings:
- Enhanced support for down-level devices
- Alerts for devices that are not compliant with their assigned policies
- Automatic assignment of a firmware-compliance policy to a device that has no assigned policy
- Non-compliance status for devices with a firmware component that has no associated target in the firmware-compliance policy

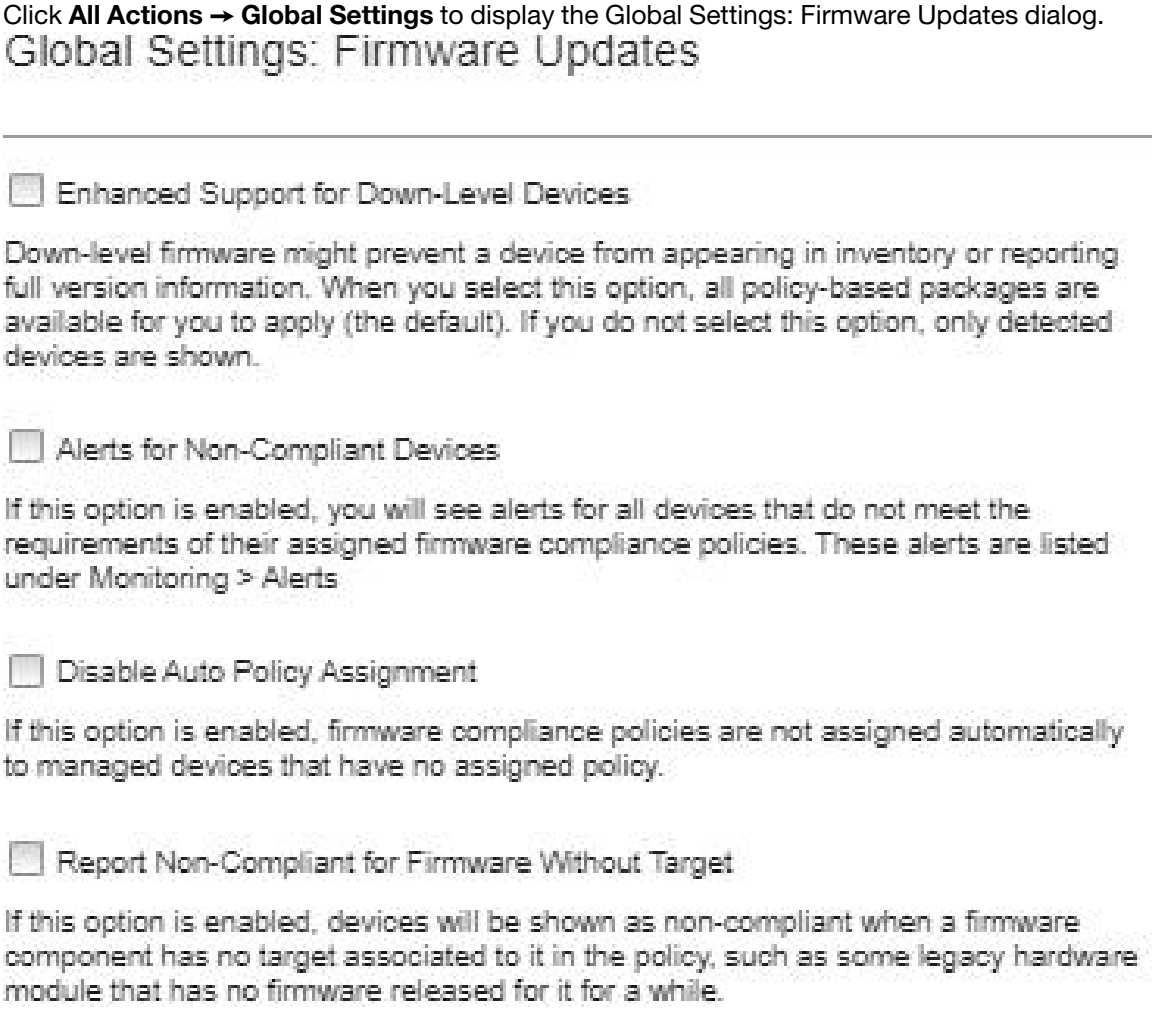
Procedure

To configure the global settings to be used for all servers, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.

Step 2. Click the **Update with Policy** or **Update without Policy** tab.

Step 3. Click **All Actions → Global Settings** to display the Global Settings: Firmware Updates dialog.



Step 4. Optionally select the following options.

- Select **Enhanced Support for Down-Level Devices** to display inventory and full-version information for all devices, even if the firmware is down-level or if the device is missing from the inventory.
- Select **Alerts for Non-Compliance Devices** to display alerts on the Alerts page for devices that do not meet the requirements of their assigned firmware-compliance policies. Alerts are hidden on the Alerts page by default. For more information, see Viewing active alerts.
- Select **Disable auto policy assignment** to disable automatic assignment of a firmware-compliance policy to a device that has no assigned policy. If this option is not selected, firmware compliance policies are assigned to devices without a policy when XClarity Administrator is restarted or when you manage a new device.
- Select **Report Non-Compliance for Firmware Without Target** to flag devices as non-compliant when a firmware component has no associated target in the firmware-compliance policy. If this option is not selected, devices without targets are flagged as compliant.

Step 5. Click **OK** to close the dialog.

Applying and activating firmware updates

Lenovo XClarity Administrator does not automatically apply firmware updates to managed devices. You can choose to apply firmware updates with or without compliance policies.

Before you begin

When using compliance policies, you can schedule updates on multiple devices at the same time. XClarity Administrator updates devices in the correct sequence automatically. The CMM is updated first, followed by switches, servers, and then storage devices.

Only downloaded firmware updates can be applied.

When you perform a firmware update, XClarity Administrator starts one or more jobs to perform the update.

While the firmware update is in progress, the target device is locked. You cannot initiate other management tasks on the target device until the update process is complete.

After a firmware update is applied to a device, one or more restarts might be required to fully activate the firmware update. You can choose whether to restart the device immediately, delay the activation, or prioritize activation. If you choose to restart immediately, XClarity Administrator minimized the number of restarts that are required. If you choose to delay activation, the updates are activated the next time the device is restarted. If you choose prioritized activation, the updates are immediately activated on the baseboard management controller, and all other firmware updates are activated the next time the device is restarted.

You can update selected firmware on a maximum of 50 devices at one time. If you choose to update selected firmware on more than 50 devices, the remaining devices are queued. A queued device is taken off the “selected-firmware update” queue when either the activation completes on an updated device or an updated device is placed in the Pending Maintenance Mode state (if a restart is required on that device). When a device in the Pending Maintenance Mode state is restarted, the device boots into Maintenance Mode and continues the update process, even if the maximum number of firmware updates is already in progress.

You can update bundled-firmware on a maximum of 10 devices at one time. If you choose to update bundled firmware on more than 10 devices, the remaining devices are queued. A queued device is taken off the “bundled-firmware update” queue when the activation completes on a device on which a bundled-firmware update was performed.

Attention: For Red Hat® Enterprise Linux (RHEL) v7 and later, restarting the operating system from a graphical mode suspends the server by default. Before you can perform the **Restart Normally** or **Restart Immediately** actions from XClarity Administrator, you must manually configure the operating system to change the behavior of the power button to power off. For instructions, see the Red Hat Data Migration and Administration Guide: Changing behavior when pressing the power button in graphical target mode.

Note: The XClarity Administrator automatically enables the LAN-over-USB interface.

Applying bundled firmware updates using compliance policies

After Lenovo XClarity Administrator identifies a managed device as not compliant, you can manually apply firmware updates to *all* components in selected ThinkSystem SR635 and SR655 servers that are not compliant with the assigned firmware-compliance policy using a bundled image that contain the applicable firmware update packages. The *bundled image* is created during the update process by collecting all firmware-update packages from the compliance policy.

Before you begin

- Read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).
- Initially, devices that are not supported for updates are hidden from the view. Devices that are not supported cannot be selected for updates.

- By default, all detected components are listed as available for applying updates; however, down-level firmware might prevent a component from appearing in inventory or reporting full-version information. To list all policy-based packages that are available for you to apply updates, click **All Actions → Global Settings**, and selecting **Enhanced Support for Down-Level Devices**. When this option is selected, "Other Available Software" is listed in the Installed Version column for undetected devices. For more information, see Configuring global firmware-update settings.

  Notes:

  – The global settings cannot be changed when updates to managed devices are in progress.

  – It takes a few minutes to generate the additional options. After a few moments, you might need to click the **Refresh** icon () to refresh the table.
- Ensure that no jobs are currently running on the target server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.
- Applying bundled firmware updates is supported only for ThinkSystem SR635 and SR655 servers.
- Ensure that each target device was booted to the OS at least once to retrieve the full inventory information.
- Baseboard management controller firmware v2.94 or later is required to use the bundled-update function.
- Only firmware updates from repository packs or individual firmware updates are used. UpdateXpress System Packs (UXSPs) are not supported.
- Only downloaded firmware updates are applied. Refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.
- Compliance check is supported only for the baseboard management controller and UEFI in ThinkSystem SR635 and SR655 servers; however, XClarity Administrator attempts to apply firmware updates to all available hardware components.
- Updates are applied according to the assigned firmware-compliance policy. You cannot choose to update a subset of components.
- XClarity Administrator v3.2 or later is required to apply firmware updates for Lenovo XClarity Provisioning Manager (LXPM), LXPM windows drivers, or LXPM Linux drivers to ThinkSystem SR635 and SR655 servers.
- The baseboard management controller and UEFI updates are skipped if the currently installed version is higher than the assigned compliance policy.
- Firmware-compliance policies must be created and assigned to the devices on which you intend to apply firmware updates. For more information, see Creating firmware-compliance policies and Assigning firmware-compliance policies.
- The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

Attention: The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.

About this task

The bundled-update process first updates the baseboard management controller and UEFI out of band. When these updates are complete, the process creates a bundled image of remaining firmware in the

compliance policy based on the machine type. Then, the process mounts the image to the selected device and restarts the device to boot the image. The image automatically runs to perform the remaining updates.

You can update bundled-firmware on a maximum of 10 devices at one time. If you choose to update bundled firmware on more than 10 devices, the remaining devices are queued. A queued device is taken off the "bundled-firmware update" queue when the activation completes on a device on which a bundled-firmware update was performed.

If an error occurs while updating a component in the device, the firmware-update process does not update the firmware for that specific component; however, the firmware-update process continues to update the other components in the device and continues to update all other devices in the current firmware-update job.

Procedure

To apply firmware updates in the form of a bundled image on managed devices, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.

Step 2. Click the **Update with Policy** tab.

Step 3. Select one or more devices and components to which firmware updates are to be applied.

You can sort the table columns to make it easier to find specific devices. In addition, you can filter the list of displayed devices by selecting an option in the **Show** menu to list only devices in a specific chassis, rack, or group, by entering text (such as a name or IP address) in the **Filter** field, or by clicking the following icons to list only devices with a specific status.

- **Hide compliant devices** icon ( )
- **Hide non-compliant devices status** icon ( )
- **Hide devices without an assigned compliance policy** icon ( )
- **Hide devices not being monitored** icon ( )
- **Hide devices with firmware pending activation** icon ( )
- **Hide devices with compliance errors** icon ( )
- **Hide devices not supported for updates** icon ( )
- **Hide devices undergoing firmware updates** icon ( )
- **Hide devices with nonstageable firmware** icon ( )

The **Groups** column indicates the groups of which each device is a member. You can hover over the **Groups** column to get a complete list of groups, by group type

The **Installed Version** column indicates the installed firmware version, compliance status, or device status.

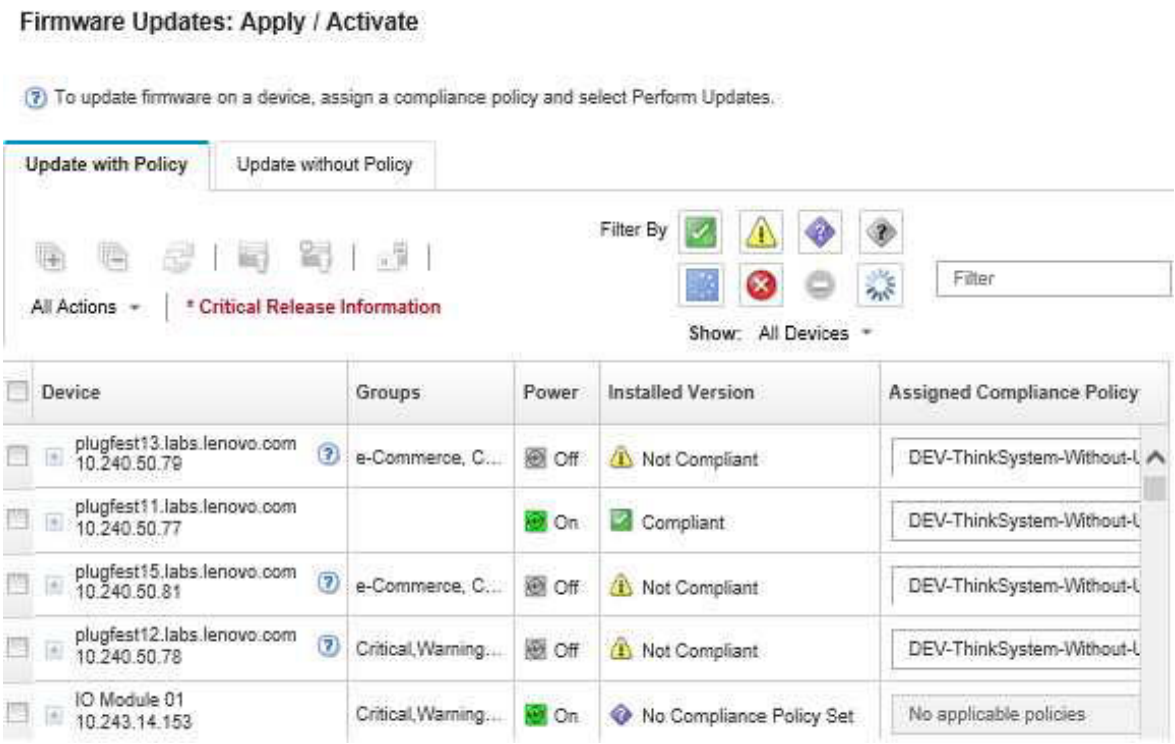
The compliance status can be one of the following:

- **Compliant**
- **Compliance Error**
- **Not Compliant**
- **No Compliance Policy Set**

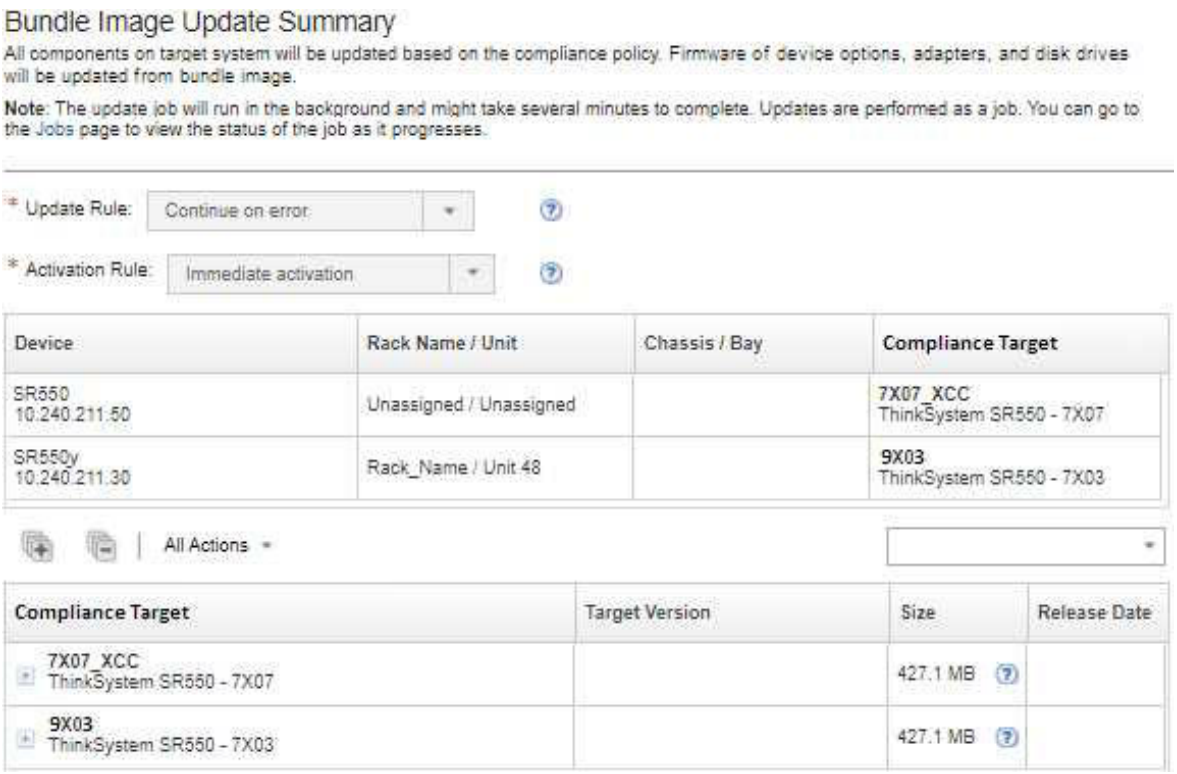
- **Not Monitored**

The device status can be one of the following:

- **Updates Not Supported**
- **Update in Progress**



Step 4. Click the **Perform Update from Bundle Image** icon ( ). The Bundle Image Update Summary dialog is displayed. This dialog lists the selected devices and the firmware updates that are included in the bundled image.



Step 5. Click **Perform Update from Bundle Image** to update immediately, or click **Schedule** to schedule this update to run at a later time.

What to do next

When applying a firmware update, if the server fails to enter maintenance mode, attempt to apply the update again.

If updates were not completed successfully, see Firmware update and repository issues in the XClarity Administrator online documentation for troubleshooting and corrective actions.

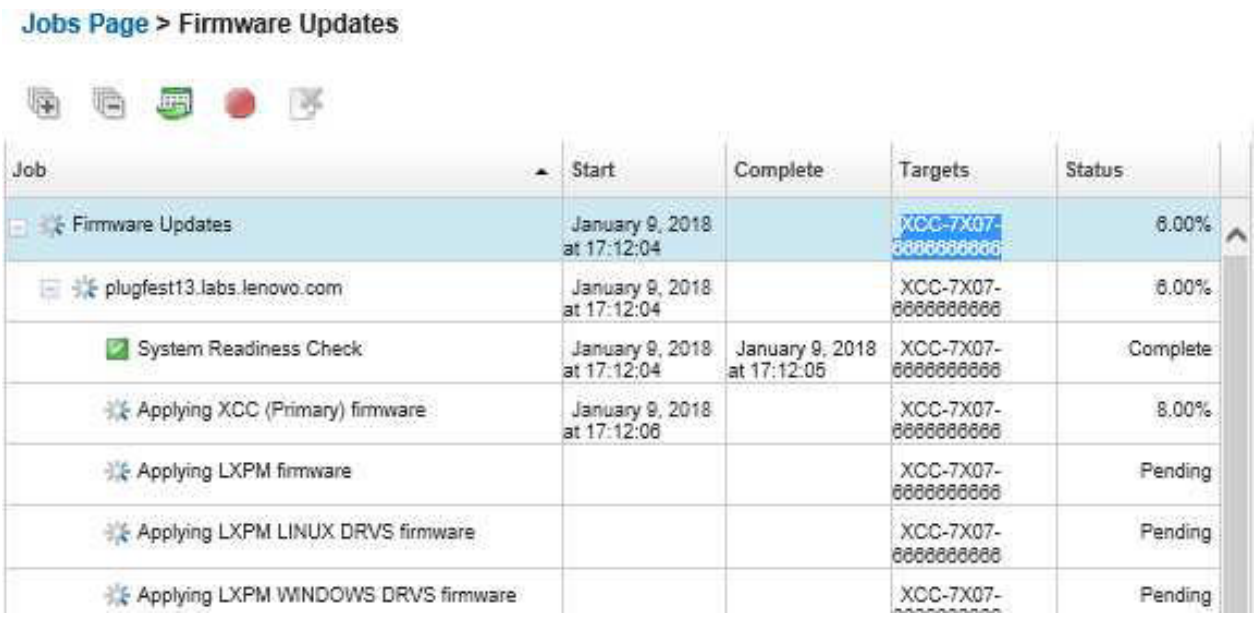
From the Firmware Updates: Apply/Activate page, you can perform the following actions.

- Export firmware and compliance information for each managed device by clicking **All Actions → Export View as CSV**.

  Note: The CSV file contains only filtered information in the current view. Information that is filtered out of the view and information in hidden columns are not included.
- Cancel an update that is being applied to a device by selecting the device and clicking the **Cancel Update** icon ( ).

  Note: You can cancel firmware updates that are in the queue to start. After the update process starts, the firmware update is cancelable only when the update process is performing a task other than applying the update, such as changing to maintenance mode or restarting the device.
- View the status of the firmware update directly from the Apply / Activate page in the **Status** column.
- Monitor the status of the update process from the jobs log. From the Lenovo XClarity Administrator menu, click **Monitoring → Jobs**.

  For more information about the jobs log, see Monitoring jobs .



When the firmware-update jobs are complete, you can verify that the devices are compliant by clicking **Provisioning → Firmware Updates: Apply/Activate** to go back to the Firmware Updates: Apply/Activate page, and then clicking the **Refresh** icon ( ). The current firmware version that is active on each device is listed in the **Installed Version** column.

Applying selected firmware updates using compliance policies

After Lenovo XClarity Administrator identifies a device as not compliant, you can manually apply and activate the firmware updates on these managed devices. You can choose to apply and activate all firmware updates that apply to a firmware-compliance policy or only specific firmware updates in a policy. Only downloaded firmware updates are applied.

Before you begin

- Read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).
- Initially, devices that are not supported for updates are hidden from the view. Devices that are not supported cannot be selected for updates.
- By default, all detected components are listed as available for applying updates; however, down-level firmware might prevent a component from appearing in inventory or reporting full-version information. To list all policy-based packages that are available for you to apply updates, click **All Actions → Global Settings**, and selecting **Enhanced Support for Down-Level Devices**. When this option is selected, “Other Available Software” is listed in the Installed Version column for undetected devices. For more information, see Configuring global firmware-update settings.

  Notes:

  – The global settings cannot be changed when updates to managed devices are in progress.

  – It takes a few minutes to generate the additional options. After a few moments, you might need to click the **Refresh** icon ( ) to refresh the table.
- Ensure that no jobs are currently running on the target server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.
- Ensure that the firmware-updates repository contains the firmware packages that you intend to deploy. If not, refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.

If you intend to install prerequisite firmware, ensure that the prerequisite firmware is downloaded in the repository as well.

In some cases, multiple versions might be needed to update firmware, and all versions would need to be downloaded to the repository. For example, to upgrade the IBM FC5022 SAN scalable switch from v7.4.0a to v8.2.0a, you must first install v8.0.1-pha, then v8.1.1, and then v8.2.0a. All three versions must be in repository to update the switch to v8.2.0a.

- Typically, devices must be restarted to activate the firmware update. If you choose to restart the device during the update process (*immediate activation*), ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.
- For ThinkSystem SR635 and SR655 servers, you can use this traditional update function to apply only baseboard management controller and UEFI firmware updates. Management-controller firmware version AMBT10M or later is required, and UEFI firmware version CFE114L or later is required. To update all components (including the management controller, UEFI, disk drives, and IO options), use the bundle update function (see Applying bundled firmware updates using compliance policies).

About this task

- You can update selected firmware on a maximum of 50 devices at one time. If you choose to update selected firmware on more than 50 devices, the remaining devices are queued. A queued device is taken off the “selected-firmware update” queue when either the activation completes on an updated device or an updated device is placed in the Pending Maintenance Mode state (if a restart is required on that device). When a device in the Pending Maintenance Mode state is restarted, the device boots into Maintenance Mode and continues the update process, even if the maximum number of firmware updates is already in progress.
- You can apply and activate firmware that is later than the currently installed firmware.
- You can choose to apply all updates for a specific device. However, you can also choose to expand a device to specify updates for specific components, such as the baseboard management controller or UEFI.
- If you choose to install a firmware-update package that contains updates for multiple components, all components to which the update package applies are updated.

Procedure

To apply and activate updates on managed devices, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.

Step 2. Click the **Update with Policy** tab.

Step 3. Select one or more devices and devices to which firmware updates are to be applied.

You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed devices by selecting an option in the **Show** menu to list only devices in a specific chassis, rack, or group, by entering text (such as a name or IP address) in the **Filter** field, or by clicking the following icons to list only devices with a specific status.

- **Hide compliant devices** icon ()
- **Hide non-compliant devices status** icon ()
- **Hide devices without an assigned compliance policy** icon ()
- **Hide devices not being monitored** icon ()

- **Hide devices with firmware pending activation** icon ()
- **Hide devices with compliance errors** icon ()
- **Hide devices not supported for updates** icon ()
- **Hide devices undergoing firmware updates** icon ()
- **Hide devices with nonstageable firmware** icon ()

The **Groups** column indicates the groups of which each device is a member. You can hover over the **Groups** column to get a complete list of groups, by group type

The **Installed Version** column indicates the installed firmware version, compliance status, or device status.

The compliance status can be one of the following:

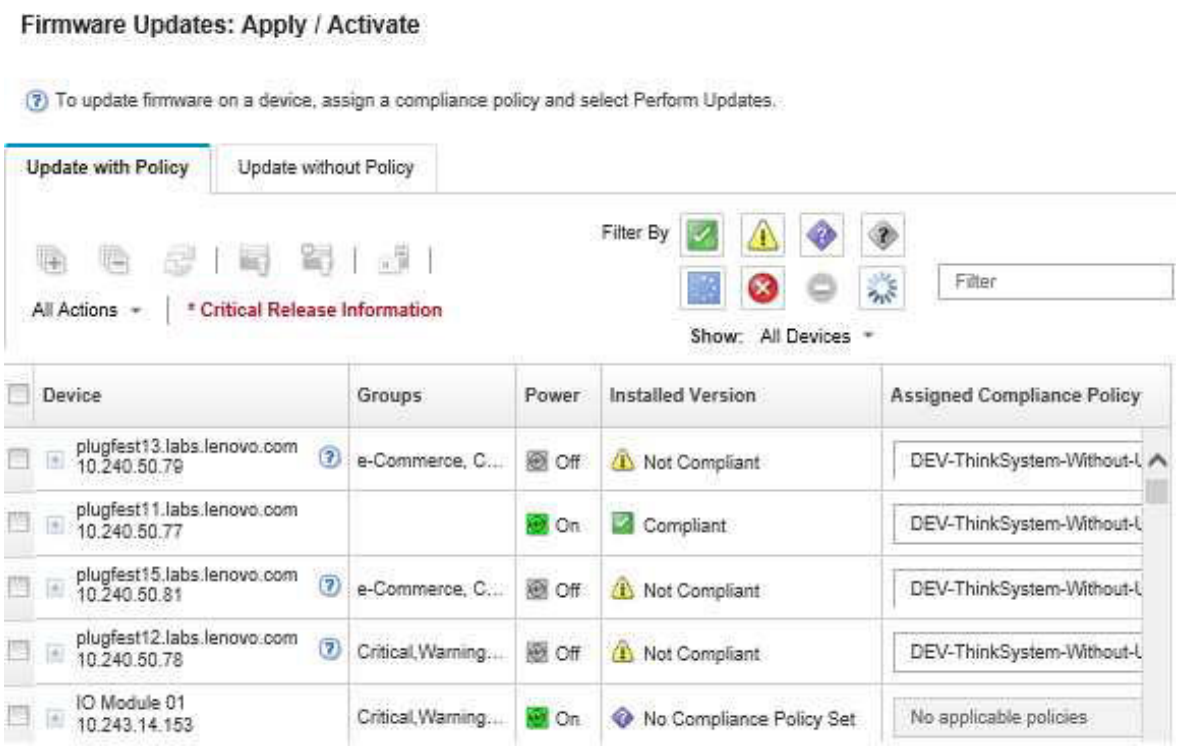
-  **Compliant**
-  **Compliance Error**
-  **Not Compliant**
-  **No Compliance Policy Set**
-  **Not Monitored**

The device status can be one of the following:

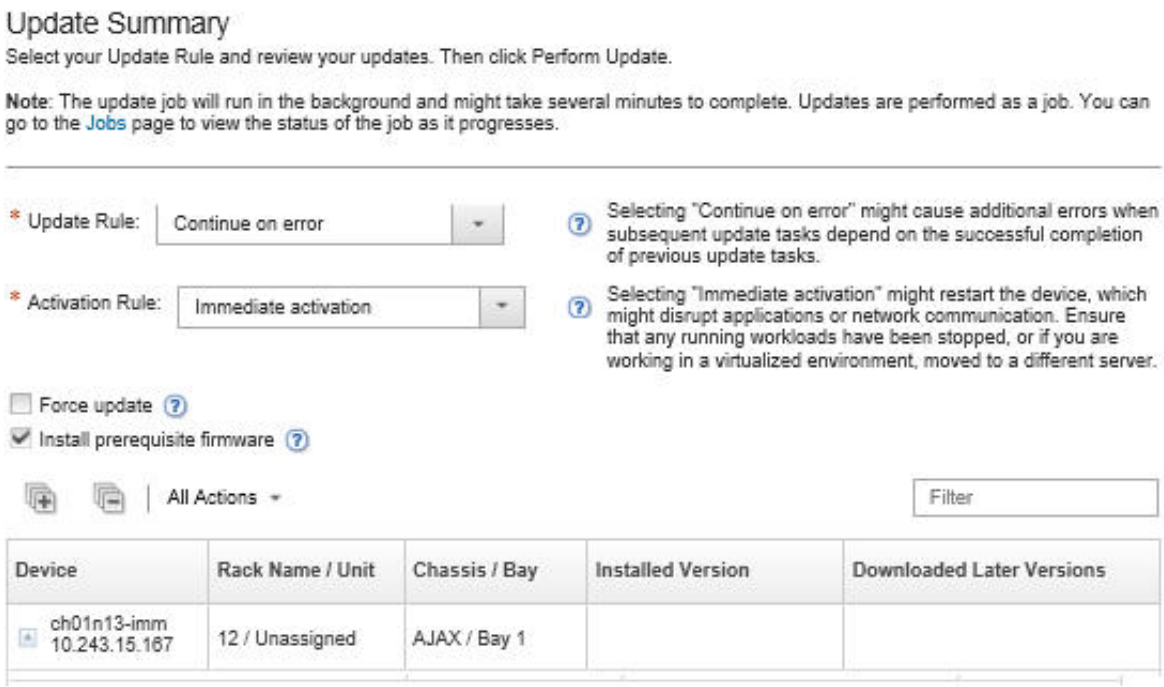
-  **Updates Not Supported**
-  **Update in Progress**

Notes: If the installed firmware version is pending activation, "(Pending Activation)" is appended to the installed firmware version or compliance status of each applicable device, for example "2.20 / A9E12EUS (Pending Activation)." To see the pending-activation status, the following firmware version must be installed on the primary baseboard management controller in the server.

- **IMM2**: TCOO46F, TCOO46E, or later (depending on the platform)
- **XCC**: CDI328M, PSI316N, TEI334I, or later (depending on the platform)



Step 4. Click the **Perform Updates** icon ( ). The Update Summary dialog is displayed.



Step 5. Select one of the following update rules

- **Stop all updates on error**. If an error occurs while updating any of the components (such as an adapter or management controller) in the target device, the firmware-update process stops for all selected devices in the current firmware-update job. In this case, none of the updates in the update package for the device are applied. The current firmware that is installed on all selected systems remains in effect.

- **Continue on error**. If an error occurs while updating any of the devices in the device, the firmware-update process does not update the firmware for that specific device; however, the firmware-update process continues to update the other devices in the device and continues to update all other devices in the current firmware-update job.
- **Continue to next system on error**. If an error occurs while updating any of the devices in the device, the firmware-update process stops all attempts to update the firmware for that specific device, so the current firmware that is installed on that device remains in effect. The firmware-update process continues to update all other devices in the current firmware-update job.

Step 6. Select one of the following activation rules:

- **Immediate activation**. During the update process, the device might be restarted automatically a number of times until the entire update process is complete. Ensure that you quiesce all applications on the device before you proceed.
- **Delayed activation**. Some but not all update operations are performed. Devices must be restarted manually to continue the update process. Additional restarts are then performed until the update operation completes.

  If a device restarts for any reason, the delayed update process completes.

  This rule is supported for only servers and rack switches. CMMs and Flex switches are immediately activated, regardless of this setting.

  Important: Do not choose **Delayed Activation** for more than 50 devices at one time. XClarity Administrator actively monitors devices with delayed activation so that the delayed activation is serviced when device is restarted. If you want to apply updates with delayed activation for more than 50 devices, break the update selection into batches of 50 devices at one time.
- **Prioritized activation**. Firmware updates on the baseboard management controller are activated immediately; all other firmware updates are firmware updates are activated the next time the device is restarted. Additional restarts are then performed until the update operation completes. This rule is supported only for servers.

Note: When enabled, the Wake-on-LAN boot option can interfere with XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.

Step 7. Optional: **Optional:** Clear **Install prerequisite firmware** if you do not want to install prerequisite firmware. Prerequisite firmware is installed by default.

Note: When using **Delayed Activation** or **Prioritized Activation** for prerequisite firmware updates, you might need to restart the server to activate the prerequisite firmware. After the initial restart, the remaining firmware updates are installed using **Immediate Activation**.

Step 8. Optional: **Optional:** Select **Force update** to update firmware on the selected components even if the firmware level is up to date or to apply a firmware update that is earlier than the one currently installed on the selected components.

Note: You can apply earlier version of firmware to device options, adapters, and drives that support down-leveling. See your hardware documentation to determine if down-leveling is supported.

Step 9. Click **Perform Update** to update immediately, or click **Schedule** to schedule this update to run at a later time.

If needed, you can perform power actions on the managed devices. The power actions are useful when **Delayed Activation** is selected and you want the updates to continue when the device is waiting in the “Pending Maintenance” state. To perform a power action on a managed device from this page, click **All Actions → Power Actions**, and then click one of the following power actions.

- **Power on**
- **Power down OS and power off**
- **Power off**
- **Shut down OS and restart**
- **Restart**

What to do next

When applying a firmware update, if the server fails to enter maintenance mode, attempt to apply the update again.

If updates were not completed successfully, see Firmware update and repository issues in the XClarity Administrator online documentation for troubleshooting and corrective actions.

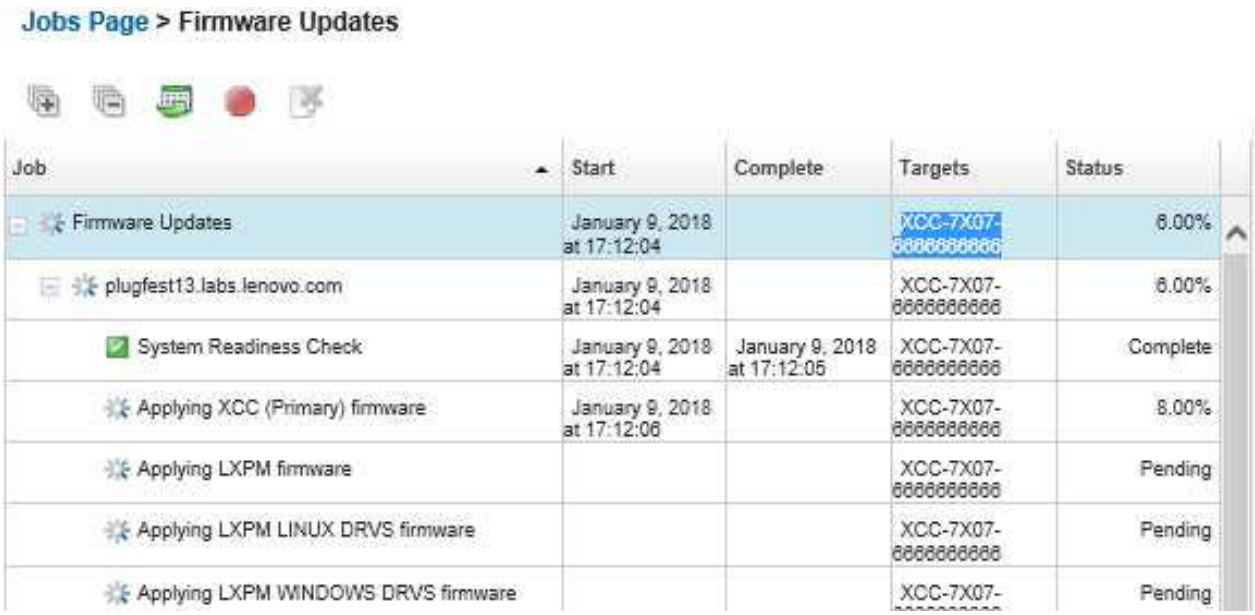
From the Firmware Updates: Apply/Activate page, you can perform the following actions:

- Export firmware and compliance information for each managed device by clicking **All Actions → Export View as CSV**.

  Note: The CSV file contains only filtered information in the current view. Information that is filtered out of the view and information in hidden columns are not included.
- Cancel an update that is being applied to a device by selecting the device and clicking the **Cancel Update** icon ( ).

  Note: You can cancel firmware updates that are in the queue to start. After the update process starts, the firmware update is cancelable only when the update process is performing a task other than applying the update, such as changing to maintenance mode or restarting the device.
- View the status of the firmware update directly from the Apply / Activate page in the **Status** column.
- Monitor the status of the update process from the jobs log. From the Lenovo XClarity Administrator menu, click **Monitoring → Jobs**.

  For more information about the jobs log, see Monitoring jobs .



When the firmware-update jobs are complete, you can verify that the devices are compliant by clicking **Provisioning → Firmware Updates: Apply/Activate** to go back to the Firmware Updates: Apply/Activate

page, and then clicking the **Refresh** icon (). The current firmware version that is active on each device is listed in the **Installed Version** column.

Applying selected firmware updates without using compliance policies

You can quickly apply and activate firmware that is later than the currently installed firmware on a single managed device or group of devices without using compliance policies.

Before you begin

- Read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).
- Initially, devices that are not supported for updates are hidden from the view. Devices that are not supported cannot be selected for updates.
- By default, all detected components are listed as available for applying updates; however, down-level firmware might prevent a component from appearing in inventory or reporting full-version information. To list all policy-based packages that are available for you to apply updates, click **All Actions → Global Settings**, and selecting **Enhanced Support for Down-Level Devices**. When this option is selected, "Other Available Software" is listed in the Installed Version column for undetected devices. For more information, see Configuring global firmware-update settings.

  Notes:

  – The global settings cannot be changed when updates to managed devices are in progress.

  – It takes a few minutes to generate the additional options. After a few moments, you might need to click the **Refresh** icon () to refresh the table.
- Ensure that no jobs are currently running on the target server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.
- Ensure that the firmware-updates repository contains the firmware packages that you intend to deploy. If not, refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.

  If you intend to install prerequisite firmware, ensure that the prerequisite firmware is downloaded in the repository as well.

  In some cases, multiple versions might be needed to update firmware, and all versions would need to be downloaded to the repository. For example, to upgrade the IBM FC5022 SAN scalable switch from v7.4.0a to v8.2.0a, you must first install v8.0.1-pha, then v8.1.1, and then v8.2.0a. All three versions must be in repository to update the switch to v8.2.0a.
- Typically, devices must be restarted to activate the firmware update. If you choose to restart the device during the update process (*immediate activation*), ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

About this task

- You can update selected firmware on a maximum of 50 devices at one time. If you choose to update selected firmware on more than 50 devices, the remaining devices are queued. A queued device is taken off the "selected-firmware update" queue when either the activation completes on an updated device or an updated device is placed in the Pending Maintenance Mode state (if a restart is required on that device). When a device in the Pending Maintenance Mode state is restarted, the device boots into Maintenance Mode and continues the update process, even if the maximum number of firmware updates is already in progress.
- You can apply and activate firmware that is later than the currently installed firmware.

- You can choose to apply all updates for a specific device. However, you can also choose to expand a device to specify updates for specific components, such as the baseboard management controller or UEFI.
- If you choose to install a firmware-update package that contains updates for multiple components, all components to which the update package applies are updated.

Procedure

To apply and activate updates on a managed device, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.

Step 2. Click the **Update without Policy** tab.

Step 3. Select the firmware level in the **Downloaded later versions** column for each device that you want to update.

Step 4. Select one or more devices and devices that you want to update.

You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed devices by selecting an option in the **Show** menu to list only devices in a specific chassis, rack, or group, by entering text (such as a name or IP address) in the **Filter** field, or by clicking the following icons to list only devices with a specific status.

- **Hide components with some later versions** icon ()
- **Hide components with no later versions** icon ()
- **Hide devices not supported for updates** icon ()
- **Hide devices undergoing firmware updates** icon ()
- **Hide devices with nonstageable firmware** icon ()

The **Groups** column indicates the groups of which each device is a member. You can hover over the **Groups** column to get a complete list of groups, by group type

The **Installed Version** column indicates the installed firmware version, compliance status, or device status.

The compliance status can be one of the following:

-  **Compliant**
-  **Compliance Error**
-  **Not Compliant**
-  **No Compliance Policy Set**
-  **Not Monitored**

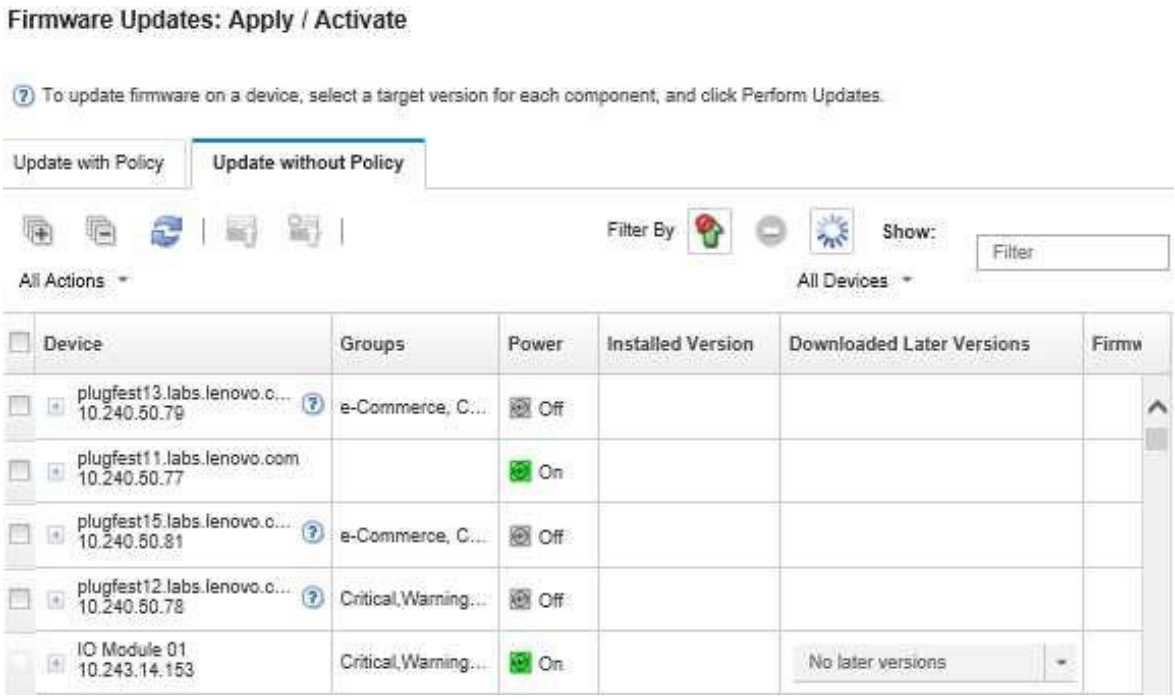
The device status can be one of the following:

-  **Updates Not Supported**
-  **Update in Progress**

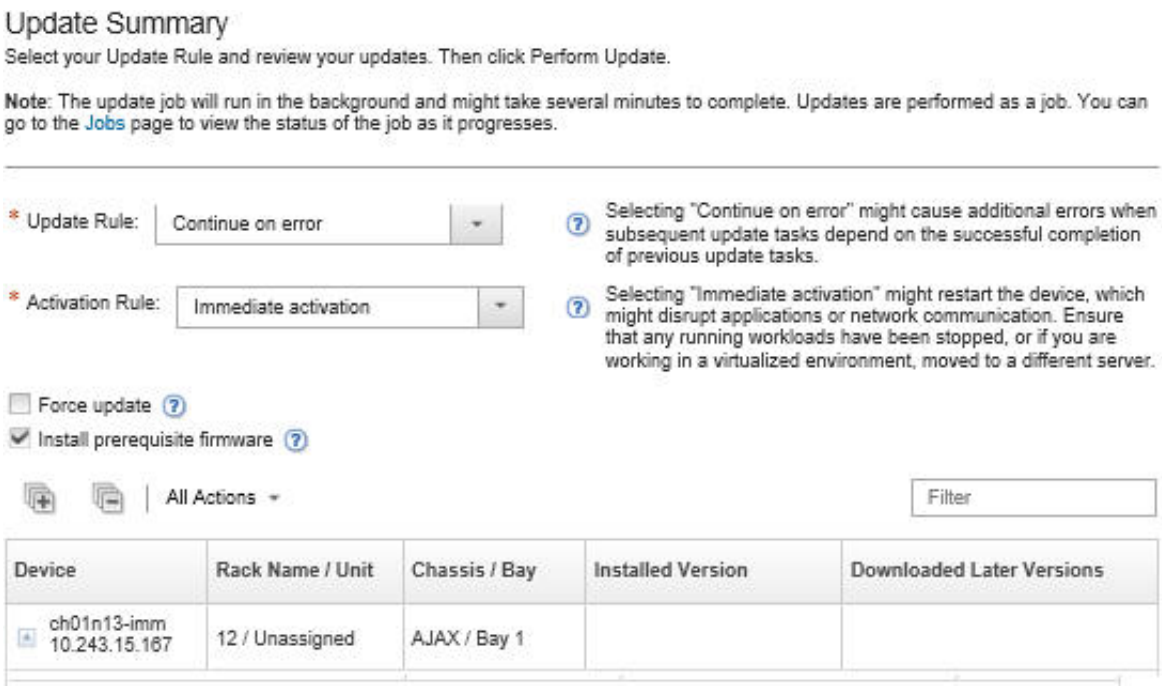
Notes: If the installed firmware version is pending activation, "(Pending Activation)" is appended to the installed firmware version or compliance status of each applicable device, for example "2.20 / A9E12EUS (Pending Activation)." To see the pending-activation status, the following firmware version must be installed on the primary baseboard management controller in the server.

- **IMM2**: TCOO46F, TCOO46E, or later (depending on the platform)

- **XCC**: CDI328M, PSI316N, TEI334I, or later (depending on the platform)



Step 5. Click the **Perform Updates** icon ( ). The Update Summary dialog is displayed.



Step 6. Select one of the following update rules

- **Stop all updates on error**. If an error occurs while updating any of the components (such as an adapter or management controller) in the target device, the firmware-update process stops for all selected devices in the current firmware-update job. In this case, none of the updates in the update package for the device are applied. The current firmware that is installed on all selected systems remains in effect.

- **Continue on error**. If an error occurs while updating any of the devices in the device, the firmware-update process does not update the firmware for that specific device; however, the firmware-update process continues to update the other devices in the device and continues to update all other devices in the current firmware-update job.
- **Continue to next system on error**. If an error occurs while updating any of the devices in the device, the firmware-update process stops all attempts to update the firmware for that specific device, so the current firmware that is installed on that device remains in effect. The firmware-update process continues to update all other devices in the current firmware-update job.

Note: When enabled, the Wake-on-LAN boot option can interfere with XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.

Step 7. Select one of the following activation rules:

- **Immediate activation**. During the update process, the device might be restarted automatically a number of times until the entire update process is complete. Ensure that you quiesce all applications on the device before you proceed.
- **Delayed activation**. Some but not all update operations are performed. Devices must be restarted manually to continue the update process. Additional restarts are then performed until the update operation completes.

  If a device restarts for any reason, the delayed update process completes.

  This rule is supported for only servers and rack switches. CMMs and Flex switches are immediately activated, regardless of this setting.

  Important: Do not choose **Delayed Activation** for more than 50 devices at one time. XClarity Administrator actively monitors devices with delayed activation so that the delayed activation is serviced when device is restarted. If you want to apply updates with delayed activation for more than 50 devices, break the update selection into batches of 50 devices at one time.
- **Prioritized activation**. Firmware updates on the baseboard management controller are activated immediately; all other firmware updates are firmware updates are activated the next time the device is restarted. Additional restarts are then performed until the update operation completes. This rule is supported only for servers.

Step 8. Optional: **Optional:** Clear **Install prerequisite firmware** if you do not want to install prerequisite firmware. Prerequisite firmware is installed by default.

Note: When using **Delayed Activation** or **Prioritized Activation** for prerequisite firmware updates, you might need to restart the server to activate the prerequisite firmware. After the initial restart, the remaining firmware updates are installed using **Immediate Activation**.

Step 9. Optional: **Optional:** Select **Force update** to update firmware on the selected components even if the firmware level is up to date or to apply a firmware update that is earlier than the one currently installed on the selected components.

Note: You can apply earlier version of firmware to device options, adapters, and drives that support down-leveling. See your hardware documentation to determine if down-leveling is supported.

Step 10. Click **Perform Update** to update immediately, or click **Schedule** to schedule this update to run at a later time.

If needed, you can perform power actions on the managed devices. The power actions are useful when **Delayed Activation** is selected and you want the updates to continue when the device is waiting in the “Pending Maintenance” state. To perform a power action on a managed device from this page, click **All Actions → Power Actions**, and then click one of the following power actions.

- **Power on**
- **Power down OS and power off**
- **Power off**
- **Shut down OS and restart**
- **Restart**

What to do next

When applying a firmware update, if the server fails to enter maintenance mode, attempt to apply the update again.

If updates were not completed successfully, see Firmware update and repository issues in the XClarity Administrator online documentation for troubleshooting and corrective actions.

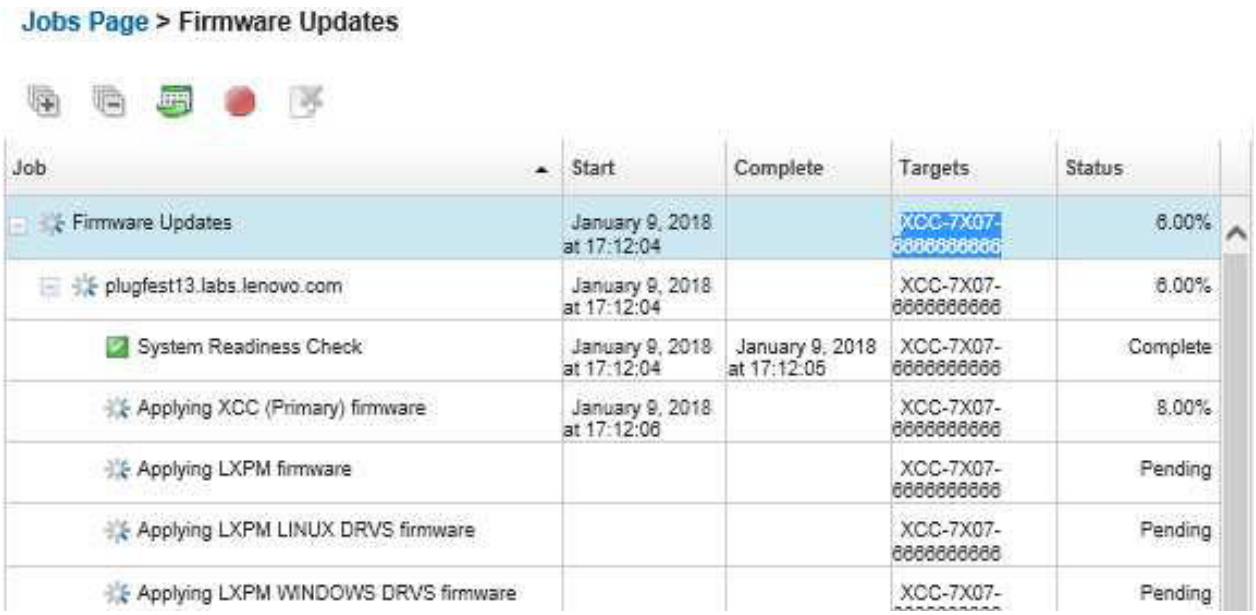
From the Firmware Updates: Apply/Activate page, you can perform the following actions:

- Export firmware and compliance information for each managed device by clicking **All Actions → Export View as CSV**.

  Note: The CSV file contains only filtered information in the current view. Information that is filtered out of the view and information in hidden columns are not included.
- Cancel an update that is being applied to a device by selecting the device and clicking the **Cancel Update** icon ( ).

  Note: You can cancel firmware updates that are in the queue to start. After the update process starts, the firmware update is cancelable only when the update process is performing a task other than applying the update, such as changing to maintenance mode or restarting the device.
- View the status of the firmware update directly from the Apply / Activate page in the **Status** column.
- Monitor the status of the update process from the jobs log. From the Lenovo XClarity Administrator menu, click **Monitoring → Jobs**.

  For more information about the jobs log, see Monitoring jobs .



When the firmware-update jobs are complete, you can verify that the devices are compliant by clicking **Provisioning → Firmware Updates: Apply/Activate** to go back to the Firmware Updates: Apply/Activate

page, and then clicking the **Refresh** icon (). The current firmware version that is active on each device is listed in the **Installed Version** column.

Updating Windows device drivers on managed servers

Using windows UpdateXpress System Packs (UXSPs), you can update OS device drivers on deployed Windows operating systems.

Before you begin

You must have **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** or **lxc-hw-admin** authority to manage and deploy OS device drivers and to perform power actions on managed servers from the Windows Driver Updates pages.

About this task

Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows.

Only device drivers for Windows Server 2012 R2 and later are supported.

For information about installing device drivers when deploying operating systems, see Installing operating systems on bare-metal servers.

Procedure

Step 1. **Configuring Windows Server for OS device-driver updates**

Lenovo XClarity Administrator uses the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems. The WinRM service must be correctly configured on the target servers before attempting to update OS device drivers (see Configuring Windows Server for OS device-driver updates).

Step 2. **Manage the OS device-driver repository**

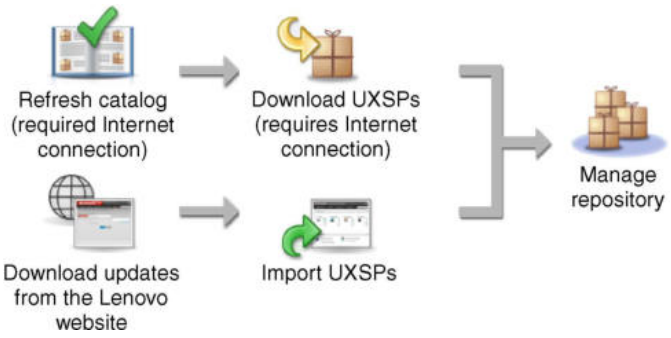
The *OS device-driver repository* includes the catalog and downloaded Windows device drivers.

The *catalog* contains information about all Windows UXSPs and device-driver updates that are available for all Lenovo servers that support Windows. When you refresh the catalog, XClarity Administrator retrieves information about the available UXSPs from the Lenovo Data Center Support website (including the metadata .xml and readme .txt files) and stores the information to the repository. The payload file (.exe) is not downloaded. For more information about refreshing the catalog, see Refreshing the OS device-driver catalog.

Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. You can download or import Windows UXSPs in the repository. UXSPs must be available in the repository before you can update Windows device drivers on managed severs. For more information about downloading device drivers, see Downloading Windows device drivers .

XClarity Administrator must be connected to the Internet to refresh the catalog and download UXSPs. If it is not connected to the Internet, you can manually download the UXSPs to a workstation that has network access to the XClarity Administrator host using a web browser. This UXSPs download is a zip format file and contains all the required device driver files for the UXSP, including the payload (.exe), metadata (.xml), and change history file (.chg), and readme files (.txt).

Note: You might see messages that the firmware (fw) files are not needed and have been removed. This is normal, because only windows device drivers are updated using this process.



Attention:

- Do not unzip the UXSP before importing the it.
- The Windows UXSPs include device drivers and firmware updates. The firmware updates in the Windows UXSPs are discarded when the UXSPs are imported to the repository and a warning message displayed. Only the device drivers are imported.

Step 3. **Applying OS device drivers**

XClarity Administrator does not automatically update device drivers to managed servers. To update device drivers, you must manually apply the device drivers on selected servers.

Attention: Before you attempt to update device drivers on managed servers, ensure that you reviewed the following considerations and completed any applicable prerequisite actions.

- Devices that are not supported cannot be selected for updates.
- Read the device-driver update considerations before you attempt to update device drivers on your managed servers (see OS device-driver update considerations).
- Ensure that the repository contains the UXSPs and device drivers that you intend to deploy (see Downloading Windows device drivers).

  Note: When XClarity Administrator is initially installed, the catalog and repository are empty.
- XClarity Administrator can use the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems HTTPS is the default. To use HTTP, click **All Actions → Global Settings** on the Windows Driver updates: Apply page, and then clear **Use HTTPS for Windows driver updates**.

  Attention: When using HTTP, Windows user credentials are sent over the network *without* encryption and can be easily viewed using commonly available network troubleshooting tools.

  Important:

  – Ensure that Windows Remote Management (WinRM) on the target server is configured to use the same setting (HTTPS or HTTP) that is defined in XClarity Administrator (see Configuring Windows Server for OS device-driver updates).
  – Ensure that WinRM on the target server is configured with basic authentication.
  – When using HTTPS, ensure that WinRM on the target server is configured with **allowUnencrypted=false**.
- Ensure that PowerShell is supported on the target server.

- Ensure that the target server is powered on before attempting to update device drivers. If the server is not powered on, select the target server, and click **All Actions → Power Actions → Power On**.
- Ensure that XClarity Administrator has information that it needs to access the host operating system (see Managing access to operating-systems on managed servers.
- If you want to use a domain account when updating OS device drivers, ensure that you created the required configuration file (see).
- Ensure that no jobs are currently running on the target server. You cannot update device drivers on a managed server that is locked by a running job. If another update job is running on the target server, this update job is queued until the current update job completes. To see a list of active jobs, click **Monitoring → Jobs**.

For more information about updating device drivers, see Applying Windows device drivers.

OS device-driver update considerations

Before you begin updating OS device drivers for managed devices by using Lenovo XClarity Administrator, review the following important considerations.

Note: You must have **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** or **lxc-hw-admin** authority to manage and deploy device drivers and to perform power actions on managed servers from the Windows Driver Updates pages.

Network considerations

- Required ports and Internet addresses must be available before you attempt to download UpdateXpress System Packs (UXSPs). For more information, see Port availability and Firewalls and proxy servers in the XClarity Administrator online documentation.
- XClarity Administrator must have access to management and data network to access the operating system.
- XClarity Administrator must be able to communicate with the target server (both the baseboard management controller and the server's data network) over the network interface (Eth0 or Eth1) that was selected when you configured the XClarity Administrator network access and that the interface is configured with an IPv4 address or an IPv6 auto ULA address.

  To specify an interface to be used for operating-system deployment, see Configuring network access).

  For more information about the operating-system deployment network and interfaces, see Network considerations in the XClarity Administrator online documentation.
- IP addresses must be are unique for the host operating system.
- XClarity Administrator can use the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems HTTPS is the default. To use HTTP, click **All Actions → Global Settings** on the Windows Driver updates: Apply page, and then clear **Use HTTPS for Windows driver updates**.

  Attention: When using HTTP, Windows user credentials are sent over the network *without* encryption and can be easily viewed using commonly available network troubleshooting tools.

Managed-device considerations

- For ThinkSystem SR635 and SR655 servers, updating Windows device drivers is not supported.
- Only ThinkSystem, Lenovo System x, and Lenovo Flex System servers are supported.
- XClarity Administrator does not validate the relationship between the management controller and operating system. The baseboard management controller is used to power on or off the server.

- Ensure that the LAN-over-USB interface is enabled. LAN-over-USB is used when updating OS device drivers.

Operating-system and device-driver considerations

- You can update device drivers for the following operating systems.
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

  Note: XClarity Administrator is tested with only Windows versions that are supported by Microsoft at the time when the XClarity Administrator version was released.
- Windows Remote Management (WinRM) must be configured for HTTPS on the target server (see Configuring Windows Server for OS device-driver updates).
- PowerShell must be supported on the target server.
- You must provide information that is needed to access the host operating system on the target server, including the OS IP address and credentials (see Managing access to operating-systems on managed servers). You must provide credentials for a user account that has administrator authority.
- XClarity Administrator updates only device drivers that are out of compliance. Device drivers are out of compliance when the version on the server is earlier than version in the selected UXSP. Device drivers that are equal to or later than version in the selected UXSP are skipped.
- Device-driver compliance is accurate only when hardware is present. If hardware is not present, device drivers are still applied to the server. When the missing hardware is added to the server, Windows loads the latest version.
- System x servers do not support some predefined device drivers that come with XClarity Administrator. To deploy device drivers to these servers, create a custom profile that includes only the needed device drivers.

Managing the OS device-drivers repository

The *OS device-driver repository* includes the catalog and downloaded Windows device drivers.

About this task

The *catalog* contains information about all Windows UXSPs and device-driver updates that are available for all Lenovo servers that support Windows. When you refresh the catalog, XClarity Administrator retrieves information about the available UXSPs from the Lenovo Data Center Support website (including the metadata .xml and readme .txt files) and stores the information to the repository. The payload file (.exe) is not downloaded. For more information about refreshing the catalog, see Refreshing the OS device-driver catalog.

Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. You can download or import Windows UXSPs in the repository. UXSPs must be available in the repository before you can update Windows device drivers on managed severs.For more information about downloading device drivers, see Downloading Windows device drivers .

XClarity Administrator must be connected to the Internet to refresh the catalog and download UXSPs. If it is not connected to the Internet, you can manually download the UXSPs to a workstation that has network access to the XClarity Administrator host using a web browser. This UXSPs download is a zip format file and contains all the required device driver files for the UXSP, including the payload (.exe), metadata (.xml), and change history file (.chg), and readme files (.txt).

After a UXSP is downloaded in the repository, information about each device driver in the pack is added to the Windows Driver Updates Repository page. This includes the release date, size, and severity. The severity indicates the impact and the need to apply the update to help you to assess how your environment might be affected.

- **Initial Release**. This is the first release of the device driver.
- **Critical**. The device driver contains urgent fixes for data corruption, security, or stability issues.
- **Suggested**. The device driver contains significant fixes for problems that you are likely to encounter.
- **Non-Critical**. The device driver contains minor fixes, performance enhancements, and textual changes.

Notes:

- The severity is relative to the previously released version of the device driver. For example, if the installed device driver is v1.01, and update v1.02 is Critical, and update v1.03 is Recommended, this means that the update from 1.02 to 1.03 is recommended, but the update from v1.01 to v1.03 is critical because it is cumulative (v1.03 includes v1.02 critical issues).
- Special cases might arise where an update is only critical or recommended for a specific machine type. Refer to the Release Notes for additional information.

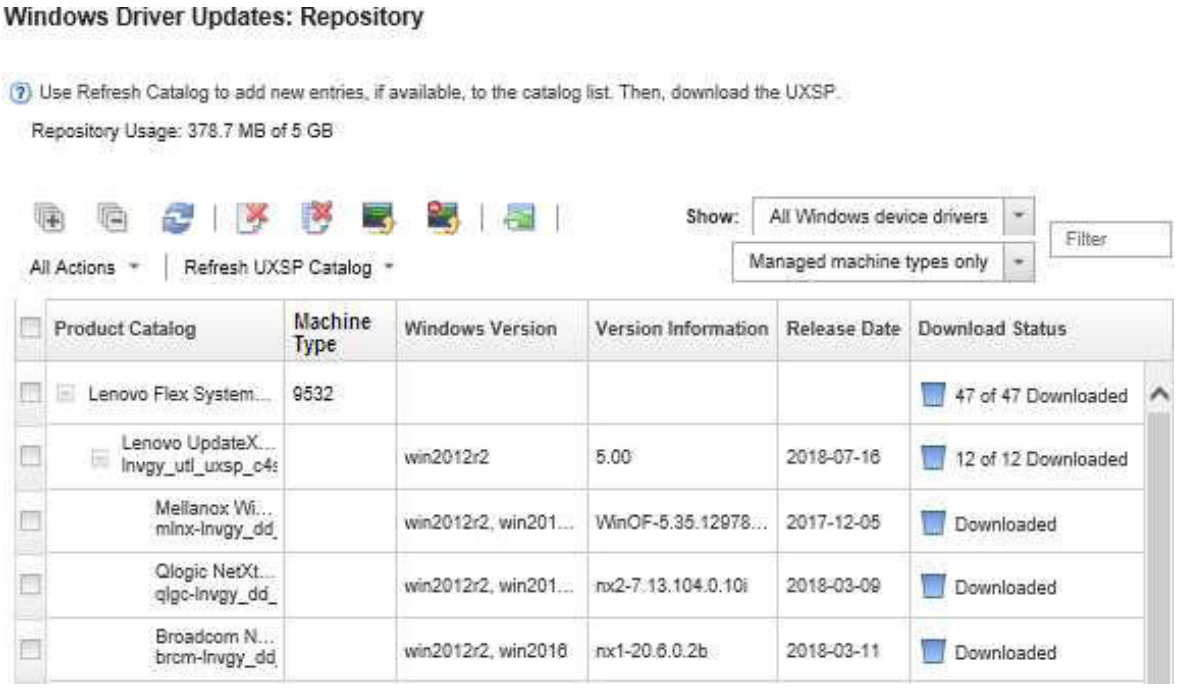
Procedure

To view UXSPs and device drivers that are available in the repository, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Repository**. The Windows Driver Updates Repository page is displayed with a list of available UXSPs, organized by device type.

Step 2. Expand a server type, and then expand the UXSPs that are available for that server type to list the device drivers that are available for that server type.

You can sort the table columns and click the **Expand** all icon ( ) and **Collapse** all icon ( ) to make it easier to find specific device drivers. In addition, you can filter the list of displayed server types and device drivers by selecting an option in the **Show** menu to list only device drivers of a specific age, device drivers for all server types or only managed-server types or by entering text in the **Filter** field.



From this page, you can perform the following actions:

- Retrieve the latest information about available UXSPs by clicking **Refresh Catalog**.

  Retrieving this information might take several minutes to complete. For more information, see Refreshing the OS device-driver catalog.
- Download UXSPs and device drivers using XClarity Administrator by refreshing the catalog and then clicking the **Download** icon (). When the UXSPs and device drivers are downloaded and added to the repository, the status changes to "Downloaded."

  For more information about downloading UXSPs and device drivers, see Downloading Windows device drivers .
- Import UXSPs that you manually downloaded to a workstation from the web or device drivers that you exported from XClarity Administrator (see Downloading Windows device drivers).
- Stop selected downloads that are currently in progress by clicking the **Cancel Downloads** icon ().
- Delete selected UXSPs or individual device drivers from the repository by clicking the **Delete** icon ().

Refreshing the OS device-driver catalog

The OS device-driver catalog contains information about all Windows UpdateXpress System Packs (UXSPs) and device drivers that are available for all Lenovo servers that support Windows device driver updates.

Before you begin

Ensure that Lenovo XClarity Administrator is connected to the Internet.

About this task

When you refresh the catalog, XClarity Administrator retrieves information about the available UXSPs from the Lenovo Data Center Support website (including the metadata .xml and readme .txt files) and stores the information to the repository. The payload file (.exe) is not downloaded. You must download the desired UXSP and OS device-driver payloads before updating device drivers on managed servers. For more information about downloading device drivers, see Downloading Windows device drivers .

Note: Refreshing the catalog might take several minutes to complete.

Procedure

To refresh the catalog, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Repository** to display the Windows Driver Updates Repository page.

Step 2. Click **Refresh Catalog**, and then click one of the following options to obtain information about the latest available UXSPs.

- **Refresh Selected - Latest Only**. Retrieves information about the most current UXSP versions that are available for only the selected servers.
- **Refresh All - Latest Only**. Retrieves information about the most current UXSP versions for all supported servers.
- **Refresh Selected**. Retrieves information about all UXSP versions that are available for only the selected servers.
- **Refresh All**. Retrieves information about all UXSP versions that are available for all supported servers.

Step 3. Click **Refresh Catalog** to refresh immediately, or click **Schedule** to schedule this refresh to run at a later time.

Downloading Windows device drivers

Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. You can download or import Windows UXSPs in the repository. UXSPs must be available in the repository before you can update Windows device drivers on managed severs.

Before you begin

Ensure that all required ports and Internet addresses are available before you attempt to download UpdateXpress System Packs (UXSPs). For more information, see Port availability and Firewalls and proxy servers in the XClarity Administrator online documentation.

To download UXSPs using XClarity Administrator, ensure that XClarity Administrator is connected to the Internet.

Internet Explorer and Microsoft Edge web browsers have an upload limit of 4 GB. If the file that you are importing is greater than 4 GB, consider using another web browser (such as Chrome or Firefox).

About this task

XClarity Administrator must be connected to the Internet to refresh the catalog and download UXSPs. If XClarity Administrator is not connected to the Internet, you can manually download the files to a workstation that has network access to the XClarity Administrator host using a web browser and then import the updates into the firmware-updates repository.

You can determine whether UXSPs are stored in the repository from the **Download Status** column on Windows Driver Updates Repository page. This column contains the following values:

- **Downloaded**. All device drivers in the UXSP or the individual device driver is downloaded in the repository.
- *x* **of** *y* **Downloaded**. Some but not all device drivers in the UXSP are downloaded in the repository. The numbers in parentheses indicate the number of available device drivers and the number of download device drivers.
- **Not Downloaded**. The UXSP or individual device driver is available on the Lenovo Support site but not downloaded in the repository.

A message is displayed on the Windows Driver Updates Repository page when the space that is available for UXSPs and device drivers is more than 50% full. Another message is displayed on the page when the repository is more than 85% full. To reduce the space that is used in the repository, you can remove unused files by selecting the target files and then clicking the **Delete** icon ( ). For more information, see Managing disk space.

Attention: The Windows UXSPs include device drivers and firmware updates. The firmware updates in the Windows UXSPs are discarded when the UXSPs are imported to the repository and a warning message displayed. Only the device drivers are imported.

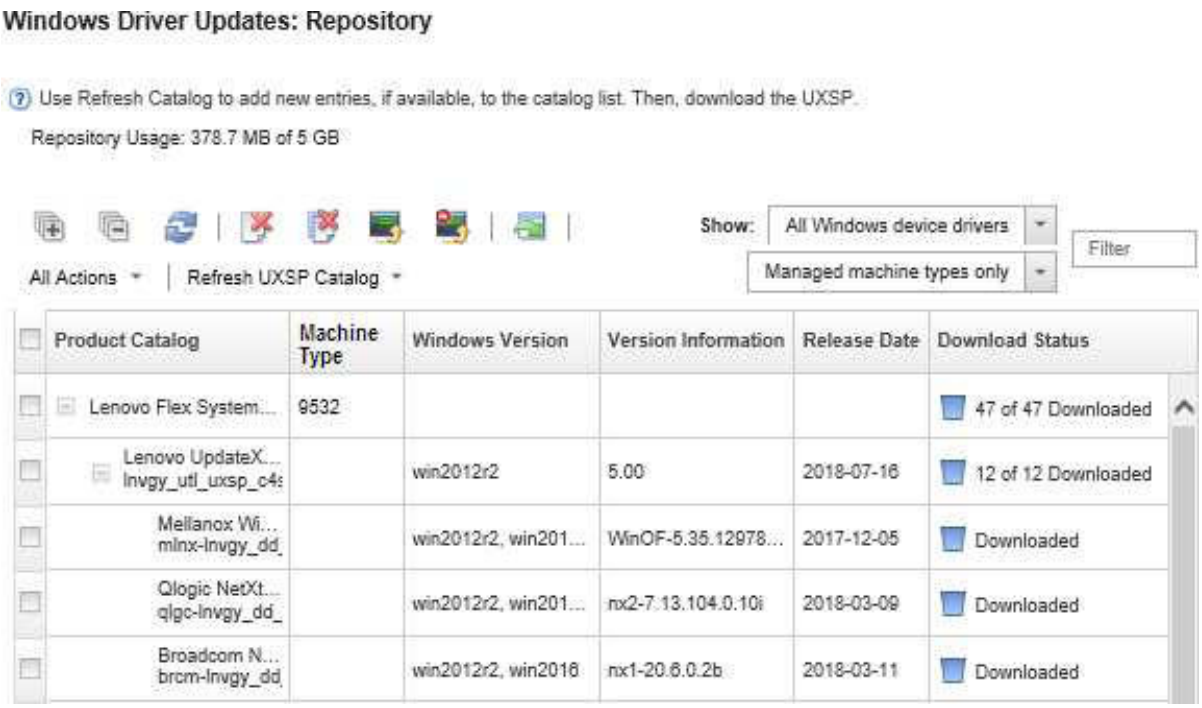
Procedure

To download UXSPs and specific device drivers, perform one of the following procedures.

- When XClarity Administrator is connected to the Internet:
  1. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Repository** to display the Windows Driver Updates Repository page.

2. Click **Refresh Catalog**, and then click one of the following options to obtain information about the latest available UXSPs.
   - **Refresh Selected - Latest Only**. Retrieves information about the most current UXSP versions that are available for only the selected servers.
   - **Refresh All - Latest Only**. Retrieves information about the most current UXSP versions for all supported servers.
   - **Refresh Selected**. Retrieves information about all UXSP versions that are available for only the selected servers.
   - **Refresh All**. Retrieves information about all UXSP versions that are available for all supported servers.

   Note: Refreshing the catalog might take several minutes to complete.
3. Expand the server type to display the list of available UXSPs. Expand the UXSP to see a list of available device drivers.



4. Select one or more target UXSPs and device drivers to download.
5. Click the **Download Selected** icon ( ).
6. Click **Download** to download immediately, or click **Schedule** to schedule this download to run at a later time.

   Downloading the UXSPs might take a few minutes. When the UXSPs and device drivers have been downloaded and stored in the repository, the row in the catalog is highlighted, and the **Download Status** column is changed to "Downloaded."

   You can monitor the status of the download process from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**. For more information about the jobs log, see Monitoring jobs.

- When XClarity Administrator *is not* connected to the Internet:
  1. Download the UXSPs to a workstation that has network connection to the XClarity Administrator host from the Lenovo Data Center Support website.

2. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Repository** to display the Windows Driver Updates Repository page.
3. Click the **Import** icon ().
4. Click **Select Files**, and browse to the location of the UXSP on the workstation.
5. Select the UXSP .zip file (do not unzip the zip file before importing), and then click **Open**.

   The UXSP .zip file contains the metadata file (.xml), payload (.exe), change history file (.chg), and readme file (.txt).
6. Click **Import**.

   You can monitor the status of the import process from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**. For more information about the jobs log, see Monitoring jobs.

What to do next

From this page, you can perform the following actions on selected UXSPs.

- Cancel a download that is currently in process by clicking the **Cancel download** icon ().
- Delete all file associated with the UXSP by clicking the **Delete** icon ().

Configuring Windows Server for OS device-driver updates

Lenovo XClarity Administrator uses the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems. The WinRM service must be correctly configured on the target servers before attempting to update OS device drivers.

Before you begin

Required ports must be available. For more information, see Port availability in the XClarity Administrator online documentation.

For more information about configuring Windows Server before updating OS device driver, see the XClarity Administrator: Preparing for OS Device Driver Updates (white paper).

Procedure

To configure Windows Server to support updating OS device drivers, complete the following steps.

- **For HTTPS**
  1. Sign and install a server certificate on each of your target Windows systems.

     Important: The certificate must contain the following information.

     – In the Subject, ensure that the Domain Component is set (for example, DC=labs, DC=com, DC=company).

     – In the Subject Alternative Name, ensure that the DNS Name and host IP Address are set (for example, DNS Name=node1325C554A6F.labs.company.com and IP Address=10.245.43.149).
  2. Configure the remote management commands and data over an HTTPS connection by running one of the following commands from an administrative command prompt, and then confirm the suggested configuration changes.

     –
     ```
     winrm quickconfig -transport:https
     ```
     –

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
@{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
```

To manually set up a WinRM HTTPS listener according to WinRM documentation, see the How to configure WinRM for HTTPS webpage.

3. Enable basic authentication of local Windows users by running the following command from an administrative command prompt.
   ```
   winrm set winrm/config/service/Auth @{Basic="true"}
   ```
4. To avoid a possible timeout and sending WinRM request errors in compliance checking and performing driver updates, increase the default value for the WinRM response timeout by running the following command from an administrative command prompt. A value of 280000 is recommended. For more information, see the Installation and Configuration for Windows Remote Management webpage.
   ```
   winrm set winrm/config @{MaxTimeoutms="280000"}
   ```
5. Open the port in your firewall that you configured for the WinRM HTTPS listener. The default HTTPS port is 5986. For example
   ```
   netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow
   protocol=TCP localport=5986
   ```
6. If you are using HTTPS listeners, adds the certificate to the XClarity Administrator trust store by completing the following steps. Adding the certificate to the trust store allows XClarity Administrator to trust the WinRM HTTPS listeners to which it connects. Repeat the following steps for any additional certification paths that need to be trusted for the Windows Remote Management service.
   a. Identify and collect the Certificate Authority root certificate that you used to sign the server certificates for the target Windows systems. If you do not have access to the CA root certificate, collect the server certificate itself or another certificate in the certification path.
   b. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.
   c. Click **Trusted Certificates** under the Certificate Management section.
   d. Click the **Create** icon ( ) to display the Add Certificate dialog.
   e. Either browse for the certificate file that you collected in step 1, or copy/paste the contents of the certificate file into the text box.
   f. Click **Create**.
7. After the WinRM listener is running on your target Windows systems, XClarity Administrator can connect to these systems and perform the device driver updates.

- **For HTTP**
  1. Configure the remote management commands and data over an HTTP connection by running the following command from an administrative command prompt, and then confirm the suggested configuration changes.
     ```
     winrm quickconfig
     ```
  2. Enable basic authentication of local Windows users by running the following command from an administrative command prompt.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  3. Allocate enough memory for the update commands on this system by running the following command from an administrative command prompt.
     ```
     winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
     ```
  4. Allow unencrypted data by running the following command from an administrative command prompt.
     ```
     winrm set winrm/config/service @{AllowUnencrypted="true"}
     ```
  5. Open the port in your firewall that you configured for the WinRM HTTP listener. The default HTTPS port is 5985. For example
     ```
     netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow
     protocol=TCP localport=5985
     ```

After the WinRM listener is running on your target Windows systems, XClarity Administrator can connect to these systems and perform the device driver updates.

Configuring global Windows device-driver update settings

Global settings serve as defaults settings when Windows device-driver updates are applied.

About this task

From the Global Settings page, you can configure the following settings:
- Use HTTPS for Windows driver updates
- Show Device Drivers for installed hardware

Procedure

To configure the global settings to be used for all servers, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Apply**. The Windows Driver Updates: Apply page is displayed.

Step 2. Click **All Actions → Global Settings** to display the Global Settings: Apply Windows driver updates dialog.



Step 3. Optionally select the following options.

- Select **Use HTTPS for Windows driver updates** to use the Windows Remote Management service (WinRM) listening over HTTPS to run device-driver update commands on target Windows systems HTTPS is the default.

  Clear this setting to use HTTP.

  Attention: When using HTTP, Windows user credentials are sent over the network *without* encryption and can be easily viewed using commonly available network troubleshooting tools.
- Select **Show Device Drivers for installed hardware** to list only device drivers for managed hardware.

  Clear this setting to list all device drivers in each imported UpdateXpress System Packs (UXSPs) are listed.

  Important: After selecting this option, you must perform a compliance check by clicking the **Check Compliance** icon

) from the Windows Driver Updates: Apply page.

Step 4. Click **OK** to close the dialog.

Applying Windows device drivers

You can apply device drivers to managed servers running Windows.

Before you begin

- Lenovo XClarity Administrator uses the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems. The WinRM service must be correctly configured on the target servers before attempting to update OS device drivers (see Configuring Windows Server for OS device-driver updates).
- Devices that are not supported cannot be selected for updates.
- Read the device-driver update considerations before you attempt to update device drivers on your managed servers (see OS device-driver update considerations).
- Ensure that the repository contains the UXSPs and device drivers that you intend to deploy (see Downloading Windows device drivers).

  Note: When XClarity Administrator is initially installed, the catalog and repository are empty.
- XClarity Administrator can use the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems HTTPS is the default. To use HTTP, click **All Actions → Global Settings** on the Windows Driver updates: Apply page, and then clear **Use HTTPS for Windows driver updates**.

  Attention: When using HTTP, Windows user credentials are sent over the network *without* encryption and can be easily viewed using commonly available network troubleshooting tools.

  Important:

  – Ensure that Windows Remote Management (WinRM) on the target server is configured to use the same setting (HTTPS or HTTP) that is defined in XClarity Administrator (see Configuring Windows Server for OS device-driver updates).

  – Ensure that WinRM on the target server is configured with basic authentication.

  – When using HTTPS, ensure that WinRM on the target server is configured with **allowUnencrypted= false**.
- Ensure that PowerShell is supported on the target server.
- Ensure that the target server is powered on before attempting to update device drivers. If the server is not powered on, select the target server, and click **All Actions → Power Actions → Power On**.
- Ensure that XClarity Administrator has information that it needs to access the host operating system (see Managing access to operating-systems on managed servers.
- If you want to use a domain account when updating OS device drivers, ensure that you created the required configuration file (see).
- Ensure that no jobs are currently running on the target server. You cannot update device drivers on a managed server that is locked by a running job. If another update job is running on the target server, this update job is queued until the current update job completes. To see a list of active jobs, click **Monitoring → Jobs**.

About this task

XClarity Administrator updates only device drivers that are out of compliance. Device drivers are out of compliance when the version on the server is earlier than version in the selected UXSP. Device drivers that are equal to or later than version in the selected UXSP are skipped.

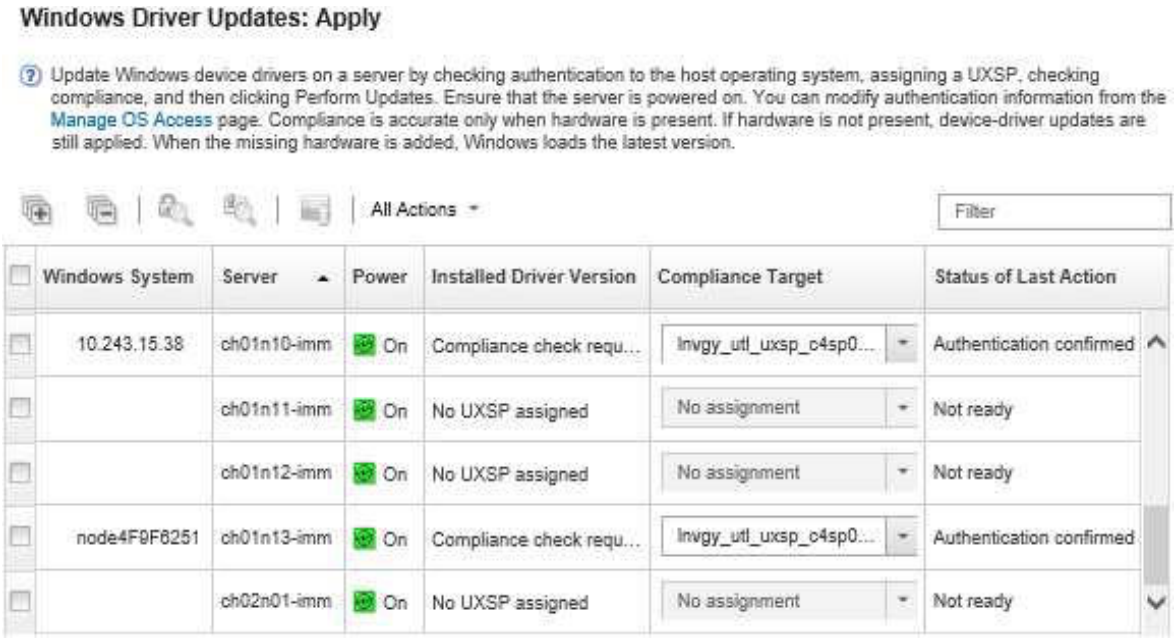
Procedure

To apply Windows device drivers to managed servers, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Apply** to display the Windows Driver Updates: Apply page.

Important:

- To discover the device drivers on the target server and determine compliance, you must select the target server and run the compliance check. After the compliance check is run for the first time, you can expand the row to see a list of device drivers on the target server.
- The **Windows System** column identifies the hostname or IP address of the host operating system.
- The **Server** column identifies the name and IP address of the managed server.



Step 2. Select one or more target servers and device drivers.

You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed servers by entering text (such as a name or IP address) in the **Filter** field.

Tip:

- You can choose to update all device drivers for a specific operating system, or you can expand an operating system and choose to update only specific devices
- The **Update Status** column shows the authentication status for each server and the update status for each device driver.
- The **OS Credential** column shows the stored credential that is used to authenticate to the operating system (for example, “901 – company\USER1.”

  If OS credentials are not defined for the host operating system on the target server, the Edit OS Credentials dialog is displayed. For a single target server, specify the user name and password that you want to use for this operation. For multiple target servers, select the stored credential to use for each server. Then, click **Save**.

  Note: The OS credentials that you select on the Edit OS Credentials dialog are not saved for the host operating system. To save OS credentials, see Managing access to operating-systems on managed servers.

Step 3. Click the **Check Authentication** icon () to run authentication and prerequisite checks.

XClarity Administrator connects to the host operating system using the stored credential that is listed in the **OS Credential** column, determines the OS version, verifies that WinRM is enabled, performs additional prerequisite checks, and then disconnects from the host OS.

For information about changing the stored credential for the host operating system, see Managing access to operating-systems on managed servers.

Step 4. For each target server, select the target UXSP that you want to use to update device drivers from the **Compliance Target** column.

Step 5. Select the target servers again, and click the **Check Compliance** icon () to verify the compliance of each device driver.

The compliance check updates the compliance status in the **Installed Driver Version** column. This column displays the overall compliance status for the server and the installed version and compliance status for each device driver as measured against the assigned UXSP.

-  **Compliant**. The installed device driver is equal to or later than the version in the assigned UXSP.
-  **Not compliant**. The installed device driver is earlier than the version in the assigned UXSP. You can click on the link to get more information about the non compliance.

Note: Device-driver compliance is accurate only when hardware is present. If hardware is not present, device drivers are still applied to the server. When the missing hardware is added to the server, Windows loads the latest version.

Step 6. Click the **Perform Updates** icon ().

Step 7. Select one of the following update rules.

- **Stop all updates on error**. If an error occurs while updating any of the device drivers on a target device, the update process stops for all target devices in the current device-driver update job. In this case, none of the device-driver updates in the UXSP for the target device are applied. The current device driver that is installed on all target devices remains in effect.
- **Continue on error**. If an error occurs while updating any of the device drivers on the target device, the update process does not update the device driver for that specific device; however, the update process continues to update other device drivers on the device and continues to update all other target devices in the current device-driver update job.
- **Continue to next system on error**. If an error occurs while updating any of the device drivers on the device, the -update process stops all attempts to update the device drivers for that specific device, so the current device drivers that are installed on that device remains in effect. The update process continues to update all other devices in the current device-driver update job.

Step 8. Click **Perform Updates** to update immediately, or click **Schedule** to schedule this update to run at a later time.

What to do next

When applying an update, if the target server fails to enter maintenance mode, attempt to apply the update again.

If updates were not completed successfully, see OS device-driver update considerations for troubleshooting and corrective actions.

From the Windows Driver Updates: Apply page, you can perform the following actions.

- View the status of the device-driver update directly from the Apply page in the **Update Status** column.
- Monitor the status of the device-driver update from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**.

  For more information about the jobs log, see Monitoring jobs.

  When the update job is complete, you can verify that the devices are compliant from the Windows Driver Updates: Apply page. The current driver version that is active on each device is listed in the **Installed Driver Version** column.

Chapter 14. Installing operating systems on bare-metal servers

You can use Lenovo XClarity Administrator to manage the OS images repository and deploy operating-system images to up to 28 bare-metal servers concurrently.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Operating-system deployment

Before you begin

After the 90-day free trial expires, you can continue to use XClarity Administrator to manage and monitor your hardware for free; however, you must purchase full-function-enablement licenses for each managed server that supports XClarity Administrator advanced functions to continue using the OS deployment function. Lenovo XClarity Pro provides entitlement to service and support and the full-function-enablement license. For more information about purchasing Lenovo XClarity Pro, contact your Lenovo representative or authorized business partner. For more information, see Installing the full-function enablement license in the XClarity Administrator online documentation.

About this task

XClarity Administrator provides a simple way to deploy operating-systems images to *bare-metal* servers, which typically do not have an operating system installed.

Attention: If you deploy an operating system to a server that has an operating system installed, XClarity Administrator performs a fresh installation that overwrites the partitions on the target disks

Several factors determine the amount of time that is required to deploy an operating system to a server:

- The amount of RAM that is installed in the server, which affects how long the server takes to start up.
- The number of and types of I/O adapters that are installed on the server, which affects the amount of time that it takes XClarity Administrator to perform an inventory of the server. It also affects the amount of time that it takes for the UEFI firmware to start when the server is started up. During an operating-system deployment, the server is restarted multiple times.
- Network traffic. XClarity Administrator downloads the operating-system image over the data network or the operating-system deployment network.
- The hardware configuration on the host on which Lenovo XClarity Administrator virtual appliance is installed. The amount of RAM, processors, and hard drive storage can affect download times.

Important: To deploy an operating-system image from XClarity Administrator, at least one of the XClarity Administrator interfaces (Eth0 or Eth1) must have IP network connectivity to the server network interface that is used to access the host operating system. Operating-system deployment uses the interface that is defined on the Network Access page. For more information about network settings, see Configuring network access.

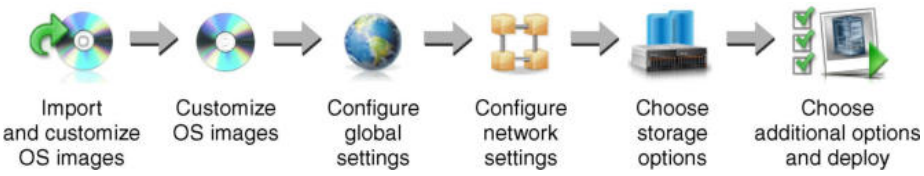
Before you perform a bare-metal operating-system deployment on a server, prepare the server by updating firmware to the latest levels and configuring the server using Configuration Patterns. For more information, see Updating firmware on managed devices and Configuring servers using configuration patterns.

Attention: It is recommended that you *do not* use XClarity Administrator to perform a bare-metal operating-system deployment on Converged and ThinkAgile appliances.

© Copyright Lenovo 2015, 2021

Procedure

The following figure illustrates the workflow for deploying an OS image to a server.



Step 1. **Import OS images.**

Before you can deploy an OS image to a server, you must first import the operating system into the repository. When you import an OS image, XClarity Administrator:

- Ensures that there is sufficient space in the OS images repository before importing the operating system. If you do not have sufficient space to import an image, delete an existing image from the repository and attempt to import the new image again.
- Creates one or more profiles of that image and stores the profile in the OS images repository. Each *profile* includes the OS image and installation options. For more information about predefined OS image profiles, see Operating-system image profiles.

A *base operating system* is the full OS image that was imported into the OS-images repository. The imported base image contains predefined profiles that describe the installation configurations for that image. You can create custom profiles in the base OS image that can be deployed for specific configurations.

You can also import supported *custom operating systems*. This custom image contains a predefined placeholder profile, which cannot be deployed. You must import a custom profile that can be deployed or create your own custom profile based on the placeholder profile. After the custom profile is added, the placeholder profile is removed automatically.

For Microsoft Windows Server 2016 and 2019, you can import a custom operating-system image for each release. The imported base image contains predefined profiles that describe the installation configurations for that image. You cannot create custom profiles in the custom OS image.

The OS images repository can store up to ten operating-system images, if space is available to store the images (up to 50GB). For a list of supported base and custom operating systems, see Supported operating systemsSupported operating systems in the Lenovo XClarity Administrator online documentation.

Step 2. **(Optional) Customize the OS image.**

You can customize an OS image by adding device drivers, boot files (for Windows only), configuration settings, unattend files, post-installation scripts, and software. When you customize a base OS image, XClarity Administrator creates a customized OS-image profile that includes the custom files and installation options.

The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Step 3. **Configure global settings.**

Global settings are configuration options that serve as defaults for operating system deployment. You can configure the following global settings.

- The password for the administrator user account to be used for deploying the operating systems
- The method to use to assign IP addresses to servers
- License keys to use when activating installed operating systems
- Optionally join an Active Directory domain as part of the Windows operating-system deployment

Step 4. **Configure network settings.**

You can specify the network settings for each server on which operating systems are to be deployed.

If you are using DHCP to assign IP addresses dynamically, you must configure the MAC address.

If you are using static IP addresses, you must configure the following network settings for a specific server before you can deploy an operating system to that server. After these settings are configured, the deployment status of the server changes to “Ready.” (Note that some fields are not available for static IPv6 addresses.)

- Hostname

  The hostname must comply with the following rules:
  – The hostname of each managed server must be unique.
  – The hostname can contain strings (labels) that are separated by a period (.).
  – Each label can contain ASCII letters, digits, and dashes (-); however, the string cannot start or end with a dash and cannot contain all digits.
  – The first label can be 2 - 15 characters in length. Subsequent labels can be 2 – 63 characters in length.
  – The total length of the hostname must not exceed 255 characters.
- MAC address of the port on the host where the operating system is to be installed.

  The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment.

  You can determine the status of the MAC address port that is used for OS deployment from the **MAC address** drop-down menu on the Network Settings dialog. If multiple ports are up or if all ports are down, AUTO is used by default.

  Notes:

  – Virtual network ports are not supported. Do not use one physical network port to simulate multiple virtual network ports.
  – When the server's network setting is set to AUTO, XClarity Administrator can automatically detect network ports in slots 1 – 16. At least one port in slots 1 – 16 must have a connection to XClarity Administrator.
  – If you want to use a network port in slot 17 or greater for the MAC address, you cannot use AUTO. Instead, you must set the server's network setting to the MAC address of the specific port that you want to use.
  – For ThinkServer servers, not all host MAC addresses are displayed. In most cases, MAC addresses for AnyFabric Ethernet adapters are listed on the Edit Network Settings dialog. MAC addresses for other Ethernet adapters (such as the Lan-On-Motherboard) are not listed. In cases where the MAC address for an adapter is not available, use the AUTO method for non-VLAN deployments.
- IP address and subnet mask

- IP gateway
- Up to two domain name system (DNS) servers
- Maximum transmission unit (MTU) speed
- VLAN ID, if VLAN IP mode is enabled

If you choose to use VLANs, you can assign a VLAN ID to the host network adapter that is being configured.

Step 5. **Choose the storage options**

For each deployment, you can choose the preferred storage location where the operating system is to be deployed. Depending on the operating system, you can choose to deploy to a local disk drive, embedded hypervisor key, or SAN.

Step 6. **Choose additional options and custom configuration settings, and deploy the OS image.**

You can configure additional deployment options, such as the license key for the OS deployment, and custom configuration settings. If you are installing Microsoft Windows, you can also configure the Active Directory domain to join.

Notes:

- If you defined custom configuration settings for a specific custom OS profile, you must define values for required custom configuration settings before you can deploy the profile to a server.
- When deploying a custom OS profile that includes custom settings, all target servers must use the same custom OS profile and the values for the custom settings apply to all target servers.

You can then choose the target servers for deployment and the OS images to be deployed. Remember that to deploy an operating system, the server must be have a deployment status of “Ready.”

You can deploy operating-system images on up to 28 servers concurrently.

Before you attempt to deploy an operating-system image, review the Operating-system deployment considerations.

Operating-system deployment considerations

Before you attempt to deploy an operating-system image, review the following considerations.

Lenovo XClarity Administrator considerations

- Ensure that no jobs are currently running on the target server. To see a list of active jobs, click **Monitoring → Jobs**.
- Ensure that the target server does not have a deferred or partially activated server pattern. If a server pattern has been deferred or partially activated on the managed server, you must restart the server to apply all configuration settings. Do not attempt to deploy an operating system to a server with a partially activated server pattern. To determine the configuration status of the server, see the **Configuration Status** field on the Summary page for the managed server (see Viewing the details of a managed server).
- Ensure that a password for the administrator account that is to be used to deploy the operating system is specified on the Global Settings: Deploy Operating Systems dialog. For more information about setting the password, see Configuring global OS-deployment settings.
- Ensure that the global default settings are correct for this operating-system deployment (see Configuring global OS-deployment settings).

Operating system considerations

- Ensure that you have all applicable operating-system licenses to activate the installed operating systems. You are responsible for obtaining licenses directly from the operating-system manufacturer.
- Ensure that the operating-system image that you intend to deploy is already loaded in the OS images repository. For information about importing images, see Importing operating-system images.
- You must import a boot file into the OS-images repository before you can deploy a Windows profile. Lenovo bundles the predefined WinPE_64.wim boot file along with a set of device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Because the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Files** tab.
- For SLES 15 and 15 SP1, you must import both the installer image and the associated package image from the Server OS Support Center webpage. For SLES 15 SP2 or later, you need to import only the Full Installation Media image because the Unified Installer and Packages DVDs from SUSE Linux Enterprise Server 15 and 15 SP1 are deprecated.
- For ThinkSystem servers, XClarity Administrator includes out-of-box device drivers to enable the installation of the operating system as well as basic network and storage configuration for the final operating system. For other servers, ensure that the operating-system image that you intend to deploy includes the appropriate Ethernet, Fibre Channel, and storage adapter device drivers for your hardware. If the I/O adapter device driver is not included in the operating system, the adapter is not supported for OS deployment. Always install the latest operating system to ensure that you have the latest inbox I/O adapter device drivers and boot files that you need. You can also add out-of-box device drivers and boot files to operating systems that have been imported into XClarity Administrator (see Customizing OS-image profiles in the XClarity Administrator online documentation).

  For VMware, use the latest Lenovo Custom Image for ESXi, which includes support for the latest adapters. For information about obtaining that image, see the VMware Support – Downloads webpage.
- Operating-system images in the XClarity Administrator repository might not be supported only on certain hardware platforms. Only OS-image profiles that are supported by the selected server are listed on the Deploy OS Images page. You can determine whether an operating system is compatible with a specific server from the Lenovo OS Interoperability Guide website.
- For ThinkSystem servers, if you want to deploy SLES 12 SP2, you must use a kISO profile. To get the kISO profiles, you must import the appropriate SLES kISO image after you import the base SLES operating system. You can download the SLES kISO image from the Linux Support – Downloads webpage.

  Notes:

  – The SLES kISO image counts towards the maximum number of imported OS images.

    The OS images repository can store up to ten operating-system images, if space is available to store the images (up to 50GB). For a list of supported base and custom operating systems, see Supported operating systemsSupported operating systems in the Lenovo XClarity Administrator online documentation.

  – If you delete all kISO profiles, you must delete the base SLES operating system and then import the base operation system and kISO image again to deploy SLES 12 SP2 on a ThinkSystem server.

  – If you create a custom OS-profile based on a kISO profile, the predefined device drivers in the base operating system are not included. The device drivers that are included in the kISO are used instead. You can also add device drivers to the custom OS-profile (see Creating a custom OS-image profile).

For more information about limitations for specific operating systems, see Supported operating systems.

Network considerations

- Ensure that all required ports are open (see Port availability for deployed operating systems).

- Ensure that XClarity Administrator can communicate with the target server (both the baseboard management controller and the servers' data network) over the interface (Eth0 or Eth1) that was selected when you configured the XClarity Administrator network access.

  To specify an interface to be used for operating-system deployment, see Configuring network access).

  For more information about the operating-system deployment network and interfaces, see Network considerations in the XClarity Administrator online documentation.
- Ensure that the IP addresses are unique for the host operating system. XClarity Administrator checks for duplicate IP addresses that you specify for the network address during the deployment process.
- If the network is slow or unstable, you might see unpredictable results when deploying operating systems.
- The XClarity Administrator network interface that is used for management must be configured to connect to the baseboard management controller using the same IP address method that you choose on the Global Settings: Deploy Operating Systems dialog. For example, if XClarity Administrator is set up to use eth0 for management, and you choose to use manually assigned static IPv6 addresses when configuring the deployed OS, then eth0 must be configured with an IPv6 address that has connectivity to the baseboard management controller.
- If you choose to use IPv6 addresses for the OS deployment global settings, the IPv6 address for XClarity Administrator must be routable to the baseboard management controller and the servers' data network.
- IPv6 mode is not supported for ThinkServer (see IPv6 configuration limitations in the XClarity Administrator online documentation).
- If you are using DHCP to assign IP addresses dynamically, you must configure the MAC address.
- If you are using static IP addresses, you must configure the following network settings for a specific server before you can deploy an operating system to that server. After these settings are configured, the deployment status of the server changes to "Ready." (Note that some fields are not available for static IPv6 addresses.)
  - Hostname

    The hostname must comply with the following rules:
    - The hostname of each managed server must be unique.
    - The hostname can contain strings (labels) that are separated by a period (.).
    - Each label can contain ASCII letters, digits, and dashes (-); however, the string cannot start or end with a dash and cannot contain all digits.
    - The first label can be 2 - 15 characters in length. Subsequent labels can be 2 – 63 characters in length.
    - The total length of the hostname must not exceed 255 characters.
  - MAC address of the port on the host where the operating system is to be installed.

    The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment.

    You can determine the status of the MAC address port that is used for OS deployment from the **MAC address** drop-down menu on the Network Settings dialog. If multiple ports are up or if all ports are down, AUTO is used by default.

    Notes:

    - Virtual network ports are not supported. Do not use one physical network port to simulate multiple virtual network ports.
    - When the server's network setting is set to AUTO, XClarity Administrator can automatically detect network ports in slots 1 – 16. At least one port in slots 1 – 16 must have a connection to XClarity Administrator.

  - If you want to use a network port in slot 17 or greater for the MAC address, you cannot use AUTO. Instead, you must set the server's network setting to the MAC address of the specific port that you want to use.
  - For ThinkServer servers, not all host MAC addresses are displayed. In most cases, MAC addresses for AnyFabric Ethernet adapters are listed on the Edit Network Settings dialog. MAC addresses for other Ethernet adapters (such as the Lan-On-Motherboard) are not listed. In cases where the MAC address for an adapter is not available, use the AUTO method for non-VLAN deployments.
- IP address and subnet mask
- IP gateway
- Up to two domain name system (DNS) servers
- Maximum transmission unit (MTU) speed
- VLAN ID, if VLAN IP mode is enabled

- If you choose to use VLANs, you can assign a VLAN ID to the host network adapter that is being configured.

For more information about the operating-system deployment network and interfaces, see Configuring network settings for managed servers and Configuring network settings for managed servers and Network considerations in the XClarity Administrator online documentation.

Storage and boot-option considerations

- Ensure that the UEFI boot option on the target server is set to “UEFI boot only” before you deploy an operating system. The “Legacy-only” and “UEFI first, then legacy” boot options are not supported for operating-system deployment.
- Each server must have a hardware RAID adapter that is installed and configured.

  Attention:

  - Only storage that is set up with hardware RAID is supported.
  - The software RAID that is typically present on the onboard Intel SATA storage adapter or storage that is set up as JBOD are not supported; however, if a hardware RAID adapter is not present, setting the SATA adapter to **AHCI SATA mode** enabled for operating-system deployment or setting unconfigured good disks to JBOD might work in some cases. For more information, see OS installer cannot find the disk on which you want to install XClarity Administrator in the XClarity Administrator online documentation.

    This exception does not apply to M.2 drives.
  - If a managed device has both local drives (SATA, SAS, or SSD) that are not configured for hardware RAID and M.2 drives, you must disable the local drives if you want to use M.2 drives, or you must disable the M.2 drives if you want to use local drives. You can disable on-board storage controller devices and legacy and UEFI storage option ROMs using the using Configuration Patterns by selecting Disable local disk on the Local Storage tab of the wizard or by creating a Configuration Pattern from an existing server and then disabling the M.2 devices in the extended UEFI pattern.
  - If a SATA adapter is enabled, the SATA mode *must not* be set to “IDE.”
- The NVMe storage that is connected to a server motherboard or HBA controller is not supported and must not be installed in the device; otherwise, OS deployment to non-NVMe storage will fail.
- When deploying RHEL, multi ports that are connected to same LUN on the target storage is not supported.
- Ensure that secure-boot mode is disabled for the server. If you are deploying a secure-boot mode enabled operating system (such as Windows), disable secure-boot mode, deploy the operating system, and then re-enable secure-boot mode.

- When deploying Microsoft Windows to a server, attached drives must not have existing system partitions (see OS deployment fails due to existing system partitions on an attached disk drive in the XClarity Administrator online documentation).
- For ThinkServer servers, ensure that the following requirements are met:
  - The boot settings on the server must include a Storage OpROM Policy that is set to `UEFI Only`. For more information, see OS installer cannot boot on a ThinkServer server - XClarity Administrator in the XClarity Administrator online documentation.
  - If you are deploying ESXi and there are network adapters that are PXE bootable, disable PXE support on the network adapters before deploying the operating system. The deployment is completed, you can re-enable PXE support, if desired.
  - If you are deploying ESXi and there are bootable devices in the boot-order list other than the drive on which the operating system is to be installed, remove the bootable devices from the boot-order list before deploying the operating system. After deployment is complete, you can add the bootable device back to the list. Ensure that the installed drive is at the top of the list.

For more information about storage-location settings, see Choosing the storage location for managed servers.

Managed-device considerations

- For information about operating-system deployment limitations for specific devices, see Supported hardware in the XClarity Administrator online documentation.
- Ensure there is no mounted media (such as ISOs) on the target server. Additionally, ensure there are no active Remote Media sessions open to the management controller.
- Ensure that the timestamp in BIOS is set to the current date and time.
- For ThinkSystem and System x servers, ensure that the Legacy BIOS option is disabled. From the BIOS/UEFI (F1) Setup utility, click **UEFI Setup → System Settings**, and verify that Legacy BIOS is set to Disabled.
- For Flex System servers, ensure that the chassis is powered on.
- For Converged, NeXtScale, and System x servers, ensure that a Feature on Demand (FoD) key for remote presence is installed. You can determine whether remote presence is enable, disabled, or not installed on a server from the Servers page (see Viewing the status of a managed server). For more information about FoD keys that are installed on your servers, see Viewing Features on Demand keys.
- For ThinkSystem servers and ThinkAgile appliances, the XClarity Controller Enterprise feature is required for operating-system deployment. For more information, see Viewing Features on Demand keys.
- For Converged and ThinkAgile appliances, it is recommended that you *do not* use XClarity Administrator to perform a bare-metal operating-system deployment.

Supported operating systems

Lenovo XClarity Administrator supports the deployment of several operating-systems. Only supported versions of the operating systems can be loaded into the XClarity Administrator OS images repository.

Important:

- For information about operating-system deployment limitations for specific devices, see Supported hardware in the XClarity Administrator online documentation.
- The cryptographic management feature of XClarity Administrator allows limiting communication to certain minimum SSL/TLS modes. For example, if TLS 1.2 is selected, then only operating systems with an installation process that supports TLS 1.2 and strong cryptographic algorithms can be deployed through XClarity Administrator.

- Operating-system images in the XClarity Administrator repository might not be supported only on certain hardware platforms. Only OS-image profiles that are supported by the selected server are listed on the Deploy OS Images page. You can determine whether an operating system is compatible with a specific server from the Lenovo OS Interoperability Guide website.
- For OS and Hypervisor related compatibility and support information and resources for Lenovo servers and solutions, see the Server OS Support Center webpage.

The following table lists the 64-bit operating systems that XClarity Administrator can deploy.

Operating system	Versions	Notes
CentOS Linux	7.2 and later 8.0 8.1 8.2	**Notes:** • All existing and future minor versions are supported unless otherwise noted. • DHCP, static IPv4, and static IPv6 address are supported. • VLAN tagging is not supported. • Out-of-box drivers are not supported. • OS profile customization is not supported. • CentOS 8.3 is not supported.
Microsoft® Windows® Server	2012 R2 2012 R2U1 2016 2019	Both the retail and volume license copies are supported. **Note:** XClarity Administrator is tested with only Windows versions that are supported by Microsoft at the time when the XClarity Administrator version was released. The following are *not supported*: • Windows Reseller Option Kit (ROK) • Windows Server Semi-Annual Channel (SAC) v1709, v1803, and v1809 • Windows Server 2019 Essentials • Windows Server 2016 Nanoserver • Windows Server 2012 Evaluation Copy • Windows Server images to managed servers with embedded hypervisor keys Windows Server 2012 R2 on servers that contain Intel CLX processors You must physically remove the embedded hypervisor key from the target servers before deploying a Windows image. This includes Hyper-V through one of the virtualization profiles. – Datacenter – Datacenter Core – Datacenter Virtualization (Hyper-V) – Datacenter Virtualization Core (Hyper-V with Core) – Standard – Standard Core – Standard Virtualization (Hyper-V) – Standard Virtualization Core (Hyper-V with Core)
Microsoft® Windows® Hyper-V Server	2016	

Operating system	Versions	Notes
Red Hat® Enterprise Linux (RHEL) Server	6.8 and later 7.2 and later 8.x	Includes KVM **Notes:** • All existing and future minor versions are supported unless otherwise noted. • When importing the DVD version of the OS image, only DVD1 is supported. • When installing RHEL on ThinkSystem servers, RHEL v7.4 or later is recommended. • To deploy RHEL 7.2, the global IP-assignment must be set to use IPv4 addresses. For information about global settings, see Configuring global OS-deployment settings. • OS deployment failures have been observed on IPv6 networks with lower bandwidths due to timeouts in the OS installer.
SUSE® Linux Enterprise Server (SLES)	12.x 15.x	Includes KVM and Xen hypervisors **Notes:** • All existing and future service packs are supported unless otherwise noted. • When importing the DVD version of the OS image, only DVD1 is supported. • OS deployment failures have been observed on IPv6 networks with lower bandwidths due to timeouts in the OS installer. • If you want to deploy SLES 12 SP2 on a ThinkSystem server, you must use a kISO profile. To get the kISO profiles, you must import the appropriate SLES kISO image. For more information, see Operating-system deployment considerations. • For SLES 15 and 15 SP1, you must import both the installer image and the associated package image from the Server OS Support Center webpage. For SLES 15 SP2 or later, you need to import only the Full Installation Media image because the Unified Installer and Packages DVDs from SUSE Linux Enterprise Server 15 and 15 SP1 are deprecated.

Operating system	Versions	Notes
Ubuntu Server	20.04.x	**Notes:** • All existing and future minor versions are supported unless otherwise noted. • Only DHCP is supported. Static IPv4 and static IPv6 address *are not* supported. • VLAN tagging *is not* supported. • The image is installed to the first disk that OS recognized, regardless of the storage option that you select. • Out-of-box drivers *are not* supported. • OS profile customization *is not* supported.
VMware vSphere® Hypervisor (ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x	Base VMware vSphere Hypervisor (ESXi) images and Lenovo VMware ESXi Custom images are supported. Lenovo VMware ESXi Custom images are customized for select hardware to give you online platform management, including updating and configuring firmware, platform diagnostics, and enhanced hardware alerts. Lenovo management tools also support simplified management of the ESXi with select System x servers. This image is available for download from the VMware Support – Downloads webpage. The license that is provided with the image is a 60-day free trial. You are responsible for meeting all VMware licensing requirements. **Important:** • All existing and future update packs are supported for 6.0, 6.5, 6.7, and 7.0 unless otherwise noted. • Base ESXi images (without Lenovo customization) include only basic in-box device drivers for network and storage. The base image does not include the out-of-box device drivers (which are included in Lenovo VMware ESXi Custom images). You can add out-of-box device drivers by creating your own custom OS0image profiles (see Customizing OS-image profiles). • For some versions of Lenovo VMware ESXi Custom images, separate images might be available for System x, ThinkSystem, and ThinkServer. Only one image for a specific release can exist in the OS-images repository at a time. • ESXi deployment is not supported for certain older servers. For information about which servers are supported, see the Lenovo OS Interoperability Guide website. • The following versions are supported for ThinkServer devices: ESXi 6.0u3, 6.5 and later. • During the installation of ESXi 5.5 (any update), or 6.0 onto a server in a Flex System chassis, the server might become unresponsive or restart shortly after the following message: `Loading image.pld` • ESXi 5.5 requires Memory Mapped I/O (MMIO) space to be configured within the initial 4 GB of the system. Depending on the configuration, certain systems attempt to use memory higher than 4 GB, which can cause a failure. To resolve the issue, see VMware deployment causes system hang or restart in the XClarity Administrator online documentation. • When deploying ESXi using a static IPv6 mode, the hostname that is defined on the Network Settings page in XClarity Administrator is not configured in the deployed ESXi instance. Instead, the default hostname `localhost` is used. You must manually set the hostname in the deployed ESXi to match the hostname that is defined in XClarity Administrator.

Operating system	Versions	Notes
		• When deploying ESXi on a managed server, the operating system does not explicitly move the drive on which the operating system is installed to the top of the boot-order list. If a boot device containing a bootable OS or a PXE server is specified before the boot device containing ESXi, then ESXi does not boot. For ESXi deployment, XClarity Administrator updates the boot-order list for most servers to ensure the ESXi boot device is at the top of the boot-order list; however, ThinkServer servers do not provide a way for XClarity Administrator to update the boot-order list. You must disable PXE boot support or remove bootable devices other than the installation drive before deploying the operating system. For more information, see Operating system does not boot after deploying ESXi on a ThinkServer server in the XClarity Administrator online documentation. **Tip:** Instead of setting **MM Config** through the Setup utility for each server, consider using one of the predefined extended UEFI patterns that are related to virtualization, which sets the MM Config option to 3 GB and disables the PCI 64-bit resource allocation. For more information about these patterns, see Defining extended UEFI settings.

Operating-system image profiles

When you import an OS image into the OS images repository, Lenovo XClarity Administrator creates one or more profiles for that image and stores the profiles in the OS images repository. Each predefined *profile* includes the OS image and installation options for that image.

OS image profile attributes

OS image profile attributes provide additional information about an OS-image profile. The following attributes can be shown.

- **kISO**. You must use a kISO profile to deploy SLES 12 SP2 to a ThinkSystem server. You can download the SLES kISO image from the Linux Support – Downloads webpage.

Predefined OS image profiles

The following table lists the profiles that are predefined by XClarity Administrator when you import an operating-system image. This table also lists the packages that are included in each profile.

You can create a customized OS image profile for a base operating system. For more information, see Customizing OS-image profiles.

Operating system	Profile	Packages included in the profile

CentOS Linux	Basic	`@X Window System`
		`@Desktop`
		`@Fonts`
		`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`

	Minimal	`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`

Operating system	Profile	Packages included in the profile	
	Virtualization	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Microsoft Windows Server **Note:** Includes Hyper-V through the *Virtualization Profile*.	Datacenter	GUI	
	Datacenter virtualization	GUI Hyper-V role	
	Datacenter virtualization core	Hyper-V role	
	Datacenter core		
	Standard	GUI	
	Standard virtualization	GUI Hyper-V role	
	Standard virtualization core	Hyper-V role	
	Standard core		
Customized Microsoft Windows Server	Datacenter_ customized		
	Standard_ customized		
Microsoft® Windows® Hyper-V Server 2016	Hyper_V	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	

Operating system	Profile	Packages included in the profile	
Red Hat Enterprise Linux (RHEL) **Note:** Includes KVM	Basic	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Minimal	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualization	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server (SLES) 12	Basic and Basic with kISO	<pattern>32bit</pattern> <pattern>Basis-Devel</pattern> <pattern>Minimal</pattern> <pattern>WBEM</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>gateway_server</pattern> <pattern>lamp_server</pattern> <pattern>mail_server</pattern> <pattern>ofed</pattern> <pattern>printing</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>	
	Minimal and Minimal with kISO	<pattern>Minimal</pattern> <pattern>file_server</pattern> <pattern>sap_server</pattern>	

Operating system	Profile	Packages included in the profile
	Virtualization-KVM and Virtualization-KVM with kISO	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>kvm_server</pattern> <pattern>kvm_tools</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	Virtualization-Xen and Virtualization-Xen with kISO	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern>
SUSE Linux Enterprise Server (SLES) 15	Basic and Basic	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Minimal and Minimal	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>

Operating system	Profile	Packages included in the profile
	Virtualization-KVM and Virtualization-KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
	Virtualization-Xen and Virtualization-Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
Ubuntu	Minimal	Openssh-server
	Virtualization	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
VMware vSphere® Hypervisor (ESXi)	Virtualization	Base VMware vSphere Hypervisor (ESXi) images and Lenovo VMware ESXi Custom images are supported.

Port availability for deployed operating systems

Some ports are blocked by certain operating-system profiles. The following tables list the ports that are open (not blocked).

Ensure that the hypervisor that is running the Lenovo XClarity Administrator appliance allows network traffic (TCP/UDP) on ports 139, 445, 3001, 3900, 8443. These are required for operating-system deployment.

RHEL Virtualization profile

By default, the Red Hat Enterprise Linux (RHEL) Virtualization profile blocks all ports except for those that are listed in the following table.

Table 9. Port availability for RHEL Virtualization profiles

Port	TCP or UDP	Direction	Communication description
22	TCP	Inbound	SSH communication
53	TCP, UDP	Outbound/Inbound	Communication with RHEL KVM networking devices
67	TCP, UDP	Outbound/Inbound	Communication with RHEL KVM networking devices
161	UDP	Outbound	Communication with SNMP agents
162	UDP	Inbound	Communication with SNMP agents
427	TCP, UDP	Outbound/Inbound	Communication with SLP service agent, SLP directory agent
3001	TCP	Outbound/Inbound	Communication with management software image-deployment service
15988	TCP	Outbound	CIM-XML over HTTP communication
15989	TCP	Outbound	CIM-XML over HTTP communication
49152 - 49215	TCP	Outbound/Inbound	KVM Virtual Server communication

RHEL Basic and Minimal profiles

By default, the RHEL Basic and Minimal profiles block all ports except for those that are listed in the following table.

Table 10. Port availability for RHEL Basic and Minimal profiles

Port	TCP or UDP	Direction	Communication description
22	TCP	Inbound	SSH communication
3001	TCP	Outbound/Inbound	Management software image-deployment service communication

SLES Virtualization, Basic, and Minimal profiles

For SUSE Linux Enterprise Server (SLES), some open ports are dynamically assigned based on the operating system version and profiles. For a complete list of open ports, see your SUSE Linux Enterprise Server documentation.

VMware ESXi Virtualization profile

For a complete list of open ports for VMware vSphere Hypervisor (ESXi) with Lenovo customization, see the VMware documentation for ESXi on the VMware Knowledge Base website.

Windows profiles

The following ports must be available for Windows profiles.

Table 11. Port availability for Windows profiles

Port	TCP or UDP	Direction	Communication description
137	UDP	Outbound/Inbound	NetBIOS Name Service
138	UDP	Outbound/Inbound	NetBIOS Datagram
139	TCP	Outbound/Inbound	NetBIOS Session
445	TCP	Outbound/Inbound	SMB over TCP

Configuring a remote file server

You can import OS images, device drivers, and boot files into the OS images repository from the local system or from a remote file server. To import files from a remote file server, you must first create a profile that is used to authenticate the connection to the remote file server.

About this task

The following cryptographic algorithms are supported:
- RSA–2048 bits
- RSA–4096 bits
- ECDSA–521 bits (secp521r1 curve)

The following protocols are supported:
- HTTP with no authentication.
- HTTP with basic authentication.
- HTTPS (certificate validation) with basic authentication.
- HTTPS (certificate validation) with no authentication.
- FTP with password authentication.
- SFTP (client validation) with password authentication.
- SFTP (client validation) with public-key authentication

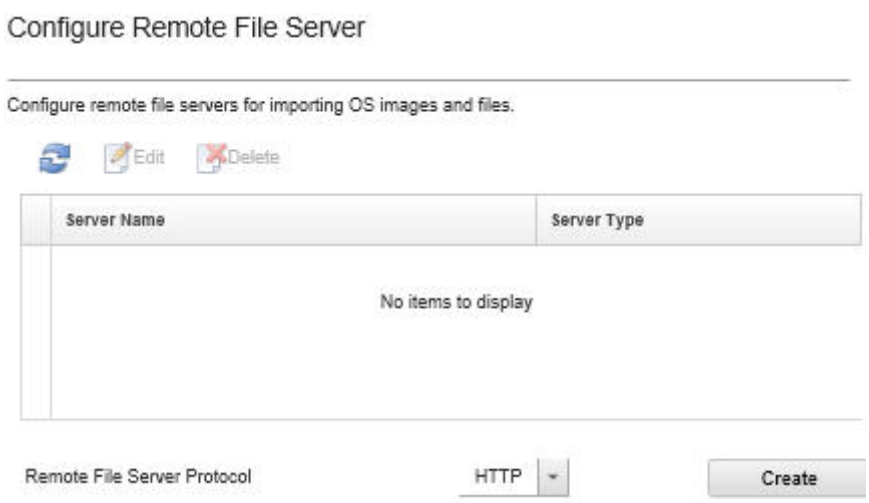
For SFTP public key authentication and HTTPS certificate validation, Lenovo XClarity Administrator validates that the remote file server' certificate. If the server certificate is not in the trust store, you are prompted to accept the server certificate and add it to the trust store. For information about troubleshooting validation issues, see Server certification validation fails in the XClarity Administrator online documentation.

Procedure

To configure a remote file server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS images** to display the Deploy Operating System: Manage OS images page.

Step 2. Click the **Configure File Server** icon ( ) to display the Configure Remote File Server dialog.



Step 3. Select the protocol for the remote file server from the **Remote File Server Protocol** list.

Step 4. Click **Create**. The Configure Remote File Server dialog is displayed.

Note: This dialog differs depending on the protocol that you selected.

Step 5. Enter the server name, address, and port.

Step 6. For HTTP, HTTPS, FTP, and SFTP with basic authentication, enter a user name and password if authentication is required to access the server.

Step 7. For SFTP with basic authentication, click **Validate Server Certificate** to obtain the public key signature.

Note: A dialog might be displayed informing you that the OS deployment process does not trust the public key of the SFTP file server. Click **OK** to store and trust the SFTP public key in the OS deployment trusted key store. If successful, the public key signature is shown in the **SFTP Server Public Key Signature** field.

Step 8. For SFTP with public-key authentication:

a. Enter a key passphrase and password and select the key type if authentication is required to access the server.

b. Click **Generate Management Server Key** to obtain the public-key signature.

c. Copy the generated key to the authorized_keys file in your SFTP remote file server.

d. Select the **The Management key was copied onto the server** checkbox in XClarity Administrator.

e. Click **Validate Server Certificate** to validate the public key signature.

Note: A dialog might be displayed informing you that the OS deployment process does not trust the public key of the SFTP file server. Click **OK** to store and trust the SFTP public key in the OS deployment trusted key store. If successful, the public key signature is shown in the **SFTP Server Public Key Signature** field.

f. Click **Save**.

Step 9. Click **Save Server**.

What to do next

From the Configure Remote File Server dialog, you can perform the following actions:

- Refresh the list of remote file server by clicking the **Refresh** icon ( ).

- Modify a selected remote file-server by clicking the **Edit** icon ().
- Remove a selected remote file server by clicking the **Delete** icon ().

Importing operating-system images

Before you can deploy a licensed operating system to managed servers, you must import the image into the XClarity Administrator OS images repository.

About this task

For information about operating system images that you can import and deploy, see Supported operating systems.

The OS images repository can store up to ten operating-system images, if space is available to store the images (up to 50GB). For a list of supported base and custom operating systems, see Supported operating systemsSupported operating systems in the Lenovo XClarity Administrator online documentation.

You can import only one image at a time. Wait until the image is displayed in the OS images repository before attempting to import another image. Importing the operating system might take a while.

When you import an operating system image, XClarity Administrator:

- Ensures that there is sufficient space in the OS images repository before importing the operating system. If you do not have sufficient space to import an image, delete an existing image from the repository and attempt to import the new image again.
- Creates one or more profiles of that image and stores the profile in the OS images repository. Each *profile* includes the OS image and installation options. For more information about predefined OS image profiles, see Operating-system image profiles.

Note: Internet Explorer and Microsoft Edge web browsers have an upload limit of 4 GB. If the file that you are importing is greater than 4 GB, consider using another web browser (such as Chrome or Firefox) or copy the file to a remote file server and import using the **Remote import** option.

Procedure

To import an operating-system image into the OS images repository, complete the following steps.

Step 1. Obtain a licensed ISO image of the operating system.

Note: You are responsible for obtaining applicable licenses for the operating system.

Step 2. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating Systems: Manage OS Images page.

Step 3. Click the **Import Files** icon () to display the Import OS Images and Files dialog.

Step 4. Click the **Local** tab to upload files from the local system, or click the **Remote** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote-file-server profile by clicking the **Configure File Server** icon (). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Enter the path and ISO-image file name, or click **Browse** to find the ISO image that you want to import.

If you chose to use the *local file server*, you must enter the absolute path to the ISO-image file. If you chose to use a *remote file server*, you must enter the absolute path (for example, `/home/user/isos.osimage.iso`) or relative path (for example, `/isos.osimage.iso`) to the ISO-image file (depending on the configuration of the remote file server). If the file is not found, verify that the path to the file is correct, and try again.

Step 7. Optional: **Optional:** Enter a description for the OS image.

Step 8. Optional: **Optional:** Select a checksum type to verify that the ISO image being imported into XClarity Administrator is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded OS image. The value must come from a secure source from an organization that you trust. If the uploaded image matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the image again or check the checksum value.

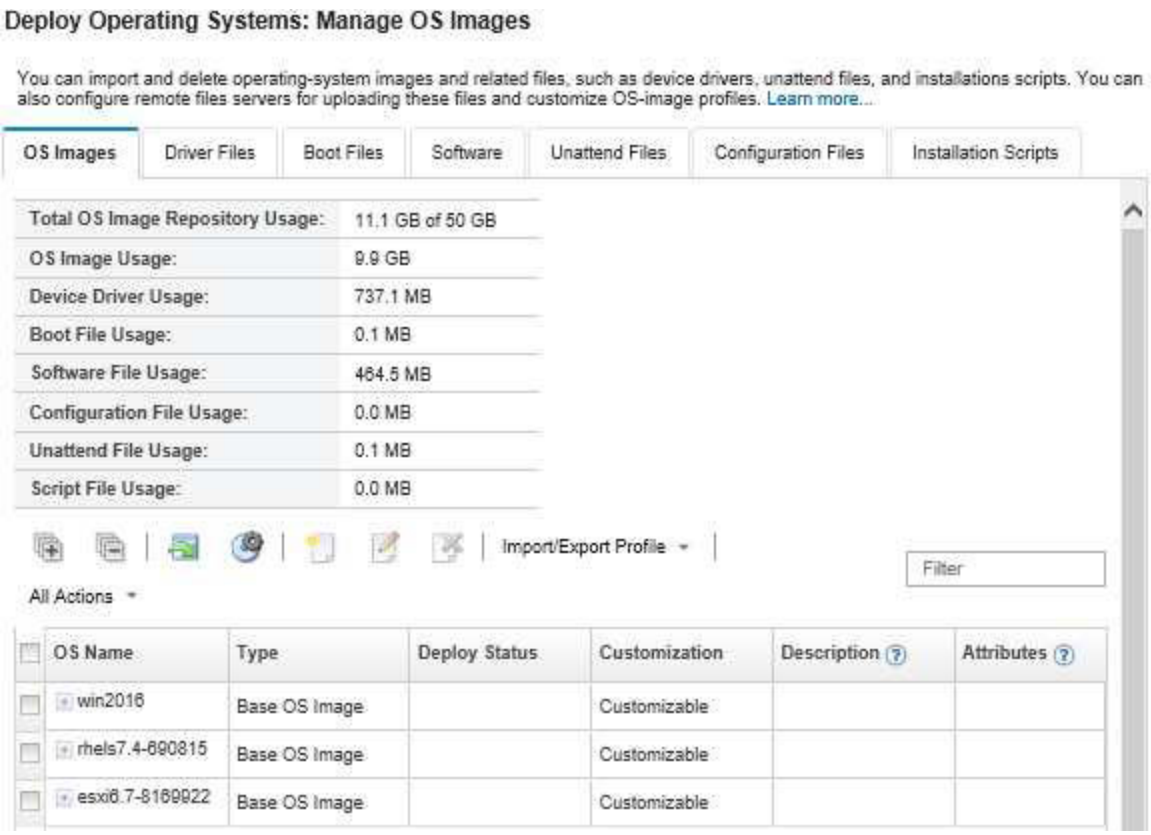
Three checksum types are supported:
- **MD5**
- **SHA1**
- **SHA256**

Step 9. Click **Import**.

Tip: ISO image is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the image. If you close the web browser tab or window in which the operating-system image is being uploaded before the upload completes, the import fails.

Results

XClarity Administrator uploads the OS image and creates an image profile in the OS images repository.



From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).
- Customize an OS image by clicking the **Create Customized Profile** icon ( ).
- Modify an OS image by clicking the **Edit** icon ( ).
- Import a customized OS image profile and apply to a base OS image by clicking **Import/Export Profile → Import Customized Profile Image** (see Importing a customized OS image profile).
- Delete a selected OS image or customized OS image profile by clicking the **Delete** icon ( ).
- Export a selected customized OS image profile by clicking **Import/Export Profile → Export Customized Profile Image**.

Note: When importing Windows Server images, you must also import the associated bundle file. Lenovo bundles the predefined WinPE_64.wim boot file along with a set of device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Because the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Files** tab.. For more information, see Importing boot files and Importing device drivers.

Customizing OS-image profiles

A *base operating system* is the full OS image that was imported into the OS-images repository. The imported base image contains predefined profiles that describe the installation configurations for that image. You can also create custom profiles in the base OS image that can be deployed for specific configurations. The custom profile contains the custom files and installation options.

Note: You cannot create a custom OS-image profile for a custom Microsoft Windows Server image.

Several example scenarios for customizing and deploying OS-images, including Windows and SLES, are available in English only. For more information, see End-to-end scenarios for setting up new devices.

You can add the following types of files to a custom OS image profile.

- **Boot files**

  A boot file acts as the bootstrap install environment. For Windows, this is a Windows Pre-installation (WinPE) file. A WinPE boot file is required to deploy Windows

  Lenovo XClarity Administrator supports predefined and custom boot files.

  – **Predefined boot files**. Lenovo provides a WinPE_64.wim boot file that can be used to deploy predefined OS-image profiles.

    Lenovo bundles the predefined WinPE_64.wim boot file along with a set of device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Because the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Files** tab.

    Notes:

    – A predefined boot file is not preloaded with XClarity Administrator. You must import a boot file into the OS-images repository before you can deploy a Windows profile.

    – If you migrated your Windows images to XClarity Administrator v2.1.0 from an earlier release, a preloaded WinPE_64.wim boot file was migrated to the OS-images repository. It is recommended that you import the bundle file for the specific Windows release that you want to deploy instead of using the preloaded boot file.

    – You cannot delete predefined boot files that were loaded when you installed XClarity Administrator; however, you can delete predefined boot files that were imported from a Lenovo bundle.

    – XClarity Administrator requires that imported bundle files be signed by Lenovo. When importing a bundle file, an .asc signature file must also be imported.

  – **Custom boot files**. You can create a WinPE boot file to customize boot options for a Windows deployment. You can then add the boot file to custom Windows profiles.

    XClarity Administrator provides scripts for creating boot files in the correct format. For information about creating a custom boot files, see Creating a boot (WinPE) file and Introduction to Windows PE (WinPE) website.

    The following file types are supported for importing custom boot files.

Operating system	Supported Boot File Types	Supported Bundle File Types
CentOS Linux	Not supported	Not supported
Microsoft® Windows® Server	A .zip file that contain a WinPE file that is created using the **genimage.cmd** script	A .zip file containing device drivers and boot files
Microsoft Windows Hyper-V Server	A .zip file that contain a WinPE file that is created using the **genimage.cmd** script	A .zip file containing device drivers and boot files
Red Hat® Enterprise Linux (RHEL) Server	Not supported	Not supported
SUSE® Linux Enterprise Server (SLES)	Not supported	Not supported

Operating system	Supported Boot File Types	Supported Bundle File Types
Ubuntu	Not supported	Not supported
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Not supported	Not supported

- **Device drivers**

  You must ensure that the operating-system image that you intend to deploy includes the appropriate Ethernet, Fibre Channel, and storage adapter device drivers for your hardware. If the I/O adapter device driver is not included in the operating system image or profile, the adapter is not supported for OS deployment. You can create custom OS-image profiles that include the out-of-box device drivers that you need.

  Lenovo XClarity Administrator supports in-box device drivers as well as predefined and custom out-of-box device drivers.

  – **In-box device drivers**. XClarity Administrator does not manage in-box device drivers. Always install the latest operating system to ensure that you have the latest in-box device drivers that you need.

    Note: You can add in-box device drivers to a customized Windows profile by creating a custom WinPE boot file and copying the device-driver files to the host system in the `C:\drivers` directory. When you create a custom OS-images profile that uses the custom boot-file, the device drivers that are in the C:\drivers directory are included in both WinPE and the final OS. They are treated as though they were inbox. Therefore, you do not need to import these in-box device drivers into XClarity Administrator when you specify device drivers to use in the custom OS-images profile creation.

  – **Predefined device drivers**. For ThinkSystem servers, XClarity Administrator is preloaded with a set of out-of-box device drivers for Linux to enable the installation of the operating system as well as basic network and storage configuration for the final operating system. You can add these predefined device drivers to your custom OS-image profiles, and then deploy the profiles to your managed servers

    Lenovo also bundles sets of predefined device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Currently, the bundle files are available only for Windows. If the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Image** tab.

    Notes:

    – By default, the predefined OS-image profiles include the predefined device drivers.

    – You cannot delete predefined device drivers that were loaded when you installed XClarity Administrator; however, you can delete predefined device drivers that were imported from a Lenovo bundle.

    – XClarity Administrator requires that imported bundle files be signed by Lenovo. When importing a bundle file, an .asc signature file must also be imported.

  – **Custom device drivers**. You can import out-of-box device drivers into the OS-images repository, and then add those device drivers to a custom OS-image profile.

    You can obtain device drivers from the Lenovo YUM Repository webpage, from the vendor (such as Red Hat), or through a custom device driver that you generated yourself. For some Windows device drivers, you can generate a custom device driver by extracting the device driver from the installation .exe to your local system and creating a .zip archive file.

    The following file types are supported for importing custom device drivers.

Operating system	Supported Device Driver File Types	Device Driver
CentOS Linux	Not supported	Not supported
Microsoft® Windows® Server	A .zip file containing the raw device-driver files, which are typically grouping of .inf, .cat, and .dll files.	A .zip file containing device-driver files
Microsoft Windows Hyper-V Server	A .zip file containing the raw device-driver files, which are typically grouping of .inf, .cat, and .dll files.	A .zip file containing device-driver files
Red Hat® Enterprise Linux (RHEL) Server	Driver update disk (DUD) in either an .rpm or .iso image format **Note:** If you apply a DUD .rpm to the customer profile, the .rpm is installed only to the final operating system. It is not installed in the install environment (initrd). To install a custom device driver to the initrd, import a DUD .iso and apply the .iso to the customer profile.	Not supported
SUSE® Linux Enterprise Server (SLES)	Driver update disk (DUD) in .rpm or .iso image format **Note:** If you apply a DUD .rpm to the customer profile, the .rpm is installed only to the final operating system. It is not installed in the install environment (initrd). To install a custom device driver to the initrd, import a DUD .iso and apply the .iso to the customer profile.	Not supported
Ubuntu	Not supported	Not supported
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Device drivers in .vib image format	Not supported

Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

- **Custom configuration settings**

  Configuration settings describe data that needs to be gathered dynamically during OS deployment. Lenovo XClarity Administrator uses a set of predefined configuration settings, including global, network, and storage location settings. You can use these predefined configuration settings and add custom configuration setting that are not available through the XClarity Administrator.

  The custom configuration settings are defined in the form of a JSON schema. The schema must conform to the JSON specification.

  When you import custom configuration settings to XClarity Administrator, XClarity Administrator validates the JSON schema. If the validation passes, XClarity Administrator generates custom macros for each setting.

  You can use the custom macros in the unattend file and post-installation script.

  In unattend files

You can associate the custom configuration file with an unattend file and include these custom macros (and predefined macros) in that unattend file.

You can add one or more custom configuration settings files in a custom profile. When you deploy the OS profile to a set of target servers, you can choose which configuration settings file to use. XClarity Administrator renders the **Custom Settings** tab on the Deploy OS Images dialog based on the JSON schema in the configuration settings file and allows you to specify values for each setting (JSON object) that is defined in the file.

Note: OS deployment will not proceed if input is not specified for any required custom configuration settings.

In post-installation scripts

After the data is gathered during OS deployment, XClarity Administrator creates an instance of the configuration settings file (which includes the custom settings in the selected file and a subset of predefined settings) on the host system that can be used by the post installation script.

Notes:

- Configuration settings file is unique to a custom OS-image profile.
- You cannot modify configuration settings for predefined OS-image profiles.
- Configuration settings are supported for only the following operating systems:
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) with Lenovo Customization 6.0u3 and later updates and 6.5 and later.

The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

- **Custom unattend files**

  You can customize OS image profiles to use unattend files to automate the deployment of the operating system.

  The following file types are supported for custom unattend files.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Server	Unattend (.xml)	For more information about unattend files, see the Unattended Windows Setup Reference webpage.
Microsoft Windows Hyper-V Server	Not supported	

Operating system	Supported File Types	More information
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	For more information about unattend files, see the Red Hat: Automating the Installation with Kickstart webpage. Consider the following when adding %pre, %post, % firstboot sections in the file. – You can include multiple %pre, %post, %firstboot sections to the unattend file; however, be aware of the ordering of the sections. – When the recommended **#predefined.unattendSettings. preinstallConfig#** macro is present in the unattend file, XClarity Administrator adds a %pre section before all other %pre sections in the file. – When the recommended **#predefined.unattendSettings. postinstallConfig#** macro is present in the unattend file, XClarity Administrator adds %post and %firstboot sections before all other %post and %firstboot sections in the file.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	For more information about unattend files, see the SUSE: AutoYaST webpage.
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Kickstart (.cfg)	Supported only for ESXi 6.0u3 and later updates and 6.5 and later. For more information about unattend files, see the VMware: Installing or Upgrading Hosts by Using a Script webpage. Consider the following when adding %pre, %post, % firstboot sections in the file. – You can include multiple %pre, %post, %firstboot sections to the unattend file; however, be aware of the ordering of the sections. – When the recommended **#predefined.unattendSettings. preinstallConfig#** macro is present in the unattend file, XClarity Administrator adds a %pre section before all other %pre sections in the file. – When the recommended **#predefined.unattendSettings. postinstallConfig#** macro is present in the unattend file, XClarity Administrator adds %post and %firstboot sections before all other %post and %firstboot sections in the file.

Attention:

– You can inject predefined and custom macros (configuration settings) in the unattend file using the unique name of the object. Predefined values are dynamic based on the XClarity Administrator instances. Custom macros are dynamic based on user input that is specified during OS deployment.

  Notes:

  – Surround the macro name with a hash symbol (#).
  – For nested objects, separate each object name using a period (for example, **#server_settings. server0.locale#**).
  – For custom macros, do not include the top-most object name. For predefined macros, prefix the macro name with "predefined."

  - When an object is created from a template, the name is appended with a unique number, starting with 0 (for example, **server0** and **server1**).
  - You can see the name for each macro from the Deploy OS Images dialog on the Custom Settings tabs by hovering over the Help icon () next to each custom setting.
  - For a list of predefined macros, see Predefined macros. For information about custom configuration settings and macros, see Custom macros.
- XClarity Administrator provides the following predefined macros that are used to communicate status from the OS installer, as well as several other critical installation steps. It is strongly recommended that you include these macros in unattend file (see Injecting predefined and custom macros to an unattend file).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

- **Custom installation scripts**

  You can customize OS image profiles to run an installation script after the OS deployment completes.

  Currently, only post-installation scripts are supported.

  The following table lists the file types for installation scripts that Lenovo XClarity Administrator supports for each operating system. Note that certain operation system versions do not support all of the file types that XClarity Administrator supports (for example, some RHEL versions might not include Perl in the minimal profile and, therefore, Perl scripts will not run). Ensure that you use the correct file type for the operating system versions that you want to deploy.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Server	Command file (.cmd), PowerShell (.ps1)	The default custom data and files path is `C:\lxca`. For more information about installation scripts, see the Add a custom script to Windows Setup webpage
Microsoft Windows Hyper-V Server	Not supported	
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm or .pl), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the RHEL: Post-installation Script webpage.
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm or .pl), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the SUSE: Custom user script webpage
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Bash (.sh), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the VMware: Installation and Upgrade Scripts webpage

- **Custom software**

You can customize OS image profiles to install custom software payloads after the OS deployment and post-installation scripts complete.

The following file types are supported for custom software.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Server	A .zip file containing the software payload.	The default custom data and files path is `C:\lxca`.
Microsoft Windows Hyper-V Server	Not supported	
Red Hat® Enterprise Linux (RHEL) Server	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.

Importing a customized OS image profile

You can import a customized OS image profile and add it to an existing compatible base OS image.

About this task

The base OS image must be imported before you can import a custom profile.

A custom OS-image profile can be added only to a based OS image of the same type. For example, if the exported profile is for a Windows 2016 image, the profile can only be imported and added to a Windows 2016 image that exists in the OS-images repository.

The OS images repository can store an unlimited number of custom profiles, if space is available to store the files.

Procedure

To import a customized OS image profile, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. From the **OS Images** tab, select the base OS image to which you want to add the customized OS image profile.

Step 3. Click **Import/Export Profile → Import Customized Profile Image**. The Import Customized OS Image Profile dialog is displayed

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Enter the profile name or click **Browse** to find the profile that you want to import.

Step 7. Optional: **Optional:** For local imports, select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:
- **MD5**
- **SHA1**
- **SHA256**

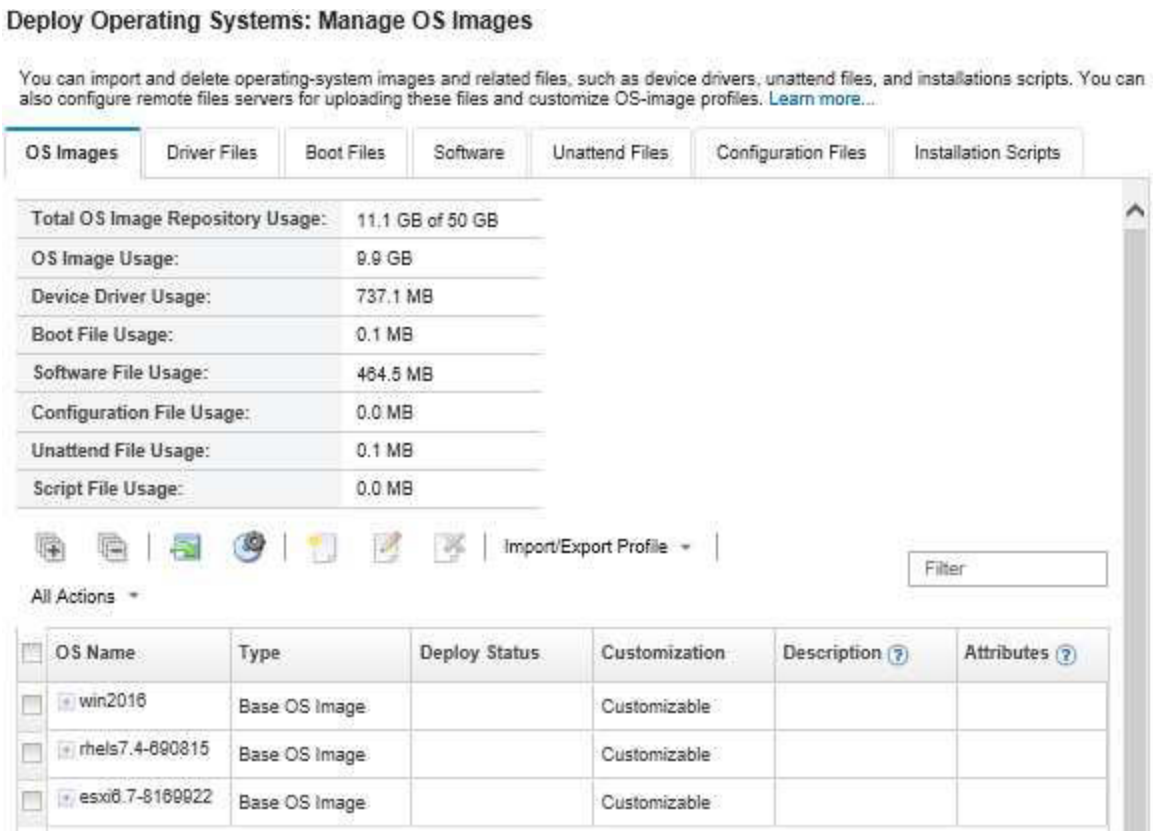
Step 8. Click **Import**.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

What to do next

The customized OS image profile is listed under the base operating system on the Manage OS Images page.



From this page, you can perform the following actions:

- Create a customized OS-image profile (see Creating a custom OS-image profile).

- Export a selected customized OS image profile by clicking **Import/Export Profile → Export Customized Profile Image**.

  Important: You can export customized OS image profiles to a remote file server that is set up to use FTP or SFTP protocols. You cannot export to a remote file server that is set up to use HTTP or HTTPS.

- Modify a selected customized OS image profile by clicking the **Edit** icon ( ).
- Remove a selected customized OS image profile by clicking the **Delete** icon ( ).

Importing boot files

You can import boot files into the OS images repository. These files can then be used to customize and deploy Windows images.

About this task

A boot file acts as the bootstrap install environment. For Windows, this is a Windows Pre-installation (WinPE) file. A WinPE boot file is required to deploy Windows

Lenovo XClarity Administrator supports predefined and custom boot files.

- **Predefined boot files**. Lenovo provides a WinPE_64.wim boot file that can be used to deploy predefined OS-image profiles.

  Lenovo bundles the predefined WinPE_64.wim boot file along with a set of device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Because the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Files** tab.

  Notes:

  - A predefined boot file is not preloaded with XClarity Administrator. You must import a boot file into the OS-images repository before you can deploy a Windows profile.
  - If you migrated your Windows images to XClarity Administrator v2.1.0 from an earlier release, a preloaded WinPE_64.wim boot file was migrated to the OS-images repository. It is recommended that you import the bundle file for the specific Windows release that you want to deploy instead of using the preloaded boot file.
  - You cannot delete predefined boot files that were loaded when you installed XClarity Administrator; however, you can delete predefined boot files that were imported from a Lenovo bundle.
  - XClarity Administrator requires that imported bundle files be signed by Lenovo. When importing a bundle file, an .asc signature file must also be imported.

- **Custom boot files**. You can create a WinPE boot file to customize boot options for a Windows deployment. You can then add the boot file to custom Windows profiles.

  XClarity Administrator provides scripts for creating boot files in the correct format. For information about creating a custom boot files, see Creating a boot (WinPE) file and Introduction to Windows PE (WinPE) website.

  The following file types are supported for importing custom boot files.

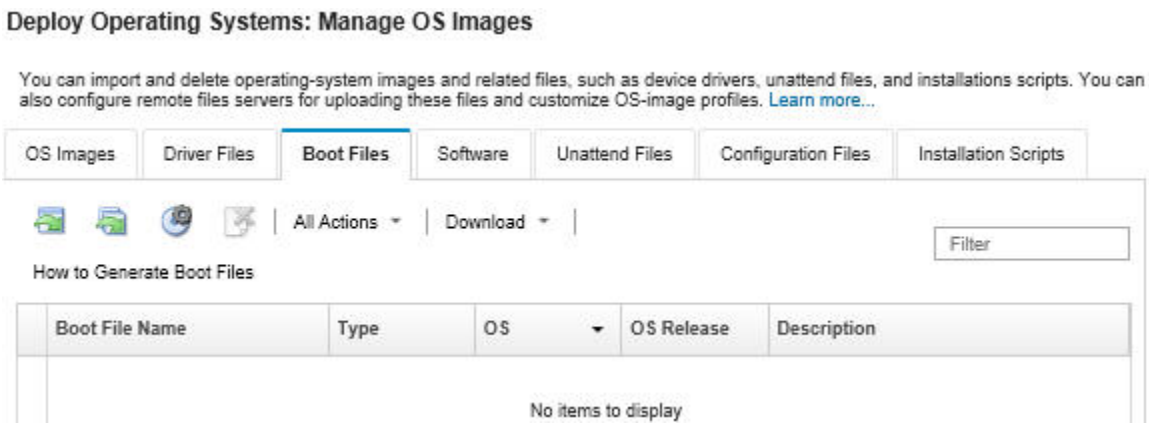
Operating system	Supported Boot File Types	Supported Bundle File Types
CentOS Linux	Not supported	Not supported
Microsoft® Windows® Server	A .zip file that contain a WinPE file that is created using the **genimage.cmd** script	A .zip file containing device drivers and boot files

Operating system	Supported Boot File Types	Supported Bundle File Types
Microsoft Windows Hyper-V Server	A .zip file that contain a WinPE file that is created using the **genimage.cmd** script	A .zip file containing device drivers and boot files
Red Hat® Enterprise Linux (RHEL) Server	Not supported	Not supported
SUSE® Linux Enterprise Server (SLES)	Not supported	Not supported
Ubuntu	Not supported	Not supported
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Not supported	Not supported

Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

- To import a Windows bundle file that contains boot files into the OS images repository, complete the following steps.
  1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
  2. Click the **Boot Files** tab.



  3. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the appropriate bundle file and the associated signature file for the OS image to the local system.
  4. Click the **Import Bundle File** icon ( ). The Import Bundle File dialog is displayed.
  5. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

     Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .
  6. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.
  7. Select the operating-system type and release.
  8. Enter the file name for the bundle file and the associated signature file or click **Browse** to find the files that you want to import.

9. **Optional:** Enter a description for the bundle file.
10. Click **Import**.

    Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

    If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

- To import an individual boot file into the OS images repository, complete the following steps.
  1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
  2. Click the **Boot Files** tab.
  3. Click the **Import File** icon (). The Import File dialog is displayed.
  4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

     Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon (). For more information, see Configuring a remote file server .
  5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.
  6. Select the operating-system type and release.
  7. Enter the file name or click **Browse** to find the boot file that you want to import.
  8. **Optional:** Enter a description for the boot file.
  9. **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

     If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

     Three checksum types are supported:
     - **MD5**
     - **SHA1**
     - **SHA256**
  10. Click **Import**.

      Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

      If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

What to do next

The boot file is listed on the **Boot Files** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ().

- Remove a selected boot file by clicking the **Delete** icon ().
- Add a boot file to an customized OS image profile (see Creating a custom OS-image profile).

Creating a boot (WinPE) file

You can create boot files that can be used to customize Windows images.

Before you begin

- Ensure that the operating system you intend to provision is installed on the host. For example, if you plan to provision Windows 2016 using the WinPE files, then install Windows 2016 on the host.
- Ensure that the Microsoft ADK that is compatible with the installed operating system is also installed on the host. For example, Windows 2012R2 requires ADK version 8.1 Update.
- Obtain the device drivers, in .inf format, that you want to add to the boot file.

  You can obtain device drivers from the Lenovo YUM Repository webpage, from the vendor (such as Red Hat), or through a custom device driver that you generated yourself. For some Windows device drivers, you can generate a custom device driver by extracting the device driver from the installation .exe to your local system and creating a .zip archive file.

  Lenovo also bundles sets of predefined device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Currently, the bundle files are available only for Windows. If the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Image** tab.
- Download the **genimage.cmd** and **startnet.cmd** files to the host in a temporary directory, such as `C:\customwim`.

  The **genimage.cmd** command is used to generate the WinPE boot files, including the .wim file. The **startnet.cmd** command is used by XClarity Administrator to bootstrap the Windows installer.
- Decide how you want to inject device drivers into the boot file. You can do this in one of the following ways:
  - Add in-box device drivers to a customized Windows profile by copying the device-driver files to the host system in the C:\drivers directory. These will be included in the boot file when genimage.cmd runs later.

    Note: When you create a custom OS-images profile that uses the custom boot-file, the device drivers that are in the C:\drivers directory are included in both WinPE and the final OS. They are treated as though they were inbox. Therefore, you do not need to import these in-box device drivers into XClarity Administrator when you specify device drivers to use in the custom OS-images profile creation.
  - Add out-of-box device drivers directly to the boot file.

    Note: If you use this method, the device drivers are only applied to the boot file and therefore to the WinPE install environment. The device drivers are not applied to the final installed OS. You must manually import the device drivers into the OS-images device driver repository and select them for use as part of the OS-image profile customization.
- For more information about boot files, see the Introduction to Window PE (WinPE) website.

Procedure

To create a boot file, complete the following steps.

Step 1. Using a user ID with administrator authority, run the Windows ADK command “Deployment and Imaging Tools Environment.” A command session is displayed.

Step 2. From the command session, change to the directory where the **genimage.cmd** and **starnet.cmd** files were downloaded (for example, `C:\customwim`).

Step 3. Ensure that no previously mounted images are on the host by running the following command:
`dism /get-mountedwiminfo`

If there are mounted images, discard them by running the following command:

`dism /unmount-wim /MountDir:C:\<mount_path> /Discard`

Step 4. If you are adding in-box device drivers to a customized Windows profile, copy the raw device-driver files, in .inf format, to the host system in the `C:\drivers` directory.

Step 5. Run the following command to generate the boot file, in .wim format, and then wait a few minutes for the command to complete.
`genimage.cmd amd64 <ADK_Version>`

Where <*ADK_Version*> is one of the following values.

- **8.1**. For Windows 2012 R2
- **10**. For Windows 2016

This command creates the boot file: `C:\WinPE_64\media\Boot\WinPE_64.wim`.

Step 6. Mount the boot file by running the following command:
`DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount`

Step 7. If you are adding out-of-box device drivers directly to the boot file, complete the following steps.

1. Create the following directory structure, where <*os_release*> is `2012`, `2012R2`, or `2016`
`drivers\<os_release>\`
2. Copy the device drivers, in .inf format, to a directory inside that path, for example:
`drivers\<os_release>\<driver1>\<driver1_files>`
3. Copy the `drivers` directory to the mount directory, for example:
`C:\WinPE_64\mount\drivers`

Step 8. Optional: Make additional customizations to the boot file, such as adding folders, files, startup scripts, language packs, and apps. For more information about customizing boot files, see the WinPE: Mount and Customize website.

Step 9. Unmount the image by running the following command.
`DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit`

Step 10. Compress the contents of the `C:\WinPE_64\media` directory into a zip file called `WinPE_64.zip`.

Step 11. Import the .zip file into XClarity Administrator (see Importing boot files).

Importing device drivers

You can import individual device drivers and bundles files into the OS images repository. These files can then be used to customize Linux and Windows images.

About this task

You must ensure that the operating-system image that you intend to deploy includes the appropriate Ethernet, Fibre Channel, and storage adapter device drivers for your hardware. If the I/O adapter device driver is not included in the operating system image or profile, the adapter is not supported for OS deployment. You can create custom OS-image profiles that include the out-of-box device drivers that you need.

Lenovo XClarity Administrator supports in-box device drivers as well as predefined and custom out-of-box device drivers.

- **In-box device drivers**. XClarity Administrator does not manage in-box device drivers. Always install the latest operating system to ensure that you have the latest in-box device drivers that you need.

Note: You can add in-box device drivers to a customized Windows profile by creating a custom WinPE boot file and copying the device-driver files to the host system in the `C:\drivers` directory. When you create a custom OS-images profile that uses the custom boot-file, the device drivers that are in the C:\drivers directory are included in both WinPE and the final OS. They are treated as though they were inbox. Therefore, you do not need to import these in-box device drivers into XClarity Administrator when you specify device drivers to use in the custom OS-images profile creation.

- **Predefined device drivers**. For ThinkSystem servers, XClarity Administrator is preloaded with a set of out-of-box device drivers for Linux to enable the installation of the operating system as well as basic network and storage configuration for the final operating system. You can add these predefined device drivers to your custom OS-image profiles, and then deploy the profiles to your managed servers

  Lenovo also bundles sets of predefined device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Currently, the bundle files are available only for Windows. If the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Image** tab.

  Notes:

  – By default, the predefined OS-image profiles include the predefined device drivers.

  – You cannot delete predefined device drivers that were loaded when you installed XClarity Administrator; however, you can delete predefined device drivers that were imported from a Lenovo bundle.

  – XClarity Administrator requires that imported bundle files be signed by Lenovo. When importing a bundle file, an .asc signature file must also be imported.

- **Custom device drivers**. You can import out-of-box device drivers into the OS-images repository, and then add those device drivers to a custom OS-image profile.

  You can obtain device drivers from the Lenovo YUM Repository webpage, from the vendor (such as Red Hat), or through a custom device driver that you generated yourself. For some Windows device drivers, you can generate a custom device driver by extracting the device driver from the installation .exe to your local system and creating a .zip archive file.

  The following file types are supported for importing custom device drivers.

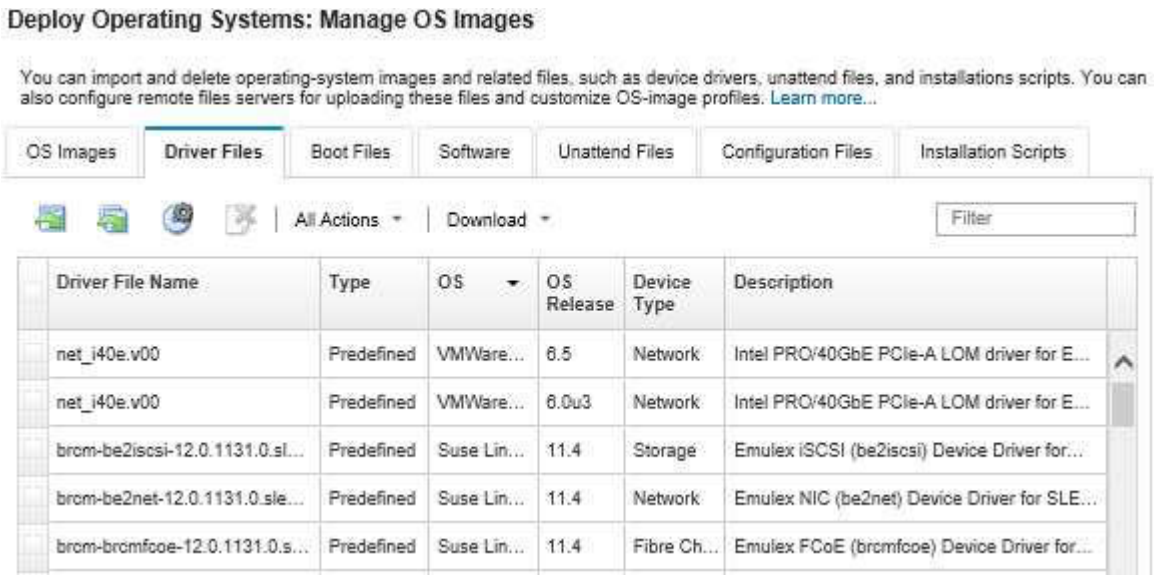
Operating system	Supported Device Driver File Types	Device Driver
CentOS Linux	Not supported	Not supported
Microsoft® Windows® Server	A .zip file containing the raw device-driver files, which are typically grouping of .inf, .cat, and .dll files.	A .zip file containing device-driver files
Microsoft Windows Hyper-V Server	A .zip file containing the raw device-driver files, which are typically grouping of .inf, .cat, and .dll files.	A .zip file containing device-driver files
Red Hat® Enterprise Linux (RHEL) Server	Driver update disk (DUD) in either an .rpm or .iso image format **Note:** If you apply a DUD .rpm to the customer profile, the .rpm is installed only to the final operating system. It is not installed in the install environment (initrd). To install a custom device driver to the initrd, import a DUD .iso and apply the .iso to the customer profile.	Not supported

Operating system	Supported Device Driver File Types	Device Driver
SUSE® Linux Enterprise Server (SLES)	Driver update disk (DUD) in .rpm or .iso image format **Note:** If you apply a DUD .rpm to the customer profile, the .rpm is installed only to the final operating system. It is not installed in the install environment (initrd). To install a custom device driver to the initrd, import a DUD .iso and apply the .iso to the customer profile.	Not supported
Ubuntu	Not supported	Not supported
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Device drivers in .vib image format	Not supported

Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

- To import a Windows bundle file that contains device-drivers into the OS images repository, complete the following steps.
  1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
  2. Click the **Driver File** tab.



  3. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the appropriate bundle file and the associated signature file for the OS image to the local system.
  4. Click the **Import Bundle File** icon ( ). The Import Bundle File dialog is displayed.
  5. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon (). For more information, see Configuring a remote file server .

6. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.
7. Select the operating-system type and release.
8. Enter the file name for the bundle file and the associated signature file or click **Browse** to find the files that you want to import.
9. **Optional:** Enter a description for the bundle file.
10. Click **Import**.

    Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

    If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

- To import an individual device driver into the OS images repository, complete the following steps.
  1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
  2. Click the **Driver Files** tab.
  3. Click the **Import File** icon (). The Import File dialog is displayed.
  4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

     Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon (). For more information, see Configuring a remote file server .
  5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.
  6. Select the operating-system type and release.
  7. Enter the file name or click **Browse** to find the device driver that you want to import.
  8. **Optional:** Enter a description for the device driver.
  9. **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

     If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

     Three checksum types are supported:
     - **MD5**
     - **SHA1**
     - **SHA256**
  10. Click **Import**.

      Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

What to do next

The device-drive image is listed on the **Driver Files** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).
- Remove a selected device driver by clicking the **Delete** icon ( ).
- Add a device driver to an customized OS image profile (see Creating a custom OS-image profile).

Importing custom configuration settings

Configuration settings describe data that needs to be gathered dynamically during OS deployment. Lenovo XClarity Administrator uses a set of predefined configuration settings, including global, network, and storage location settings. You can use these predefined configuration settings and add custom configuration setting that are not available through the XClarity Administrator.

About this task

The custom configuration settings are defined in the form of a JSON schema. The schema must conform to the JSON specification.

When you import custom configuration settings to XClarity Administrator, XClarity Administrator validates the JSON schema. If the validation passes, XClarity Administrator generates custom macros for each setting.

You can use the custom macros in the unattend file and post-installation script.

In unattend files

You can associate the custom configuration file with an unattend file and include these custom macros (and predefined macros) in that unattend file.

You can add one or more custom configuration settings files in a custom profile. When you deploy the OS profile to a set of target servers, you can choose which configuration settings file to use. XClarity Administrator renders the **Custom Settings** tab on the Deploy OS Images dialog based on the JSON schema in the configuration settings file and allows you to specify values for each setting (JSON object) that is defined in the file.

Note: OS deployment will not proceed if input is not specified for any required custom configuration settings.

In post-installation scripts

After the data is gathered during OS deployment, XClarity Administrator creates an instance of the configuration settings file (which includes the custom settings in the selected file and a subset of predefined settings) on the host system that can be used by the post installation script.

Notes:

- Configuration settings file is unique to a custom OS-image profile.
- You cannot modify configuration settings for predefined OS-image profiles.
- Configuration settings are supported for only the following operating systems:

- Microsoft® Windows® Server
- Red Hat® Enterprise Linux (RHEL) Server
- SUSE® Linux Enterprise Server (SLES)
- VMware vSphere® Hypervisor (ESXi) with Lenovo Customization 6.0u3 and later updates and 6.5 and later.

The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

To import configuration-settings files into the OS-images repository, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Configuration Settings** tab.



Step 3. Click the **Import File** icon ( ). The Import Configuration Settings dialog is displayed.

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Select the operating-system type.

Step 7. Enter the file name of the configuration-settings file, or click **Browse** to find the file that you want to import.

Step 8. Optional: **Optional:** Enter a description of the configuration-settings.

Tip: Use the **Description** field to distinguish between custom files with the same name.

Step 9. Optional: **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:

- **MD5**
- **SHA1**
- **SHA256**

Step 10. Click **Import**. The JSON format is validated when you import the file. If errors are found, a dialog is displayed with the error message and location.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

Attention: If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

What to do next

The configuration-settings files are listed on the **Configuration Settings** tab on the Manage OS Images page.

From this page, you can also perform the following actions.

- Create a configuration-setting file by clicking the **Create** icon ( ), and then specifying the file name, description, OS type, and configuration settings and values. Click **Validate** to validate the schema before saving the file.

  The editor identifies the location of any errors that are found in the file. Note that some messages are English only.

- View and modify a configuration-settings file by clicking the **Edit** icon ( ).

  You cannot edit a configuration-settings file that is associated with an unattend file.

  The editor identifies the location of any errors that are found in the file. Note that some messages are English only.

- Copy a configuration-settings file by clicking the **Copy** icon ( ).

  If you copy a configuration-settings file that is associated with an unattend file, the associated unattend file is also copied and the association is automatically created between both copied files.

- Remove selected configuration-setting files by clicking the **Delete** icon ( ).

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).

For information about adding an configuration-settings to a customized OS image profile, see Creating a custom OS-image profile.

Custom macros

Macros give you the ability to add variable data (configuration settings) to an unattend file or post-installation script. Lenovo XClarity Administrator allows you to define your own custom settings by creating a custom configuration-settings file, using JSON format.

The value for each custom configuration setting varies based on user input that is specified during OS deployment.

When you import custom configuration settings in XClarity Administrator, XClarity Administrator validates the JSON schema. If the validation passes, XClarity Administrator generates custom macros for each setting.

To inject custom macros in to an unattend file or post-installation script, use the unique name of the object, separate nested objects using a period, and then surround the macro name with a hash symbol (#), for example, **#server_settings.server0.locale#**.

Notes:

- Do not include the top-most object name.
- When an object is created from a template, the name is appended with a unique number, starting with 0 (for example, server0 and server1).
- You can see the name for each macro from the Deploy OS Images dialog on the Custom Settings tabs by hovering over the **Help** icon () next to each custom setting.

Configuration settings

You can define custom configuration settings that:

- Are common to all target servers or unique to a specific target server.
- Have static (non-configurable) values or with dynamic (configurable) values that are entered when you deploy the OS-image profile.
- Have a variable number of elements based on a template. For example, you can define a configuration setting that let's you specify 0 – 3 NTP servers during deployment.

Common settings

During OS deployment, the UI elements on the **Common Settings** tabs on the Deploy OS Image dialog are rendered based on the objects that are represented in the **content** object. The objects describe the settings and values that the all target servers need for OS deployment.

To represent settings that are common to all servers, the JSON file must contain a parent object with a nested object that contains the `"common":true` name/value pair.

The following example uses the same configurable (dynamic) NTP servers for all servers.

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": true,
      "description": "NTP Servers",
      "label": "NTP Servers",
      "maxElements": 3,
      "minElements": 0,
      "name": "common-ntpservers",
      "optional": true,
      "template": [{
         "autoCreateInstance": true,
         "category": "dynamic",
         "common": true,
         "description": "A NTP Server",
         "label": "NTP Server",
         "name": "ntpserver",
         "optional": true,
         "regex": "[\\w\\.]{1,64}$",
         "type": "string"
      }],
      "type": "array"
   },
   ...,
}
```

The following example uses the same non-configurable (static) post-installation script log directory.

```
{
   "category": "dynamic",
   "content": [{
      "category": "static",
      "common": true,
      "description": "Directory location for post-installation script logging.",
      "name": "logpath",
      "optional": false,
      "type": "string",
      "value": "/tmp/mylogger.log"
   },
   ...,
}
```

Server-specific settings

During OS deployment, the UI elements on the **Server-Specific Settings** tab on the Deploy OS Image dialog are rendered based on the objects that are represented in the template's **content** objects. The objects describe the settings and values that a specific target server needs for OS deployment.

After the server-specific values are gathered in the UI, a **content** object is created in the JSON for each target server based on the **template** object. Each **content** object contain a unique **name** and **targetServer** field, and any values that were inputted for that server.

To represent the server-specific settings, the JSON file must contain a parent object with the following content:

- The `"category":"dynamic"` name/value pair.
- A nested object that contains the `"common":false` name/value pair. Only one `"common": false` object is supported in the content of the parent object.
- A template object with an embedded content object. This template array can contain only one object.

For example, if you want to define a unique OS locale for each target server

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": false,
      "name": "server-settings",
      "optional": false,
      "template": [{
         "category": "dynamic",
         "common": false,
         "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
         }],
         "name": "server",
         "optional": false,
         "type": "assoc_array"
      }],
      "type": "assoc_array"
   },
```

```
    ...,
}
```

JSON specification

The following table describes the fields that are allowed in the JSON specification.

Parameter	Required / Optional	Type	Description
autoCreateInstance	Optional	Boolean	Indicates whether an instance of the template object is created automatically in JSON file at deployment time. This can be one of the following values. • **true**. An instance of the template object is created automatically in JSON file at deployment time. • **false**. (default) An instance of the template object *is not* created automatically in JSON file at deployment time **Note:** This field can be placed only in the template object.
category	Required	String	Indicates how the value of each setting is populated. This can be one of the following values: • **dynamic**. The value is input by the user at run time. Lenovo XClarity Administrator prompts you for this value during OS deployment. • **predefined**. The value is preset by Lenovo XClarity Administrator. • **static**. The value is specified in the schema and does not change at run time. Nested objects inherit the value of this field from its parent object. If **category** is set to `static` in the parent object, then it must be set to `static` in all nested objects as well. If **category** is set to `dynamic` in the parent object, it can be either `static` or `dynamic` in the nested objects.
choices	Optional	Array of values that match the **type** property	Array of static values (such as strings or integers) for the configuration setting from which the user can select during OS deployment (for example, `["enabled","disabled"]`).
common	Optional	Boolean	Indicates whether this configuration schema applies to all target servers. • **true**. The object applies to all target servers. • **false**. (default) The object applies to a specific target server. Nested objects inherit the value of this field from its parent object. If **common** is set to `true` in the parent object, then it must be set to `true` in all nested objects as well. If **common** is set to `false` in the parent object, then it must be set to `false` in all nested objects.

Parameter	Required / Optional	Type	Description
content	Optional	Array of objects	Pattern that represents nested objects in the schema. After user-inputted data is gathered during OS deployment, this field is used to represent the final values for a given template in the instance of the configuration-settings file that is created for the deployment.
default	Optional	Varies depending on the **type**	The default value.
description	Optional	String	Description of the object
label	Optional	String	Label for the setting in the user interface that is displayed during OS deployment
max	Optional	Integer	Maximum value, when **type** is set to integer. The default value is unlimited.
maxElements	Optional	Integer	Maximum number of entries in the array for this object.
min	Optional	Integer	Minimum value, when **type** is set to integer. The default value is 0.
minElements	Optional	Integer	Minimum number of entries in the array for this object.
name	Required	String	Unique name of the object. This name can contain only the following characters: alphanumeric characters (a-z, A-Z, and 0-9), underscore (_), and dash (-). You can reference the **name** as a custom macro in the unattend file. When referencing a nested **name** object, separate each object using a period (for example, `mydeploy.node.locale`).
optional	Required	Boolean	Indicates whether the object is optional. This can be one of the following values. • **true**. The field is optional • **false**. The field is required.
regex	Optional	String	Regular expression for validating the value (for example, `"[\\w\\.]{1,64}$"`)
script	Optional	Array of strings	List of scripts, separated by a comma, that have dependencies on the data in this object (for example, `["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]`). **Note:** The scripts must be available to the OS-image profile as an installation script or custom software.
targetServer	Optional	String	UUID of the server that is the target for the OS deployment. If common is true, this field can be empty or null, and the target server is specified during OS deployment.

Parameter	Re-quired / Optional	Type	Description

template	Optional	Array of objects	Pattern that represents reusable objects.
			During OS deployment, this template can represent multiple instances of the object. The **minElements** and **maxElements** fields can be used to limit the number of instances.
			
			The following example uses a template to represent an array of 1 - 3 NTP servers.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"template": [{`
			`"autoCreateInstance": true,`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver",`
			`"optional": true,`
			`"regex": "[\\w\\.]{1,64}$",`
			`"type": "string"`
			`}],`
			`"type": "array"`
			`},`
			
			After user-inputted values are gathered during OS deployment, an instance of the configuration-settings file is created with specific content for each device on which the OS is to be deployed.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"content": [{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver0",`
			`"optional": true,`
			`"regex": "[\\w\\.]{1,64}$",`
			`"type": "string",`
			`"value": "192.0.2.1"`
			`}],`
			`"template": [{`
			`"category": "dynamic",`

Parameter	Re-quired / Optional	Type	Description

			<pre>"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			}</pre> **Notes:** • A template is *required* at the top level of server-specific objects (common=false). • If **category** is `static`, the template field is ignored.

type	Required	String	Data type for the object. This can be one of the following values. • **array** • **assoc_array** • **boolean** • **integer** • **password** • **string** • **user_data**
value	Optional	String	A single static value for the configuration setting. **Notes:** • If **default** is set, this field can be empty or null; otherwise, specify a value that matches **type**. • If **type** is `password`, specify a non-encrypted string. • If **type** is `assoc_array` or `array`, you must also specify an empty **content** field. • If **type** is `user_data`, specify valid JSON-formatted **value**. • If **regex** is set, this value is validated using the specified regular expression.

The following example configuration settings define locale settings for SLES deployments that can be added to a custom profile.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "template": [{
            "autoCreateInstance": true,
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
```

```
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
        "category": "dynamic",
        "common": true,
        "description": "A NTP Server",
        "label": "NTP Server",
        "name": "ntpserver",
        "optional": true,
        "regex": "[\\w\\.]{1,64}$",
        "type": "string"
    }],
    "type": "array"
},
{
    "category": "static",
    "common": true,
    "description": "Directory for post-installation script logging.",
    "name": "logpath",
    "optional": false,
    "type": "string",
    "value": "/tmp/mylogger.log"
}],
"description": "Custom configuration file for deployment of custom locale, NTP server,
                and directory for post-installation script logs.",
"label": "My Custom Deployment",
"name": "myCustomDeploy",
```

```
    "optional": false,
    "type": "array"
}
```

The following example is the instance of the configuration settings file that is created on the host system after user-inputted values are defined during deployment.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "content": [{
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
                "category": "dynamic",
                "choices": ["english-us", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the keyboard locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "Keyboard Locale",
                "name": "keyboardLocale",
                "optional": false,
                "type": "string",
                "value": "english-us"
            }],
            "name": "server0",
            "optional": false,
            "type": "assoc_array",
            "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
        },
        {
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
```

```
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server1",
        "optional": false,
        "type": "assoc_array",
        "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
    }],
    "template": [{
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "content": [{
        "category": "dynamic",
        "common": true,
```

```
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver0,
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.1"
        },
        {
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver1",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.2"
        }],
        "template": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
        }],
        "type": "array"
    },
    {
        "category": "static",
        "common": true,
        "description": "Directory for post-installation script logs.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Predefined macros

Macros give you the ability to add variable data (configuration settings) to an unattend file or post-installation script. Lenovo XClarity Administrator provides a set of predefined configuration settings that you can use.

To inject predefined macros to an unattend or post-installation script file, prefix the macro with "predefined" for predefined macros, separate nested objects using a period, and then surround the macro name with a hash symbol (#), for example **#predefined.globalSettings.ipAssignment#**.

The value for each predefined macro varies based on the XClarity Administrator instance. For example, the **Deploy OS Images → Global Settings → IP Assignment** field allows you to specify the IP mode. After the user-inputted value is gathered during OS deployment, the value is represented in the predefined

configurations settings by the predefined macro **#predefined.globalSettings.ipAssignment#** and in the instance of the configuration-settings JSON file under the ipAssignment Object name.

The following table lists the predefine macros (configuration settings) that are available in XClarity Administrator.

Macro name	Type	Description
predefined	Object	Information about all predefined OS-deployment settings
globalSettings	Object	Information about global OS-deployment settings
credentials	Array of objects	Information about user credentials
name	String	
type	String	Operating system type. This can be one of the following values. • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	String	Host network setting option for operating system deployment. This can be one of the following values. • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	String	Indicates whether VLAN mode is used. This can be one of the following values. • **true**. VLAN mode is used. • **false**. VLAN mode is not used.
hostPlatforms	Object	Deployment settings from the host platforms
licenseKey	String	License key to be used for Microsoft Windows or VMware ESXi. If you do not have a license key, you can set this field to null.
networkSettings	Array	Information about network settings
dns1	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	String	Alternative DNS server for the host server to be used after the operating system is deployed
gateway	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
hostname	String	Hostname for the host server. If a hostname is not specified, a default hostname is assigned.
ipAddress	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings.
mtu	Long	Maximum transmission unit for the host to be used after the operating system is deployed.
prefixLength	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to static IPv6 in the Global OS deployment settings.

Macro name	Type	Description
selectedMAC	String	MAC address of the host server to which the IP address is to be bound. The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment, and selectedMAC is set to the newly detected MAC address. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. **Tip:** To obtain the MAC address, use the **macaddress** response property in GET /hostPlatforms.
subnetCIDRNumber	Integer	Subnet mask of the host server to be used after the operating system is deployed, in Classless Inter-Domain Routing (CIDR) format. This is used when the network setting is set to static in the Global OS deployment settings. The CIDR number is typically preceded by a slash "/" and follows the IP address. For example, an IP address of 131.10.55.70 with a subnet mask of 255.0.0.0 (which has 8 network bits) would be represented as 131.10.55.70 /8. For more information, see the CIDR Notation Tutorial webpage. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
subnetMask	String	Subnet mask of the host server to be used after the operating system is deployed, in dotted decimal notation (for example, 255.0.0.0). This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
vlanId	String	VLAN ID for operating-system VLAN tagging. This parameter is valid only if in VLAN mode is enabled. To determine if VLAN mode is enabled use GET /osdeployment/globalSettings in the XClarity Administrator online documentation). **Important:** Only specify a VLAN ID when a VLAN tag is required to function on the network. Using VLAN tags can affect the network routability between the host operating system and the XClarity Administrator.
selectedImage	String	Profile ID of the operating-system image to be deployed. **Tip:** To obtain the operating-system image profile IDs, use the **availableImages** response property in GET /hostPlatforms.
storageSettings	Array	Preferred storage location on which you want to deploy operating-system images

Macro name	Type	Description
targetDevice	String	Target device. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”
unattendFileId	String	ID of the unattend file to be used with this deployment
uuid	String	UUID of the host server to which the operating system is to be deployed
imageSettings	Object	Information about each OS image and image profile
name	String	Operating-system image name
profile	String	Image profile name
otherSettings	Object	Additional settings that are related to the currently running OS deployment jobs
deployDataAndSoftwareLocation	String	Path to the extracted software payload, custom files, and deployment data (such as certificates and logs)

installRepoUrl	String	(SLES 15 and later only) URL for the imported package image
		You can use this predefined macro in the custom unattend for the media_url in the add-on section, for example:
		`<add-on>`
		`  <add_on_products config:type="list">`
		`  <listentry>`
		`  <media_url>`**`#predefined.otherSettings.installRepoUrl#`**
		`  </media_url>`
		`  <product>sle-module-basesystem</product>`
		`  <product_dir>/Module-Basesystem</product_dir>`
		`  </listentry>`
		`  </add_on_products>`
		`</add-on>`

lxcaIp	String	IP address of the XClarity Administrator instance
lxcaRelease	String	XClarity Administrator release (for example. 2.0.0)
jobId	String	ID of the currently running OS deployment job
ntpServer	String	NTP server that is associated with XClarity Administrator
statusSettings	Object	OS deployment status settings
urlStatus	String	HTTPS URL (including the port) that XClarity Administrator uses for reporting status

Macro name	Type	Description
certLocation	String	Folder containing the certificates that are needed to access the **urlStatus** web service from the host OS on first boot
sdkLocation	String	Location of XClarity Administrator provided helper scripts and interfaces for access to the XClarity Administrator
timezone	String	Time zone that is set for XClarity Administrator (for example, America/New_York)
unattendSettings	Object	Settings that are used to populate the unattend file. These values are specific to the version of XClarity Administrator
networkConfig	String	(ESXi and RHEL only) XClarity Administrator predefined content for use at unattend install time. This configures the network settings for the operating system
preinstallConfig	String	XClarity Administrator predefined content for use at pre-installation unattend time. This includes pre-installation status. • For ESXi and RHEL, this uses the %pre pre-installation scripts hook. • For SLES, this uses the <scripts> pre-installation scripts hook. **Attention:** It is strongly recommended that you include this macro in the custom unattend file. You can place the macro in the unattend file anywhere after line 1 (after the <xml> tag).
postinstallConfig	String	XClarity Administrator predefined content for use after the server is configured and booted for the first time. This includes post-installation status. • For ESXi and RHEL, this uses the %post post- installation scripts hook • For SLES, this uses the <scripts> post-installation scripts hook. • For Windows ,this uses the “specialize settings” section. **Attention:** It is strongly recommended that this macro be included in the custom unattend file. You can place the macro in the unattend file anywhere after line 1 (after the <xml> tag).
reportWorkloadNotComplete	String	When this macro is present, the postinstallConfig macro does not report OS Installation Completed (17) status. The custom profile must report complete.
storageConfig	String	(ESXi and RHEL only) XClarity Administrator predefined content for use at unattend install time. This configures the storage settings for the operating system.

Importing custom unattend files

You can import custom unattend files into the OS images repository. These files can then be used to customize Linux and Windows OS-images profiles.

About this task

The following file types are supported for custom unattend files.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Server	Unattend (.xml)	For more information about unattend files, see the Unattended Windows Setup Reference webpage.

Operating system	Supported File Types	More information
Microsoft Windows Hyper-V Server	Not supported	
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	For more information about unattend files, see the Red Hat: Automating the Installation with Kickstart webpage. Consider the following when adding %pre, %post, %firstboot sections in the file. • You can include multiple %pre, %post, %firstboot sections to the unattend file; however, be aware of the ordering of the sections. • When the recommended **#predefined.unattendSettings.preinstallConfig#** macro is present in the unattend file, XClarity Administrator adds a %pre section before all other %pre sections in the file. • When the recommended **#predefined.unattendSettings.postinstallConfig#** macro is present in the unattend file, XClarity Administrator adds %post and %firstboot sections before all other %post and %firstboot sections in the file.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	For more information about unattend files, see the SUSE: AutoYaST webpage.
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Kickstart (.cfg)	Supported only for ESXi 6.0u3 and later updates and 6.5 and later. For more information about unattend files, see the VMware: Installing or Upgrading Hosts by Using a Script webpage. Consider the following when adding %pre, %post, %firstboot sections in the file. • You can include multiple %pre, %post, %firstboot sections to the unattend file; however, be aware of the ordering of the sections. • When the recommended **#predefined.unattendSettings.preinstallConfig#** macro is present in the unattend file, XClarity Administrator adds a %pre section before all other %pre sections in the file. • When the recommended **#predefined.unattendSettings.postinstallConfig#** macro is present in the unattend file, XClarity Administrator adds %post and %firstboot sections before all other %post and %firstboot sections in the file.

Attention:

- You can inject predefined and custom macros (configuration settings) in the unattend file using the unique name of the object. Predefined values are dynamic based on the XClarity Administrator instances. Custom macros are dynamic based on user input that is specified during OS deployment.

  Notes:

  - Surround the macro name with a hash symbol (#).
  - For nested objects, separate each object name using a period (for example, **#server_settings.server0.locale#**).
  - For custom macros, do not include the top-most object name. For predefined macros, prefix the macro name with "predefined."

  - When an object is created from a template, the name is appended with a unique number, starting with 0 (for example, **server0** and **server1**).
  - You can see the name for each macro from the Deploy OS Images dialog on the Custom Settings tabs by hovering over the Help icon ( ) next to each custom setting.
  - For a list of predefined macros, see Predefined macros. For information about custom configuration settings and macros, see Custom macros.
- XClarity Administrator provides the following predefined macros that are used to communicate status from the OS installer, as well as several other critical installation steps. It is strongly recommended that you include these macros in unattend file (see Injecting predefined and custom macros to an unattend file).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

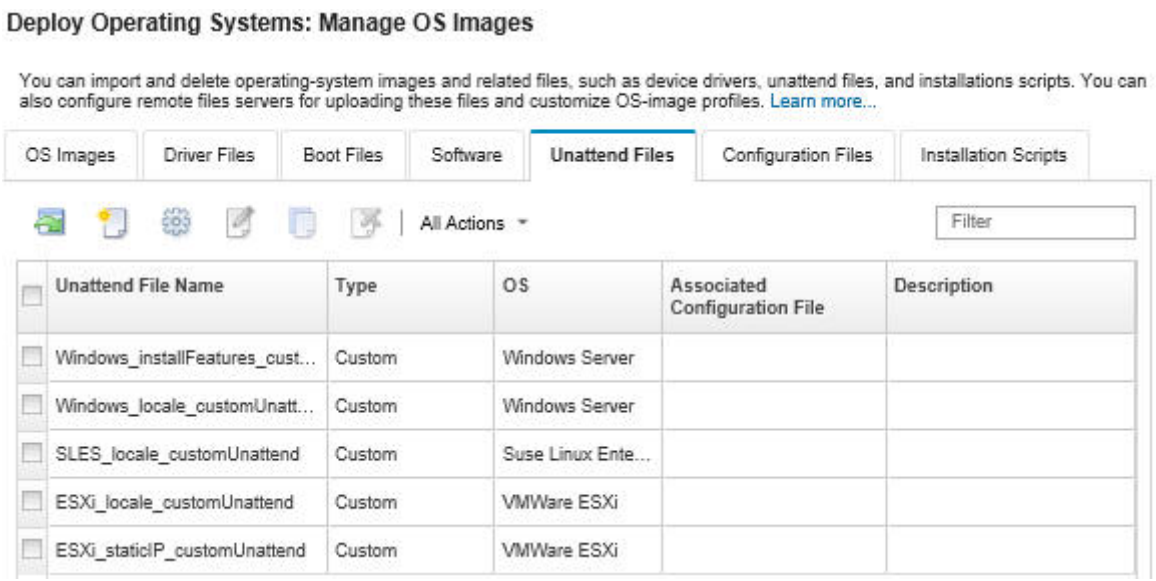
The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

To import unattended files into the OS-images repository, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Unattend Files** tab.



Step 3. Click the **Import File** icon ( ). The Import File dialog is displayed.

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Select the operating-system type.

Step 7. Enter the file name of the unattend file, or click **Browse** to find the file that you want to import.

Step 8. Optional: **Optional:** Enter a description for the unattend file.

Tip: Use the **Description** field to distinguish between custom files with the same name.

Step 9. Optional: **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:
- **MD5**
- **SHA1**
- **SHA256**

Step 10. Click **Import**.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

What to do next

The unattend-file image is listed on the **Unattend Files** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create an unattend file by clicking the **Create** icon ( ).

  The editor identifies the location of any errors that are found in the file. Note that some messages are English only.
- Associate an unattend file with a configuration-settings file (see Associating an unattend file with a configuration settings file).
- View and modify an unattend file by clicking the **Edit** icon ( ).

  The editor identifies the location of any errors that are found in the file. Note that some messages are English only.
- Copy an unattend file by clicking the **Copy** icon ( ).

  If you copy an unattend file that is associated with a configuration-settings file, the associated configuration-settings file is also copied and the association is automatically created between both copied files.
- Remove selected unattend files by clicking the **Delete** icon ( ).
- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).

For information about adding an unattend file to a customized OS image profile, see Creating a custom OS-image profile.

Injecting predefined and custom macros to an unattend file

You can add predefined and custom macros to an unattend file.

About this task

Macros give you the ability to add dynamic data (configuration settings) to an unattend file. You provide the data values when the OS-image profile is deployed.

Lenovo XClarity Administrator provides a set of *predefine* macros that you can add to an unattend file without associating a custom configuration-settings file. For a list of predefined macros, see Predefined macros.

It is strongly recommended that you include the following predefined macros in the custom unattend files.

- **#predefined.unattendSettings.preinstallConfig#** and **#predefined.unattendSettings postinstallConfig#**. Used to communicate status from the OS installer, as well as several other critical installation steps.

  See the following example OS-deployment scenarios for more information about how to include the installation-configuration macros.
  - Deploying RHEL and a Hello World PHP application using a custom unattend file
  - Deploying SLES 12 SP3 with a configurable locale and NTP servers
  - Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address
  - Deploying Windows 2016 with custom features
- **#predefined.unattendSettings.networkConfig#**. (For ESXi and RHEL only) Enables XClarity Administrator to configure the network. This macro uses the network settings that are specified on the Deploy OS Images page. If you do not include this macro in the unattend file or if the network settings are not defined in XClarity Administrator, you must configure the IP interface as part of the unattend file so that the host has a network route back to XClarity Administrator.

  See the following example OS-deployment scenarios for more information about how to include the network-configuration macro.
  - Deploying RHEL and a Hello World PHP application using a custom unattend file
  - Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address
- **#predefined.unattendSettings.storageConfig#**. (For ESXi and RHEL only) Enables XClarity Administrator to configure storage on the host. This macro uses the storage settings that are specified on the Deploy OS Images page. If you do not include this macro in the unattend file or if the storage settings are not defined in XClarity Administrator, you must specify the storage configuration in unattend file.

  See the following example OS-deployment scenarios for more information about how to include the storage-configuration macro.
  - Deploying RHEL and a Hello World PHP application using a custom unattend file
  - Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address

You can create *custom* macros by creating a configuration-settings file and then associating the unattend file with a custom configuration-settings file. When you import the custom configuration-settings file, XClarity Administrator creates a macro for each configuration setting in the file.

Procedure

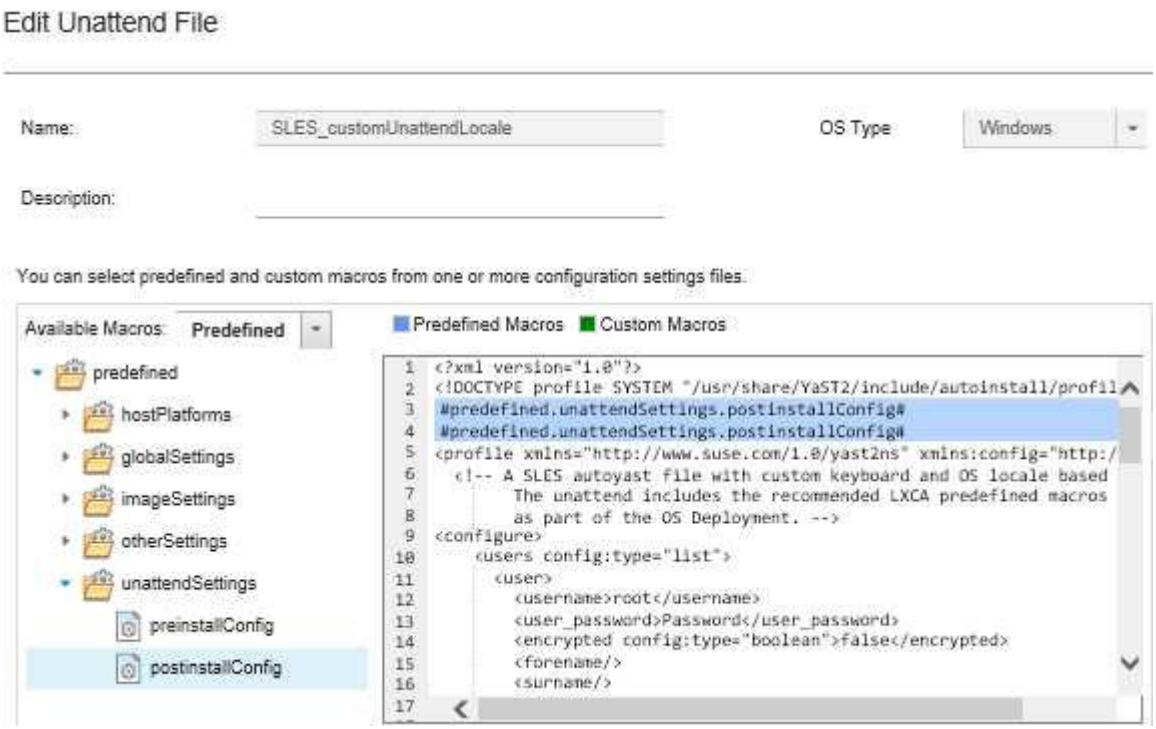
Complete the following steps to add macros to an unattend file.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Unattend Files** tab.

Step 3. Select the unattend file that you want to edit.

Step 4. Click the **Edit** icon ( ) display the Edit Unattend File dialog.



Step 5. Add the recommended predefined macros, for example:

1. Place the cursor in the unattend file anywhere after line 1 (after the <xml> tag).
2. Expand the **predefine → unattendSettings** list in the list of available macros.
3. Click the **preinstallConfig** and **postinstallConfig** to add the required predefined macros to the unattend file.

   The following code is added to the file:

   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#

Step 6. Add additional predefined or custom macros by placing the cursor in the correct location in unattend file and then clicking the macro from the list.

Step 7. Click **Save**.

Associating an unattend file with a configuration settings file

You can associate (bind) configuration settings to an unattend file, and then add the associated custom macros to the unattend file.

About this task

You can add predefined macros to an unattend file without associating a custom configuration settings file.

You cannot edit configuration settings files that are associated with unattend files. However, you can copy an associated file and then edit the copy.

Procedure

Complete the following steps to associate an unattend file with a configuration-settings file.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Unattend Files** tab.

Step 3. Select the custom attend file.

Step 4. Click the **Associate a Configuration File** icon () to display the Associate an Unattend File dialog.

Step 5. Select a configuration-settings file to associate with the unattend file.

Step 6. Add predefined and custom macros to the unattend file by placing the cursor at the location in the editor where you want to add the macro and then clicking the macro in the available list (see Injecting predefined and custom macros to an unattend file).

You can inject macros in the unattend file using the unique name of the object. For nested name objects, separate each object using a period (for example, `server_specific_settings.server.locale`). Note that you do not include the top-most name.

Step 7. Click **Associate** to bind the files together.

Importing custom installation scripts

You can import installation scripts into the OS images repository. These files can then be used to customize Linux and Windows images.

About this task

Currently, only post-installation scripts are supported.

The following table lists the file types for installation scripts that Lenovo XClarity Administrator supports for each operating system. Note that certain operation system versions do not support all of the file types that XClarity Administrator supports (for example, some RHEL versions might not include Perl in the minimal profile and, therefore, Perl scripts will not run). Ensure that you use the correct file type for the operating system versions that you want to deploy.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Server	Command file (.cmd), PowerShell (.ps1)	The default custom data and files path is `C:\lxca`. For more information about installation scripts, see the Add a custom script to Windows Setup webpage
Microsoft Windows Hyper-V Server	Not supported	
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm or .pl), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the RHEL: Post-installation Script webpage.
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm or .pl), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the SUSE: Custom user script webpage

Operating system	Supported File Types	More information
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Bash (.sh), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the VMware: Installation and Upgrade Scripts webpage

Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

After the data is gathered during OS deployment, XClarity Administrator creates an instance of the configuration settings file (which includes the custom settings in the selected file and a subset of predefined settings) on the host system that can be used by the post installation script.

You can inject predefined and custom macros (configuration settings) in the post-installation script using the unique name of the object. Predefined values are dynamic based on the XClarity Administrator instances. Custom macros are dynamic based on user input that is specified during OS deployment.

Notes:

- Surround the macro name with a hash symbol (#).
- For nested objects, separate each object name using a period (for example, **#server_settings.server0.locale#**).
- For custom macros, do not include the top-most object name. For predefined macros, prefix the macro name with "predefined."
- When an object is created from a template, the name is appended with a unique number, starting with 0 (for example, **server0** and **server1**).
- You can see the name for each macro from the Deploy OS Images dialog on the Custom Settings tabs by hovering over the Help icon () next to each custom setting.
- For a list of predefined macros, see Predefined macros. For information about custom configuration settings and macros, see Custom macros.

The recommended predefined macros in the unattend file report final operating-system deployment status and report status when downloading and running post-installation scripts. You can modify the post-installation script to include custom status reporting, depending on the target operating system. For more information, see Adding custom status reporting to installation scripts.

Procedure

To import installation scripts into the OS-images repository, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Installation Scripts** tab.



Step 3. Click the **Import File** icon ( ). The Import Installation Script dialog is displayed.

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Select the operating-system type.

Step 7. Enter the file name of the installation script, or click **Browse** to find the file that you want to import.

Step 8. Optional: **Optional:** Enter a description for the installation script.

Tip: Use the **Description** field to distinguish between custom files with the same name.

Step 9. Optional: **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:

- **MD5**
- **SHA1**
- **SHA256**

Step 10. Click **Import**.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

What to do next

The installation scripts are listed on the **Installation Scripts** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ().
- Remove selected installation scripts by clicking the **Delete** icon ().

For information about adding an installation script to a customized OS image profile, see Creating a custom OS-image profile.

Adding custom status reporting to installation scripts

The recommended predefined macros in the unattend file report final operating-system deployment status and report status when downloading and running post-installation scripts. You can include additional status reporting in the post-installation scripts.

Linux

For Linux, you can use the following **curl** command to report status.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Where <*status_ID*> can be one of the following values.

- **44**. Workload deployment succeeded
- **45**. Workload deployment is running with warning
- **46**. Workload deployment failed
- **47**. Workload deployment message
- **48**. Custom post-install script error

Note that the **curl** command uses predefined macros for the HTTPS URL that Lenovo XClarity Administrator uses for reporting status (**predefined.otherSettings.statusSettings.urlStatus**) and for the folder that contains the certificates that are needed to access the urlStatus web service from the host OS on first boot (**predefined.otherSettings.statusSettings.certLocation**).The following example reports that an error occurred in the post-installation script.

The following example reports that an error occurred in the post-installation script.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

For Wiindows, you can import the **LXCA.psm1** script and then call the following commands to report status.

- **initializeRestClient**

  Initializes the REST client. Use the following syntax to run this command. This command is required before running the reporting commands.

  ```
  initializeRestClient
  ```

- **testLXCAConnection**

  Verifies that the XClarity Administrator can connect to the host server. Use the following syntax to run this command. This command is optional but recommended in the installation script before running the reporting commands..

  ```
  testLXCAConnection -masterIP "#predefined.otherSettings.lxcaIp#"
  ```

- **reportWorkloadDeploymentSucceeded**

Reports a successful-completion message to be logged in the XClarity Administrator jobs log. Use the following syntax to run this command.

Tip: If the **#predefined.unattendSettings.reportWorkloadNotComplete#** macro is included in a custom unatted file or post-installation script, include the **reportWorkloadDeploymentSucceeded** command in the post-installation script to signal a successful-completion. Otherwise, XClarity Administrator automatically reports a complete status after all post-installation scripts are run.

```
reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
-UUID "#predefined.hostPlatforms.uuid#"
```

- **reportWorkloadDeploymentRunningWithWarning**

  Reports a warning message to be logged in the XClarity Administrator jobs log. Use the following syntax to run this command.

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- **reportWorkloadDeploymentFailed**

  Reports a failure message to be logged in the XClarity Administrator jobs log. Use the following syntax to run this command.

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
  ```

- **reportCustomPostInstallScriptError**

  Reports a post-installation script error message to be logged in the XClarity Administrator jobs log. Use the following syntax to run this command.

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- **reportWorkloadDeploymentMessage**

  Reports a general message to be logged in the XClarity Administrator jobs log without affecting the state of the deployment. Use the following syntax to run this command.

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

Where <*message_text*> is the message that you want to return to XClarity Administrator for each status condition.

Note that these commands use predefined macros for the IP address of the XClarity Administrator instance (**#predefined.otherSettings.lxcaIp#**) and for the UUID of the host server to which the operating system is to be deployed (**#predefined.hostPlatforms.uuid#**).

The following example is a PowerShell installation script that installs Java and reports an error if the installation fails

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"

Write-Output "Reporting status to Lenovo XClarity Administator..."
   reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
   -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java...."
   Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
```

```
   [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
   reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
      -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

Importing custom software

You can import software into the OS images repository. These files can then be used to customize Linux and Windows images

About this task

The custom software files are installed after the operating-system deployment and post-installation scripts are complete.

The following file types are supported for custom software.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Server	A .zip file containing the software payload.	The default custom data and files path is `C:\lxca`.
Microsoft Windows Hyper-V Server	Not supported	
Red Hat® Enterprise Linux (RHEL) Server	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.

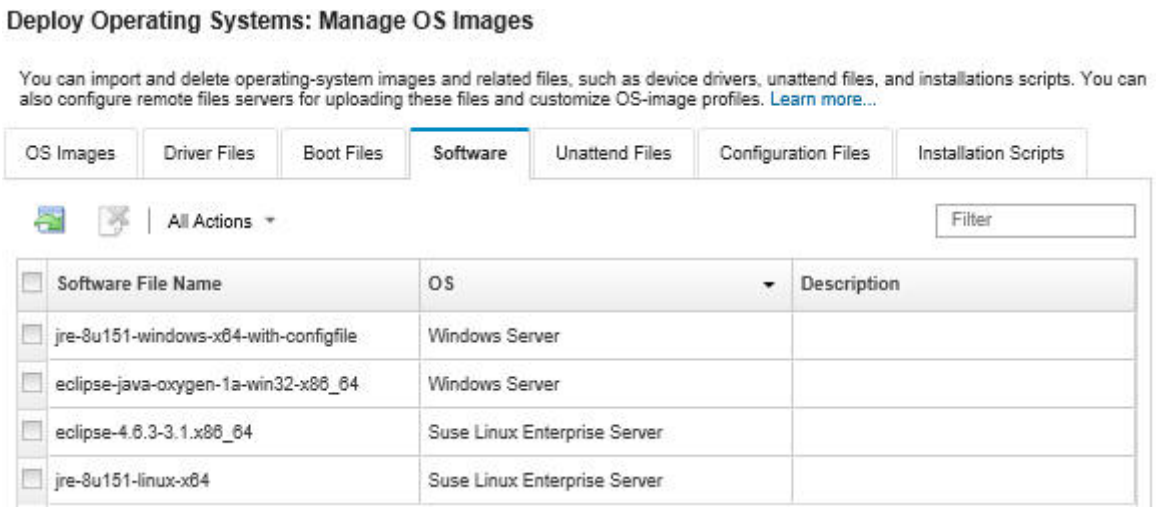
Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

To import software into the OS-images repository, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Software** tab.



Step 3. Click the **Import File** icon ( ). The Import Installation Script dialog is displayed.

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Select the operating-system type.

Step 7. Enter the file name of the software file, or click **Browse** to find the file that you want to import.

Step 8. Optional: **Optional:** Enter a description of the software file.

Tip: Use the **Description** field to distinguish between custom files with the same name.

Step 9. Optional: **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:

- **MD5**
- **SHA1**
- **SHA256**

Step 10. Click **Import**.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

What to do next

The installation scripts are listed on the **Software** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ().
- Remove selected software files by clicking the **Delete** icon ().

For information about adding a software file to a customized OS image profile, see Creating a custom OS-image profile.

Creating a custom OS-image profile

You can add custom device drivers, boot files (Windows only), configuration settings, unattend files, installation scripts, and software to a predefined OS-image profile that exists in the OS-images repository. When you add files to an OS image, Lenovo XClarity Administrator creates a custom profile for that OS image. The custom profile includes the custom files and installation options.

Before you begin

The custom files that you want to add must exist in the OS-images repository (see Importing boot files, Importing device drivers, Importing custom configuration settings, Importing custom unattend files, Importing custom installation scripts, and Importing custom software).

Procedure

To customize an OS image, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **OS Images** tab.

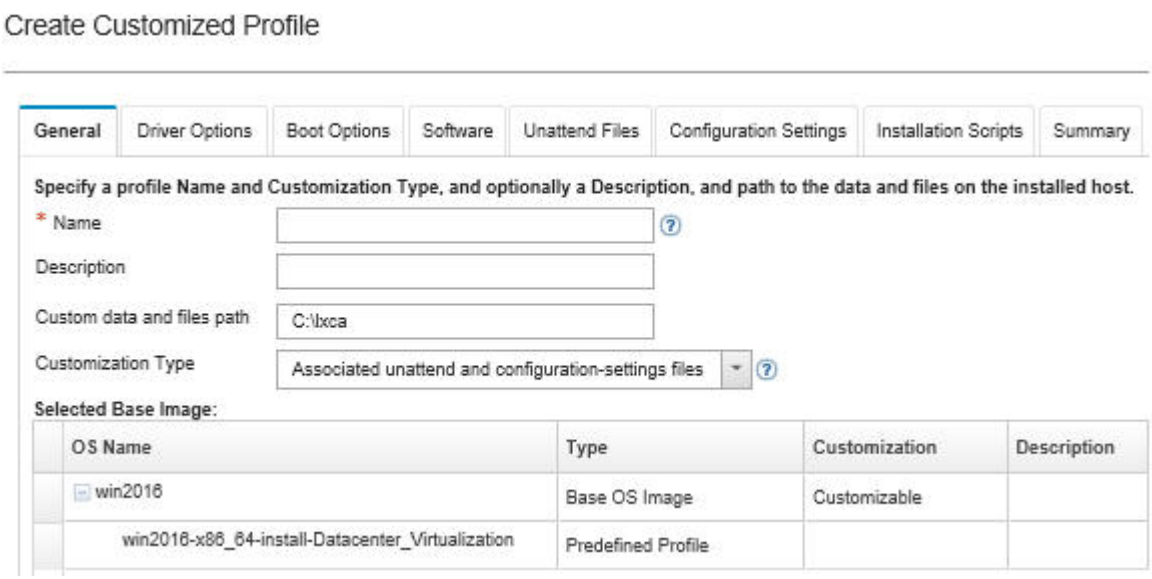
Step 3. Select the predefined OS-image profile that you want to customize.

The **Customization** column identifies which OS images can be customized. Click the **Help** icon () for more information about the customization for a specific OS image.

- **Customizable**. The OS image support customization but is not customized.
- **Non Customizable**. The OS image does not support customization.

Note: You can import additional base OS images (in .iso format) from a local or remote system by clicking the **Import File** icon ().

Step 4. Click the **Create Customized Profile** icon (). The New Custom OS Image dialog is displayed.



Step 5. On the **General** tab, specify a name, description, path for the custom files and deployment data on the deployment host, and customization type for the new customized OS-image profile.

The customization type can be one of the following:
- **Only unattend files**
- **Only configuration files**
- **Unassociated unattend and configuration files**
- **Associated unattend and configuration files**
- **None**

Step 6. Click **Next**.

Step 7. On the **Device Drivers** tab, select the device drive that you want to add to the Linux OS-image profile.

For a list of supported formats, see Importing device drivers.

The selected file is applied after you complete the configuration wizard.

Note: You can import additional device drivers from a local or remote system by clicking the **Import File** icon ( ).

Step 8. Click **Next**.

Step 9. (Windows only) On the **Boot Options** tab, select the boot files that you want to add to the Windows OS-image profile.

For a list of supported formats, see Importing boot files.

The selected file is applied after you complete the configuration wizard.

Step 10. Click **Next**.

Step 11. On the **Configuration Settings** tab (if applicable), select one or more custom configuration files that you want to add to the OS-image profile. You can select at most one file

Step 12. Click **Next**.

Step 13. On the **Unattend Files** tab:

a. Select the unattend file that you want to add to the OS-image profile.

For a list of supported formats, see Importing custom unattend files.

The selected file is applied after you complete the configuration wizard.

b. Select a configuration file to associate with the unattend file from the **Associated Configuration File** column

c. Optionally select custom macros that are available in the selected configuration file or add custom macros in .xml format.

Step 14. Click **Next**.

Step 15. On the **Installation Scripts** tab (if applicable), select the installation scripts that you want to add to the Windows OS-image profile. You can select at most one post-installation script.

For a list of supported formats, see Importing custom installation scripts.

The selected file is applied after you complete the configuration wizard.

Note: You can import additional installation scripts from a local or remote system by clicking the **Import File** icon ( ).

Step 16. Click **Next**.

Step 17. On the **Software** tab, select the software that you want to add to the Linux OS-image profile.

For a list of supported formats, see Importing custom software.

The selected file is applied after you complete the configuration wizard.

Note: You can import additional software from a local or remote system by clicking the **Import File** icon ( ).

Step 18. Click **Next**.

Step 19. Review the settings on the **Summary** tab, and click **Customize** to create the customized OS-image profile.

What to do next

The customized OS images profile is listed under the base operating system on the **OS Images** tab on the Manage OS Images page.

From this page, you can perform the following actions:

- Import a customized OS image profile and apply to a base OS image by clicking **Import/Export Profile → Export Customized Profile Image** (see Importing a customized OS image profile).
- Export a selected customized OS image profile by clicking **Import/Export Profile → Export Customized Profile Image**.
- Modify a selected customized OS image profile by clicking the **Edit** icon ( ).
- Remove a selected customized OS image profile by clicking the **Delete** icon ( ).

Configuring global OS-deployment settings

Global settings serve as defaults settings when operating systems are deployed.

About this task

From the Global Settings page, you can configure the following settings:

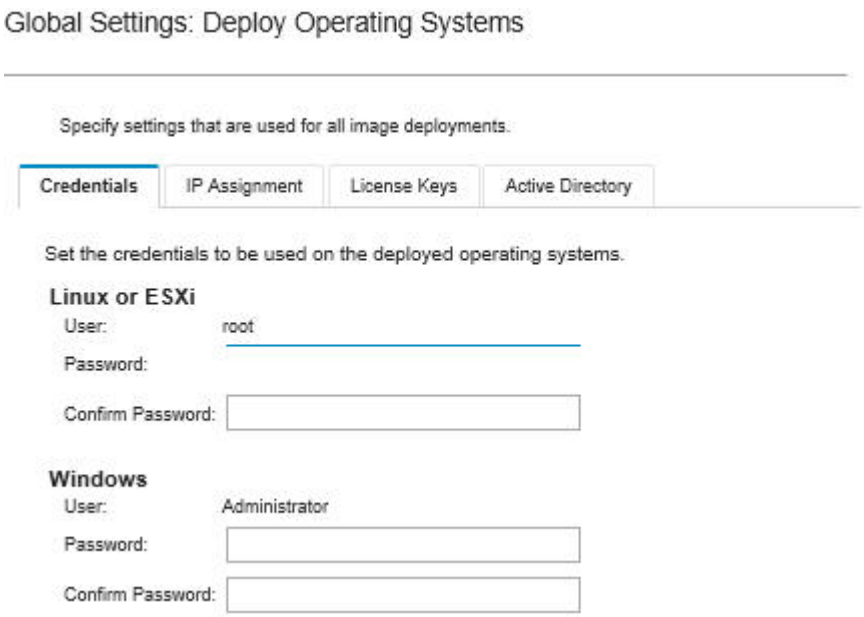
- The password for the administrator user account to be used for deploying the operating systems
- The method to use to assign IP addresses to servers
- License keys to use when activating installed operating systems
- Optionally join an Active Directory domain as part of the Windows operating-system deployment

Procedure

To configure the global settings to be used for all servers, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy OS Images page.

Step 2. Click the **Global Settings** icon ( ) to display the Global Settings: Deploy Operating Systems dialog.



Step 3. On the **Credentials** tab, enter the password for the administrator account to be used to log in to the operating system.

Step 4. On the **IP Assignment** tab, select the following options.

a. **Optional:** Select **Use VLANs** to allow configuring VLAN settings in the Network Settings dialog (see Configuring network settings for managed servers).

Notes: Notes:

- VLAN tagging is not supported for Linux operating-system deployments.
- VLAN tagging is not supported for operating-system deployments on ThinkServer devices.
- VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server.

b. Select the method for assigning IP addresses when configuring the deployed operating system:

Note: The XClarity Administrator network interface that is used for management must be configured to connect to the baseboard management controller using the same IP address

method that you choose on the Global Settings: Deploy Operating Systems dialog. For example, if XClarity Administrator is set up to use eth0 for management, and you choose to use manually assigned static IPv6 addresses when configuring the deployed OS, then eth0 must be configured with an IPv6 address that has connectivity to the baseboard management controller.

- **Manually assign a static IPv4 address**. If you choose to assign static IPv4 addresses, ensure that you configure the static IPv4 address, gateway address, and subnet mask for the server before deploying the operating system (see Configuring network settings for managed servers).
- **Use Dynamic Host Configuration Protocol (DHCP) to assign the addresses**. If you already have an existing DHCPv4 infrastructure in your network, you can use that infrastructure to assign IP addresses to servers.

  Note: DHCP IPv6 is not supported for operating-systems deployment.
- **Manually assign a static IPv6 address**. If you choose to assign static IPv6 addresses, ensure that you configure the static IPv6 address, gateway address, and subnet mask for the server before deploying the operating system (see Configuring network settings for managed servers).

Step 5. Optional: **Optional:** On the **License Keys** tab, specify the global volume-license keys to use when activating installed Windows operating systems.

When you specify global volume-license keys on this tab, you can select the specified license keys for any Windows OS-image profiles from the Deploy OS Images page.

Tip: XClarity Administrator supports global volume-license keys for Windows installations and individual retail-license keys for both Windows and VMware ESXi. You can specify individual retail-license keys as part of the deployment procedure (see Deploying an operating-system image).

Step 6. Optional: **Optional:** On the **Active Directory** tab, configure the Active Directory settings for Windows operating-system deployments. For information about integrating with Active Directory, see Integrating with Windows Active Directory.

Step 7. Click **OK** to close the dialog.

Configuring network settings for managed servers

Network settings are configuration options that are specific to each server. You must configure the network settings for a managed server before you can deploy an operating system to that server.

About this task

If you are using DHCP to assign IP addresses dynamically, you must configure the MAC address.

If you are using static IP addresses, you must configure the following network settings for a specific server before you can deploy an operating system to that server. After these settings are configured, the deployment status of the server changes to “Ready.” (Note that some fields are not available for static IPv6 addresses.)

- Hostname

  The hostname must comply with the following rules:
  - The hostname of each managed server must be unique.
  - The hostname can contain strings (labels) that are separated by a period (.).
  - Each label can contain ASCII letters, digits, and dashes (-); however, the string cannot start or end with a dash and cannot contain all digits.
  - The first label can be 2 - 15 characters in length. Subsequent labels can be 2 – 63 characters in length.

  - The total length of the hostname must not exceed 255 characters.
- MAC address of the port on the host where the operating system is to be installed.

  The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment.

  You can determine the status of the MAC address port that is used for OS deployment from the **MAC address** drop-down menu on the Network Settings dialog. If multiple ports are up or if all ports are down, AUTO is used by default.

  Notes:

  - Virtual network ports are not supported. Do not use one physical network port to simulate multiple virtual network ports.
  - When the server's network setting is set to AUTO, XClarity Administrator can automatically detect network ports in slots 1 – 16. At least one port in slots 1 – 16 must have a connection to XClarity Administrator.
  - If you want to use a network port in slot 17 or greater for the MAC address, you cannot use AUTO. Instead, you must set the server's network setting to the MAC address of the specific port that you want to use.
  - For ThinkServer servers, not all host MAC addresses are displayed. In most cases, MAC addresses for AnyFabric Ethernet adapters are listed on the Edit Network Settings dialog. MAC addresses for other Ethernet adapters (such as the Lan-On-Motherboard) are not listed. In cases where the MAC address for an adapter is not available, use the AUTO method for non-VLAN deployments.
- IP address and subnet mask
- IP gateway
- Up to two domain name system (DNS) servers
- Maximum transmission unit (MTU) speed
- VLAN ID, if VLAN IP mode is enabled

If you choose to use VLANs, you can assign a VLAN ID to the host network adapter that is being configured.

Procedure

To configure network settings for one or more servers, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy Operating System: Deploy OS images page.

Step 2. Select one or more servers to configure. You can select up to 28 servers to be configured at one time.

Step 3. Click **Changed Selected → Network Settings** to display the Edit Network Settings page.

Step 4. Complete the fields in the table for each server.

Tip: As an alternative to filling in each row, you can update all rows in the table for some of the fields:

a. Click **Change All Rows → Hostname** to set the hostnames for all servers, using either a predefined or a custom naming scheme.

b. Click **Change All Rows → IP address** to assign a range of IP addresses, subnet mask, and gateway. The IP address is assigned for each server, starting with the first IP address and ending with the last IP address that is displayed. The subnet mask, and gateway IP address are applied to each server.

c. Click **Change All Rows → Domain Name System (DNS)** to set the DNS servers to be used by the operating system for DNS lookup. If the network defines DNS servers automatically, or if you do not want to define DNS servers, select **None**.

d. Click **Change All Rows → Maximum Transmission Unit (MTU)** to set the MTU to be used on the configured Ethernet adapter on the deployed operating system.

e. Click **Change All Rows → VLAN** to set a specific VLAN ID for operating-system VLAN tagging.

   This option is available only when Use VLANs is enabled on the Global Settings dialog (see Configuring global OS-deployment settings).

   Important:

   - Only specify a VLAN ID when a VLAN tag is required to function on the network. **Using VLAN** tags can affect the network routability between the host operating system and the XClarity Administrator.
   - Chassis or top-of-rack switches must be independently configured to handle VLAN tagged packets. Ensure that XClarity Administrator and the data network are configured to handle these packets correctly.
   - VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server.

Step 5. Click **OK** to save the settings. Settings are saved and persistent only in your web browser's local storage cache.

Results

Each configured server now shows **Ready** as the deployment status on the Deploy Operating System: Deploy OS images page.

Choosing the storage location for managed servers

Choose the preferred storage location where you want to deploy the operating-system image for one or more servers.

Before you begin

Review storage and boot-option considerations before choosing a storage location (see Operating-system deployment considerations).

You can deploy an operating system to the following types of storage:

- **Local disk drive**

  Only disks attached to a RAID-controller or SAS/SATA HBA are supported.

  Lenovo XClarity Administrator installs the operating-system image on the first enumerated local RAID disk in the managed server.

  If the RAID configuration on the server is not configured correctly, or if it is inactive, the local disk might not be visible to Lenovo XClarity Administrator. To resolve the issue, enable the RAID configuration through configuration patterns (see Defining local storage) or through the RAID management software on the server.

  Notes:

  – If an M.2 drive is also present, the local disk drive must be configured for hardware RAID.

- If an SATA adapter is enabled, the SATA mode *must not* be set to “IDE.”
- For ThinkServer servers, operating systems can be deployed only to the local disk. SAN storage and embedded hypervisors are not supported.
- For ThinkServer servers, configuration is available only through the RAID management software on the server.

For an example scenario for deploying VMware ESXi 5.5 to a locally installed disk drive, see Deploying ESXi to a local hard drive.

- **(ESXi only) Embedded hypervisor (USB or SD media adapter)**

  This location is applicable only when a VMware ESXi image is being deployed to managed servers.

  The embedded hypervisor can be one of the following devices:

  - IBM License USB key (PN 41Y8298) or Lenovo Licensed USB key that is mount to a specific port on one of the following servers:
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - SD media adapter that is installed on the following servers:
    - Flex System x240 M5
    - System x3500 M5
    - System x3550 M5
    - System x3650 M5

    In addition, the drive must be configured as follows:
    - The appropriate drives on the media adapter must be defined.
    - The mode of the SD media adapter must be set to **Operational**.
    - The owner must be set to System or System Only.
    - Access must be set to Read/Write.
    - The drive must be assigned a LUN number of 0.

    Important: If the SD Media Adapter is not configured correctly, operating system deployment to the SD Media Adapter from the Lenovo XClarity Administrator will not be successful.

    You can change the mode of the SD Media Adapter to **Configuration** and configure the media adapter through the management controller CLI using the **sdraid** command. For additional information about setting the mode of the SD Media Adapter and configuring the adapter from the CLI, see the Integrated Management Module II online documentation.

  If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment.

  Note: Attempting to deploy Microsoft Windows to a managed server that has a hypervisor key installed might cause issues even if you do not select the embedded hypervisor key. If Windows deployment errors occur, remove the embedded hypervisor key from the managed server, and attempt to deploy Microsoft Windows to that server again.

- **M.2 drive**

  Lenovo XClarity Administrator installs the operating-system image on the first M.2 drive that is configured on the managed server.

  M.2 storage is supported only on ThinkSystem servers.

Attention: If a managed device has both local drives (SATA, SAS, or SSD) that are not configured for hardware RAID and M.2 drives, you must disable the local drives if you want to use M.2 drives, or you must disable the M.2 drives if you want to use local drives. You can disable on-board storage controller devices and legacy and UEFI storage option ROMs using the using Configuration Patterns by selecting Disable local disk on the Local Storage tab of the wizard or by creating a Configuration Pattern from an existing server and then disabling the M.2 devices in the extended UEFI pattern.

- **SAN storage**

  Lenovo XClarity Administrator installs the operating-system image on the SAN boot target that is configured on the managed server.

  The following protocols are supported.
  - Fibre Channel
  - Fibre Channel over Ethernet
  - SAN iSCSI (using only Emulex VFA5.2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW or Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW adapters)

  On managed rack servers, you can only deploy Windows or RHEL to SAN storage. Ensure that the SAN boot target is configured on the managed servers. You can also configure the FC SAN boot target using a server pattern (see Defining boot options)

  When deploying VMware ESXi:

  - Local hard disks must be disabled or removed from the server. You can disable the local hard disks using server patterns (see Defining local storage).
  - If multiple SAN volumes are available, only the first volume is used for deployment.

  Ensure that the OS volume to which you are installing is the only volume that is visible to the operating system.

  For an example scenario for deploying VMware ESXi 5.5 to SAN volumes that are attached to servers, see Deploying ESXi to SAN storage.

Note: Each server must have a hardware RAID adapter or SAS/SATA HBA that is installed and configured. The software RAID that is typically present on the onboard Intel SATA storage adapter or storage that is set up as JBOD are not supported; however, if a hardware RAID adapter is not present, setting the SATA adapter to **AHCI SATA mode** enabled for operating-system deployment or setting unconfigured good disks to JBOD might work in some cases. For more information, see OS installer cannot find the disk on which you want to install XClarity Administrator in the XClarity Administrator online documentation.

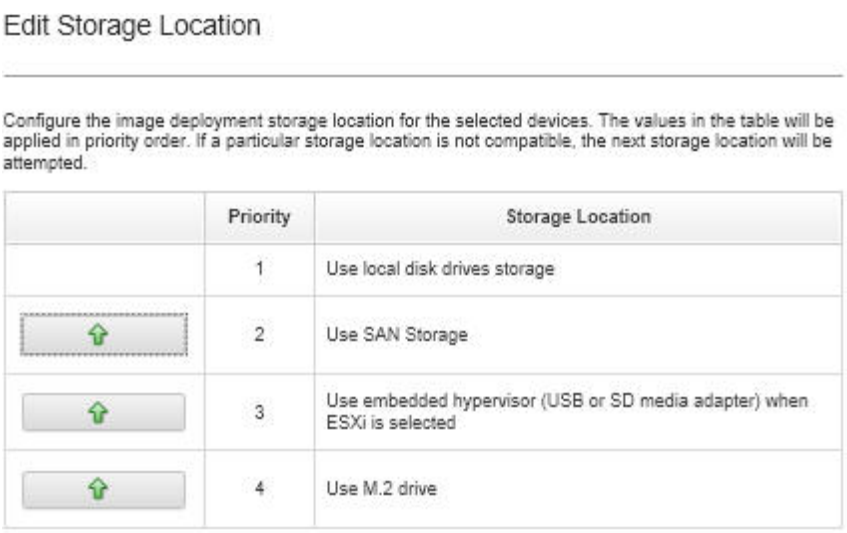
Procedure

To choose storage location for one or more managed servers, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy OS Images page.

Step 2. Select the servers for which you want to change the storage settings.

Step 3. Click **Change Selected → Storage Location** to change the priority order of storage locations for all selected servers. If the first storage location is not compatible, the next storage location is attempted.



You can set the priority for the following storage locations:
- **Use local disk drive storage**
- **Use embedded hypervisor (USB or SD media adapter) when ESXi is selected**
- **Use M.2 drive**
- **Use SAN storage**

Step 4. For each server, select the preferred storage location where you want to deploy the operating-system image from the **Storage** column. You can choose from the following values, which correspond to values in the previous step.
- **Local Disk Drive**
- **Embedded Hypervisor**
- **M.2 Drive**
- **SAN Storage**

If you select **SAN Storage**, a dialog is displayed to configure the SAN volume. Ensure that the target SAN volume is reachable during deployment.

If the selected storage location is not compatible with the server, Lenovo XClarity Administrator attempts to deploy the operating system to the next storage location in the priority defined in the previous step.

Deploying an operating-system image

You can use Lenovo XClarity Administrator to deploy an operating-system image to up to 28 servers concurrently.

Before you begin

Read the operating-system deployment considerations before you attempt to deploy operating systems on your managed servers (see Operating-system deployment considerations).

On the **OS Images** tab, ensure that the **Deploy Status** of the operating system that you want to deploy is set to “Ready.” To deploy the Windows operating system, a WinPE boot file is required. If a matching WinPE file is not available, the **Deploy Status** is set to “Not Ready” and the operating system cannot be deployed. You must manually download and import a WinPE file (see Importing boot files).

From the Manage OS Images page, you can filter the list of OS images by clicking **Show All → Deploy Status**. You can filter the list to show only servers that have a status of “Ready,” “Not Ready,” and “Warning”.

Note: If the deployment status for an operating-system image is “Not Ready,” the operating system is not included in the list of deployable operating systems.

The English locale is supported by default. To specify a language-specific locale, you must use a custom configuration file and unattend file. For more information, see Deploying SLES 12 SP3 with a configurable locale and NTP servers and Deploying Windows 2016 for Japanese .

Note: Operating-system deployment to non-RAID attached storage is not supported.

Attention: If the server currently has an operating system installed, deploying an OS-image profile will overwrite the current operating system.

Procedure

To deploy an operating-system image to one or more managed servers, complete the following steps.

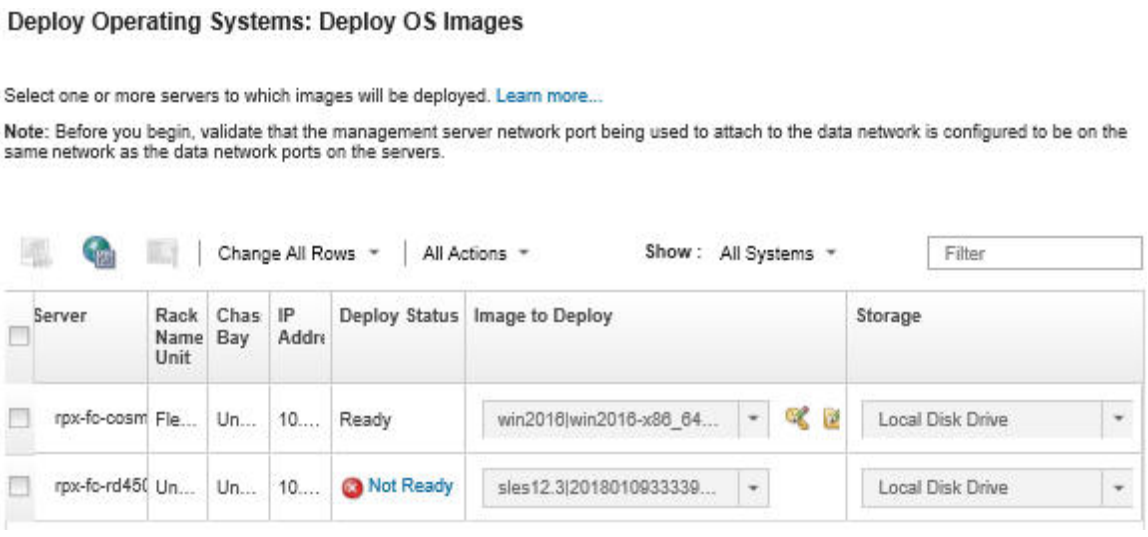
Step 1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy Operating System: Deploy OS images page.

Tip: For scalable complexes, the operating system is deployed on the primary partition; therefore, only the primary partition is included in the server list.

Step 2. Select one or more servers to which the operating system is to be deployed. You can deploy an operating system on up to 28 servers at one time.

You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed devices by selecting an option in the **Show** menu to list only devices in a specific chassis, rack, or group or by entering text (such as a name or IP address) in the **Filter** field.

Tip: You can choose multiple compute nodes from multiple chassis if you intend to deploy the same operating system to all compute nodes.



Step 3. Click **Change Selected → Network Settings** to configure network settings.

For more information, see Configuring network settings for managed servers.

Step 4. For each server, select the OS-image profile to be deployed from the drop-down list in the **Image to Deploy** column.

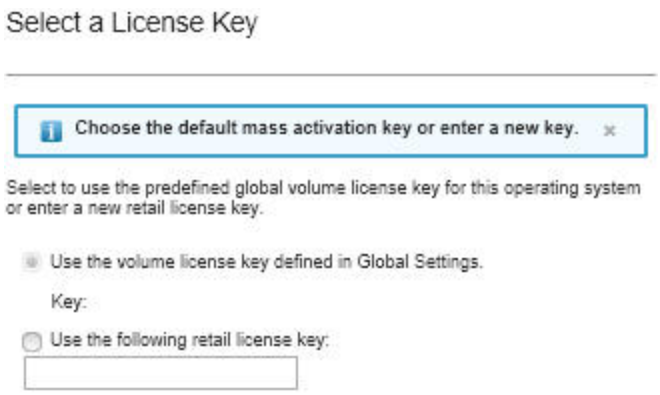
Ensure that you select an OS-image profile that is compatible with the selected server. You can determine compatibility from profile attributes that are listed the **Attribute** column on the Manage OS Images page. For information about profile attributes, see Operating-system image profiles.

Step 5. For each server, click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.

XClarity Administrator supports default volume-license keys for Windows installations and individual retail keys for both Windows and VMware ESXi.

To use the global volume-license key that you specified in the Global Settings dialog, select **Use the volume license key defined in Global Settings**. For more information about global volume-license keys, see Configuring global OS-deployment settings.

To use an individual retail-license key, select **Use the following retail license key**, and enter the key in the following field.



Step 6. Optional: **Optional:** If you selected a Windows operating system for any server, you can join the Windows operating system to an Active Directory domain as part of the operating-system deployment by clicking the **Folder** icon ( ) that is displayed next to the operating-system image, and then selecting the Active Directory name.

To use the default Active Directory that you specified in the Global Settings dialog, select **Use the Active Directory defined in Global Settings**. For more information about joining an Active Directory domain, see Integrating with Windows Active Directory.

To use an individual Active Directory, select **Use the following Active Directory**, and select the Active Directory domain.

Step 7. For each server, select the preferred storage location where you want to deploy the operating system image from the **Storage** column.
- **Local Disk Drive**
- **Embedded Hypervisor**
- **M.2 Drive**
- **SAN Storage**

If the selected storage location is not compatible with the server, XClarity Administrator attempts to deploy the operating system to the next storage location in the priority.

Note: For ThinkServer servers, only **Local disk** is available

For more information about how to configure the storage location, see Choosing the storage location for managed servers.

Note: To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

Step 8. Verify that the deployment status for all selected servers is Ready.

Important: Ensure that the deployment status of all selected servers is Ready. If the status of a server is Not Ready, you cannot deploy an operating-system image to that server. Click the **Not Ready** link to get information to help resolve the problem. If the network settings are not valid, click **Change Selected → Network Settings** to configure the network settings.

Step 9. Click the **Deploy images** icon () to initiate the operating-system deployment.

If custom configuration settings were added to the OS-image profile, the **Custom Settings** tab is displayed on the Deploy OS Image dialog. Specify custom settings, common server settings, and specific server settings, and then click **Next** to continue with the OS deployment. Note that OS deployment will not proceed if input is not specified for any required custom configuration settings.

What to do next

You can monitor the status of the deployment process from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**. For more information about the job log, see Monitoring jobs.

You can also set up a remote-control session through the baseboard management controller for the server to watch the installation as it progresses. For more information about remote control, see Using remote control to manage Converged, Flex System, NeXtScale, and System x servers.

Deployment information is saved for the operating system. You can view the deployment information by clicking **Provisioning → Manage OS Access**, and then hovering over the server name.

Integrating with Windows Active Directory

When you deploy a Windows image using Lenovo XClarity Administrator, you are able to join an Active Directory domain as part of the operating-system deployment.

Before you begin

To join an Active Directory domain as part of a Windows image deployment, you must configure both the management server and the Windows Server that is running the affected Active Directory domain controller. To perform this configuration, you need the following access:

- An administrator account with the authority to authenticate and join the Active Directory servers domain. This account must have privileges similar to those of the default Domain Administrators group, and you can use an account in this group for this configuration.
- Access to a domain name system (DNS) that resolves to the Active Directory server that is running the domain controller. This DNS must be specified in the **Network Settings → DNS** option for the server to which you are deploying the operating system.
- The Active Directory server administrator must create the required computer name on the domain server before you deploy the operating system. The join attempt does not create computer name. If no name is specified, the join fails.
- The Active Directory server administrator must specify the hostname of the server to which the image is being deployed as a computer name under the target organizational unit by clicking the **Network Settings → Hostname** field.

The specified hostname (computer name) must be unique. Specifying a name that is already in use by another Windows installation causes the join the fail.

You can join the Active Directory domain using one of the following methods:

- **Use an Active Directory domain**

  You can choose to use a specific Active Directory domain from a list of predefined domains. Complete the following steps to define an Active Directory domain in XClarity Administrator. If you intend to use multiple domains, repeat these steps for each domain name.

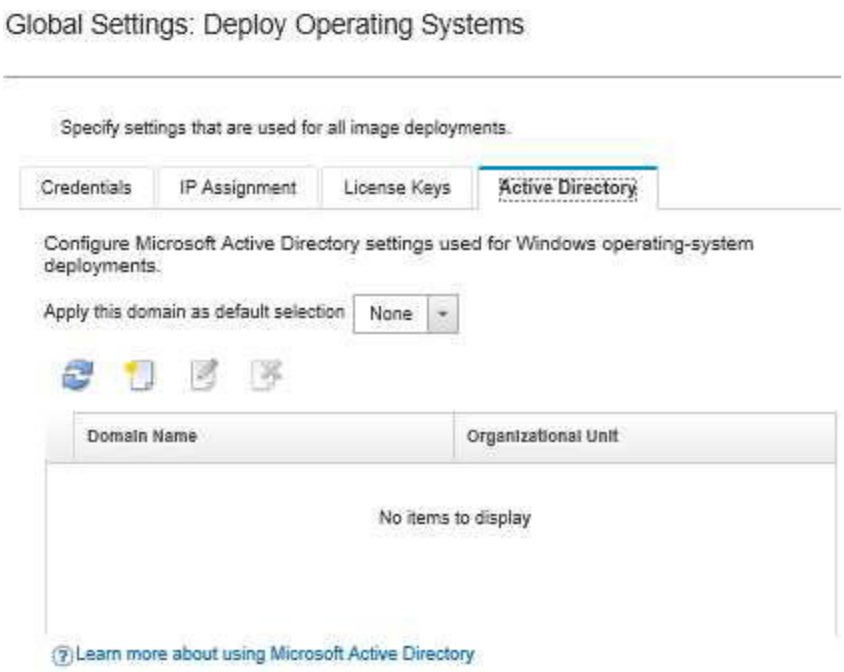
  1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy OS Images page.
  2. Click the **Global Settings** icon ( ) to display the Global Settings: Deploy Operating Systems dialog.
  3. Click The **Active Directory** tab.
  4. Click the **Create** icon ( ) to display the Add New Active Directory Domain dialog.
  5. Specify the domain name and organizational unit.

     Operating-system deployment supports joining a domain and creating nested organizational units within a domain. If you are specifying organizational units, it is not necessary to specify the OU as part of the join explicitly. Active Directory is able to derive the correct OU using the domain name and computer name.
  6. Click **OK**.

- **Use the default Active Directory domain**

  You can choose to use the default Active Directory domain that is defined in global settings. Complete the following steps to set the default Active Directory domain in XClarity Administrator.

  1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy OS Images page.
  2. Click the **Global Settings** icon ( ) to display the Global Settings: Deploy Operating Systems dialog.
  3. Click The **Active Directory** tab.



4. From the **Apply this domain as default selection** drop-down menu, select the Active Directory domain to be used by default for every Windows deployment.
5. Click **OK**.

- **Use metadata blob data**

  You can use Active Directory Computer Account Metadata (in Base-64 encoded blob format) to join the Active Directory domain for any server. Complete the following steps to generate metadata blob data.

  1. Use an administrator account to log in to the computer. The computer must be part of the Active Directory domain to which you are joining.
  2. Click **Start → Programs → Accessories**. Right-click **Command Prompt**, and then click **Run as administrator**.
  3. Change to the C:\windows\system32 directory.
  4. Run the **djoin** command using the following format to perform an offline domain join:
     `djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob`

     where:

     – *<AD_domain_name>* is the name of the Active Directory domain.

     – *<hostname>* is the hostname of the server to which the image is being deployed as a computer name under the target organizational unit by clicking the **Network Settings → Hostname** field.

     This command creates a file named `blob` that contains the metadata blob data. The content of this file is used by the operating-system deployment process to specify the Active Directory join details, so keep this data close by.

     The metadata blob data is sensitive data.

For detailed information about deploying an operating-system image, see Deploying an operating-system image.

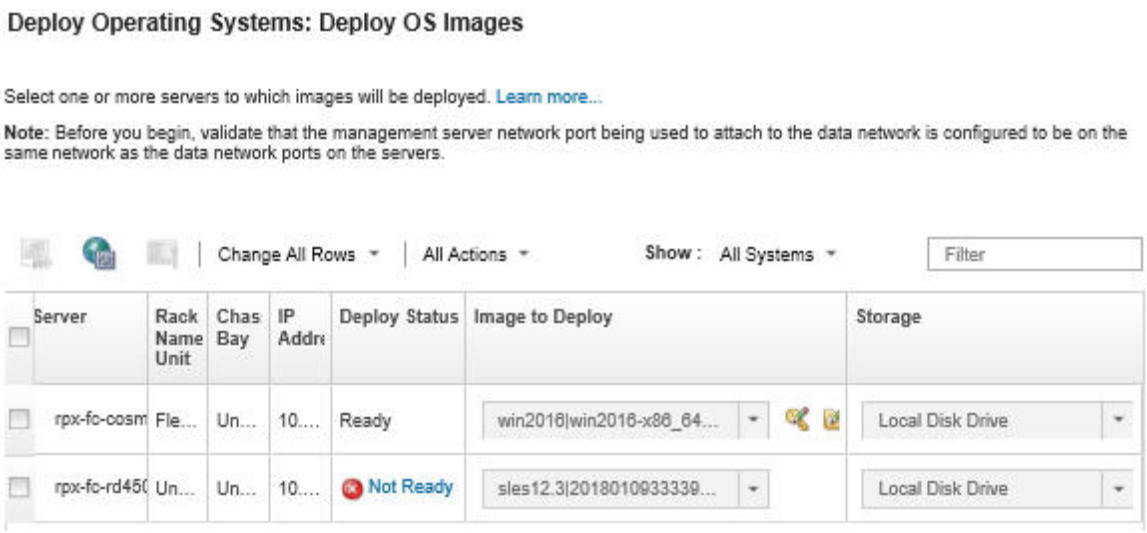
Procedure

To join an Active Directory domain, complete the following steps.

Step 1. Import the Windows operating-system image in to the OS images repository (see Importing operating-system images).

Step 2. Select one or more servers to which the operating system is to be deployed. You can deploy an operating system on up to 28 servers at one time.

Tip: You can choose multiple compute nodes from multiple chassis if you intend to deploy the same operating system to all compute nodes.



Step 3. Click **Change Selected → Network Settings** to configure network settings.

a. Click **Change All Rows → Domain Name System (DNS)**, and specify at a minimum a DNS that resolves to the Active Directory domain.

b. For each server, specify a hostname that matches an existing computer name in the domain and organizational unit that you are joining.

For more information about setting network settings, see Configuring network settings for managed servers.

Step 4. For each server, select the Windows operating-system image to be deployed in the **Image to Deploy** column. A folder and license key icons is displayed next to the image name.

Step 5. For each server, click the **License Key** icon (), and specify the license key to use to active the operating system after it is installed:

Step 6. For each server, click the **Folder** icon (), and specify the Active Directory domain. You can choose one of the following values:

- **Use the Active Directory defined in Global Settings** to use the default domain.
- **Use the following Active Directory** to select a specific domain.
- **Use metadata block data** to specify the contents of the blob file.

  The metadata blob data contains sensitive information and is not displayed in the field. This information is available only until the deployment operation is complete. It is not persistent.

Step 7. For each server, select the preferred storage location where you want to deploy the operating-system image from the **Storage** column.

- **Local Disk Drive**
- **Embedded Hypervisor**
- **M.2 Drive**
- **SAN Storage**

If the selected storage location is not compatible with the server, XClarity Administrator attempts to deploy the operating system to the next storage location in the priority.

For more information about how to configure the storage location, see Choosing the storage location for managed servers.

Note: To ensure that operating- system deployments are successful, detach all storage from the managed server except the storage chosen for the operating-system deployment.

Step 8. Verify that the deployment status for all selected servers is Ready.

If the status of a server is Not Ready, you cannot deploy an operating-system image to that server. Click the **Not Ready** link to get information to help resolve the problem. If the network settings are not valid, click **Changed Selected → Network Settings** to configure the network settings.

Step 9. Click the **Deploy images** icon () to initiate the operating-system deployment.

The Deploy Confirmation dialog prompts you for the credentials to use for authenticating to the Active Directory server and joining the domain. For security reasons, these credentials are not stored in XClarity Administrator. You must supply the credential for every Windows deployment that joins the domain.

You can monitor the status of the deployment process from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**. For more information about the job log, see Monitoring jobs.

Results

When the operating-system deployment is complete, open a web browser to the IP address that you specified on the Edit Network Settings page, and log on to continue with the configuration process.

OS-deployment scenarios

Use these scenarios to help you customize and deploy operating systems to your managed servers.

Deploying RHEL with custom device drivers

This scenario installs the Red Hat Enterprise Linux (RHEL) operating system and additional device drivers that are not available in the base operating system. A custom profile is used that includes the additional device drivers. The custom profile can then be selected on the Deploy OS Images page.

Before you begin

When deploying operating systems using Lenovo XClarity Administrator, the operating system must include the appropriate Ethernet, Fibre Channel, and storage-adapter device drivers for your hardware. If a device driver is not included in the operating system, that adapter is not supported for OS deployment. In XClarity Administrator v1.2.0 and later, you can customize an operating system by adding device drivers.

You can obtain device drivers from the Lenovo YUM Repository webpage, from the vendor (such as Red Hat), or through a custom device driver that you generated yourself. For some Windows device drivers, you can generate a custom device driver by extracting the device driver from the installation .exe to your local system and creating a .zip archive file.

Note: RHEL device drivers must be in .rpm or .iso image format.

Procedure

To deploy RHEL with custom device drivers, complete the following steps.

Step 1. Download the base RHEL operating system from the Red Hat website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.

3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the RHEL image to import (for example, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the custom device drivers to the local system and import the files into the OS-images repository. For more information, see Importing device drivers.

1. Click the **Device Drivers** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `RHEL` for the operating system.
5. Select the operating-system version.
6. Select the device type.
7. Click **Browse** to find and select the device driver to import (for example, `kmod-i40e-2.0.12-1.el7.x86_64.rpm`).
8. Click **Import** to upload the file to the OS-images repository.

Step 3. Create a custom OS-image profile that includes the custom device drivers. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom RHEL with device drivers`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **None** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, select the custom device drivers to include in profile, and click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, click **Next**.
7. Click **Customize** to create the custom OS-image profile.

Step 4. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.

   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom RHEL with device drivers`) from the drop-down list in the **Image to Deploy** column.

Note: Ensure that all target servers use the same custom profile.

d. (Optional) Click the **License Key** icon () and specify the license key to use to activate the operating system after it is installed.

e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

f. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon () to initiate the operating-system deployment.
4. On the **Summary** tab, review the settings.
5. Click **Deploy** to deploy the operating system.

Deploying RHEL and a Hello World PHP application using a custom unattend file

This scenario installs the RHEL operating system along with custom software (Apache HTTP, PHP, and a hello-world PHP application). A custom OS-image profile is used that includes the custom unattend that registers the operating system with the internal Lenovo RHEL subscription service so that it can use the yum repositories, installs the Apache and PHP packages, configures the firewall to allow Apache connections, creates a Hello World PHP application and copies to the Apache web server directory, and configures the Apache configuration files to support PHP.

Before you begin

You can deploy RHEL with custom software in a few different ways. This example uses a custom attend file that you include in the custom OS-image profile. You can also use a post-installation script that installs custom software that you import into the repository and include in the custom OS-image profile. For installing software using a post-installation script, see Deploying RHEL and a Hello World PHP application using custom software and a post-installation script.

This scenario uses the following sample file.

- RHEL_installSoftware_customUnattend.cfg This custom unattend file uses values in predefined and custom macros and installs and configures the custom software.

Procedure

To deploy RHEL with custom software using a custom unatttend file, complete the following steps.

Step 1. Download the base RHEL operating system from the Red Hat website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the RHEL image to import (for example, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).

6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Modify the RHEL unattend (kickstart) file to register the operating system with your RHEL satellite subscription service, install HTTP (Apache) and PHP packages, and create a simple Hello World PHP application, add the required predefined macros and other predefined macros where applicable, such as the IP address, gateway, DNS and host name settings, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

Add commands to register the host with your RHEL satellite, for example:

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

Important: In the example unattend file, specify the IP address of your satellite server and your organization based on our subscription service configuration.

Add commands to update the host and to install and configure apache and php packages, for example:

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
php
php-mysql
php-gd
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original

sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

Note: The example unattend file modifies the default packages that are being installed with the kickstart file. It specifies the Apache and PHO packages as part of the %packages section.

For ESXi and RHEL only, XClarity Administrator provides the **#predefined.unattendSettings.networkConfig#** macro, which adds all network settings that are defined in the UI to the unattend file, and the **#predefined.unattendSettings.storageConfig#** macro, which adds all storage settings that are defined in the UI to the unattend file. The example unattend file already contains these macros.

XClarity Administrator also provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file. The example file already contains the required macros.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

The example file already contains the required macros and additional predefined macros for dynamically specifying network settings for the target server and timezone. For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file.

You can also add commands to send custom messages to the jobs log in XClarity Administrator. For more information, see Adding custom status reporting to installation scripts.

To import the custom installation script, complete these steps. For more information, see Importing custom installation scripts.

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `RHEL` for the operating system.
5. Click **Browse** to find and select the software file to import (for example, `RHEL_installSoftware_customUnattend.cfg`).
6. Click **Import** to upload the file to the OS-images repository.

Step 3. Create a custom OS-image profile that includes the custom software and post-installation script. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom RHEL with software using custom unattend`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Only unattend files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, click **Next**.

7. On the **Unattend Files** tab, select custom unattend file (for example, `RHEL_installSoftware_customUnattend.cfg`), and click **Next**.
8. On the **Installation Scripts** tab, click **Next**.
9. On the **Summary** tab, review the settings.
10. Click **Customize** to create the custom OS-image profile.

Step 4. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip:

      - VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
      - The network settings that you specify on the Network Settings dialog are added to the unattend file at runtime using the **#predefined.hostPlatforms.networkSettings.<*setting*>#** macros.

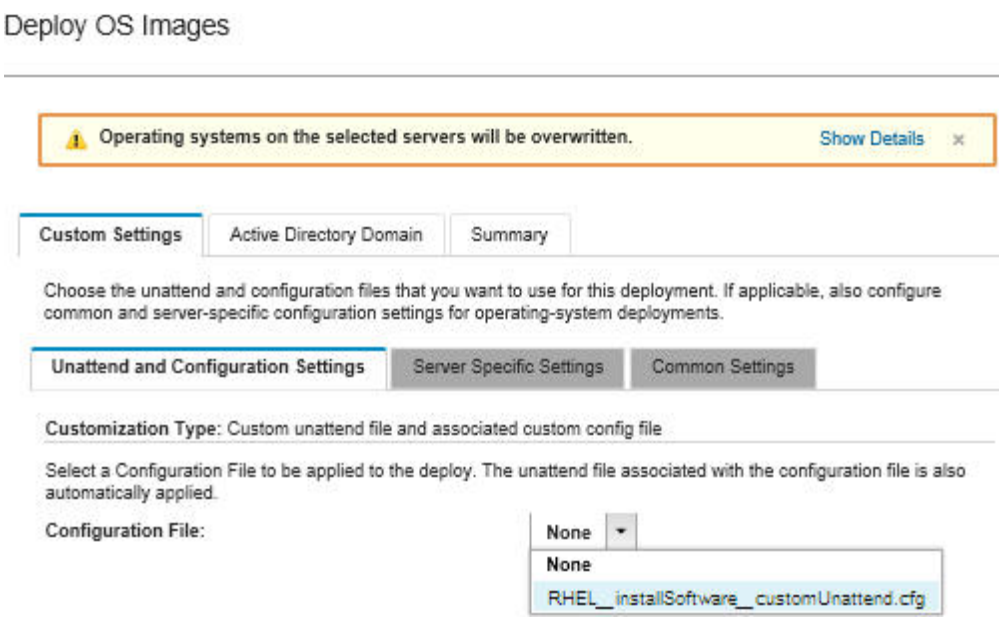
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom RHEL with software using custom unattend`) from the drop-down list in the **Image to Deploy** column

      Note: Ensure that all target servers use the same custom profile.

   d. (Optional) Click the **License Key** icon () and specify the license key to use to activate the operating system after it is installed.
   e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

   f. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon () to initiate the operating-system deployment.
4. On the Custom Settings tab, click the **Unattend and Configuration Settings** subtab, and select the custom unattend file (for example, `RHEL_installSoftware_customUnattend.cfg`).



5. On the **Summary** tab, review the settings.
6. Click **Deploy** to deploy the operating system.

Deploying RHEL and a Hello World PHP application using custom software and a post-installation script

This scenario installs the RHEL operating system along with custom software (Apache HTTP, PHP, and a hello-world PHP application). A custom OS-image profile is used that includes the custom software and a post-installation script that registers the operating system with the internal Lenovo RHEL subscription service so that it can use the yum repositories, installs the Apache and PHP packages, configures the firewall to allow Apache connections, creates a Hello World PHP application and copies to the Apache web server directory, and configures the Apache configuration files to support PHP. The custom software packages are exported to the host during the deployment and made available for the custom post-installation script to use.

Before you begin

You can deploy RHEL and a Hello World PHP application in a few different ways. This example uses a post-installation script that installs custom software that you import into the repository and include in the custom OS-image profile. You can also use a custom attend file that you include in the custom OS-image profile. For installing software using a custom attend file, see Deploying RHEL and a Hello World PHP application using a custom unattend file.

This scenario uses the following sample files.

- httpd.conf. This is the installation file for Apache HTTP.
- hello_world.php This is the Hello World PHP application.
- RHEL_installSoftware_customScript.sh This post-installation script installs and configures the custom software.

Notes:

- RHEL installation scripts can be in one of the following formats: Bash (.sh), Perl (.pm or .pl), Python (.py)
- Software files and installation scripts are installed from the custom data and files path that you specify during deployment. The default custom data and files path is `/home/lxca`.

Procedure

To deploy RHEL with custom software using a post-installation script, complete the following steps.

Step 1. Download the base RHEL operating system from the Red Hat website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the RHEL image to import (for example, `RHEL-<ver>–<date>-Server-x86_64-dvd1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the custom software to the local system and import the files into the OS-images repository. For more information, see Importing custom software.

Tip: To import custom software into XClarity Administrator, the files must be contained in a tar.gz file. For this example, compress the example software files `httpd.conf` and `index.php` into a tar.gz file named `RHEL_installSoftware_customsw.tar.gz` before continuing

1. Click the **Software** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `RHEL` for the operating system.
5. Click **Browse** to find and select the software file to import (for example, `RHEL_installSoftware_customsw.tar.gz`).
6. Click **Import** to upload the file to the OS-images repository.

Step 3. Create a custom post-installation script, and import the file to the OS-images repository.

Add commands to register the host with the RHEL satellite, for example:

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

Add a command to update the host and install and configure apache and php packages, for example:

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

Add commands to add our PHP application to the web serversatellite, for example:

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/lxca/index.php /var/www/html/index.php
```

Add commands to configure Apache HTTP, for example:

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf /etc/httpd/conf/httpd.conf
```

Note that these commands use predefined macros for the path to the extracted data and software files (**predefined.otherSettings.deployDataAndSoftwareLocation**).

You can also add commands to send custom messages to the jobs log in XClarity Administrator. For more information, see Adding custom status reporting to installation scripts.

To import the custom installation script, complete these steps. For more information, see Importing custom installation scripts.

1. Click the **Installation Scripts** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `RHEL` for the operating system.
5. Click **Browse** to find and select the post-installation script to import (for example, `RHEL_installSoftware_customScript.sh`).
6. Click **Import** to upload the file to the OS-images repository.

Step 4. Create a custom OS-image profile that includes the custom software and post-installation script. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon () to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom RHEL with software using post-installation script`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **None** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, select the software installation files (for example `httpd.conf` and `index.php`), and click **Next**.
7. On the **Installation Scripts** tab, select the installation scripts (for example, `RHEL_installSoftware_customScript.sh`), and click **Next**.
8. On the **Summary** tab, review the settings.
9. Click **Customize** to create the custom OS-image profile.

Step 5. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.

c. Select the custom OS-image profile (for example, *<base_OS>*|*<timestamp>*_Custom RHEL with software using post-installation script) from the drop-down list in the **Image to Deploy** column

Note: Ensure that all target servers use the same custom profile.

d. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

e. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Summary** tab, review the settings.
5. Click **Deploy** to deploy the operating system.

Deploying SLES 12 SP3 with custom packages and time zone

This scenario installs the SLES 12 SP3 operating system (in English) and several optional SLES packages. It also prompts for the time zone. A custom OS-image profile is used that includes a custom configuration file and custom unattend file. This custom profile can be selected on the Deploy OS Images page. Then, the SLE packages that you want to deploy can be selected and time zone can be specified on the **Custom Settings** tab. The selected values are substituted for the custom macros in the custom unattend, and the SLES autoyast installer uses those values in the unattend file to configure the operating system.

Before you begin

This scenario uses the following sample files.

- SLES_installPackages_customConfig.json. This configuration file prompts for the time zone and optional SLES packages (Linux, Apache, MySQL, PHP software package, SLES mail server package, and SLES file server package) to install.
- SLES_installPackages_customUnattend.xml This unattend file uses values in predefined macros and custom macros that are defined in the configuration file.

Procedure

To deploy SLES 12 SP3 to servers using a custom OS-image profile, complete the following steps.

Step 1. Download the base SLES operating system from the SUSE website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the SLES 12 SP3 image to import (for example, SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Create a custom configuration-settings file, and import the file to the OS-images repository.

The configuration-settings file is a JSON file that describe the data that needs to be gathered dynamically during the OS deployment process. For this scenario, we want to specify the optional SLES packages that can be installed (including SLES Linux, Apache, MySQL, PHP software package, SLES mail-server package, and SLES file-server package) and a time zone to use for each OS deployment. For more information about creating a configuration-settings file, see Custom macros.

To import the configuration-settings file, complete these steps. For more information, see Importing custom configuration settings.

1. Click the **Configuration Files** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the configuration-settings file to import (for example, `SLES_installPackages_customConfig.json`).
6. Click **Import** to upload the file to the OS-images repository.

   Note: When you import a custom configuration-settings file, XClarity Administrator generates custom macros for each setting in the file. You can add those macros to the unattend file. During OS deployment, the macros are replaced with actual values.

Step 3. Modify the SLES unattend file to specify dynamic values for the optional SLES packages and time zone, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

In the **<general>** section, add the time zone information, for example:

```
<timezone>
   <hwclock></hwclock>
   <timezone></timezone>
</timezone>
```

In the **<patterns>** section, add three pattern tags. These tags are used for the custom macros for the optional SLES package settings, for example:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern></pattern>
   <pattern></pattern>
   <pattern></pattern>
</patterns>
```

Notes:

- These tags are in the sample unattend file.
- When you use a custom unattend file, XClarity Administrator does not provide many of the normal convenience features that you get when you use a predefined unattend file. For example, the targets **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>**, and **<UserAccounts>** for Administrator, **<Interfaces>** for networking, and **<package>** list for installation features must be specified in the custom unattend file that is being uploaded.

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `SLES_installPackages_customUnattend.xml`).
6. Click **Import** to upload the file to the OS-images repository.

   Note: A warning that there are missing predefined macros in the unattend file is displayed. You can ignore the warning for now. You will add the predefined macros in the next step
7. Click **Close** in the warning dialog to open the Edit Unattend File dialog.

Step 4. Associate the custom unattend file with the custom configuration-settings file, and add the required predefined and custom macros (settings) from the configuration-settings file to the unattend file. For more information, see Associating an unattend file with a configuration settings file and Injecting predefined and custom macros to an unattend file.

Tip: You can optionally associate the custom unattend file with the custom configuration-settings file and add macros when importing the unattend file.

1. From the Edit Unattend File dialog, select the configuration-settings file to associate with the unattend file from the **Associate a Configuration File** drop-down list (for example, `SLES_installPackages_customConfig`).
2. Add the required predefined macros to the unattend file.
   a. Select **Predefined** from the **Available Macros** drop-down list.
   b. Place the cursor in the unattend file anywhere after line 1 (after the **<xml>** tag).
   c. Expand the **predefined → unattendSettings** list in the list of available predefined macros.
   d. Click the **preinstallConfig** and **postinstallConfig** macros to add the macros to the unattend file.

   For example:

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

3. Add the custom macro for specifying the time zone.
   a. Select **Custom** from the **Available Macros** drop-down list.
   b. Place the cursor after the **<hwclock>** tag, and click **timezone** to add the time zone macro.
   c. Place the cursor after the **<timezone>** tag, and click **timezone** to add the time zone macro.

   For example:

```
<timezone>
```

```
    <hwclock>#timezone#</hwclock>
    <timezone>#timezone#</timezone>
</timezone>
```

4. Add the custom macro for specifying the optional SLES packages.
   a. Expand the **server-settings → node** list in the list of available custom macros.
   b. Place the cursor in one of the empty **<pattern>** tags, and click **fileserver**.
   c. Place the cursor in one of the empty **<pattern>** tags, and click **lampserver**.
   d. Place the cursor in one of the empty **<pattern>** tags, and click **mailserver**.

   For example:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern>#server-settings.node.fileserver#</pattern>
   <pattern>#server-settings.node.lampserver#</pattern>
   <pattern>#server-settings.node.mailserver#</pattern>
</patterns>
```

5. Click **Save** to bind the files together and save the changes to the unattend file.

Step 5. Create a custom OS-image profile that includes the custom configuration-settings and unattend files. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom SLES with optional packages`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Associated unattend and configuration-settings files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, click **Next**.
7. On the **Unattend Files** tab, select the unattend file (for example, `SLES_installPackages_customUnattend.xml`), and click **Next**.

   The associated configuration-settings file is automatically selected.
8. On the **Installation Scripts** tab, click **Next**.
9. On the **Summary** tab, review the settings.
10. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

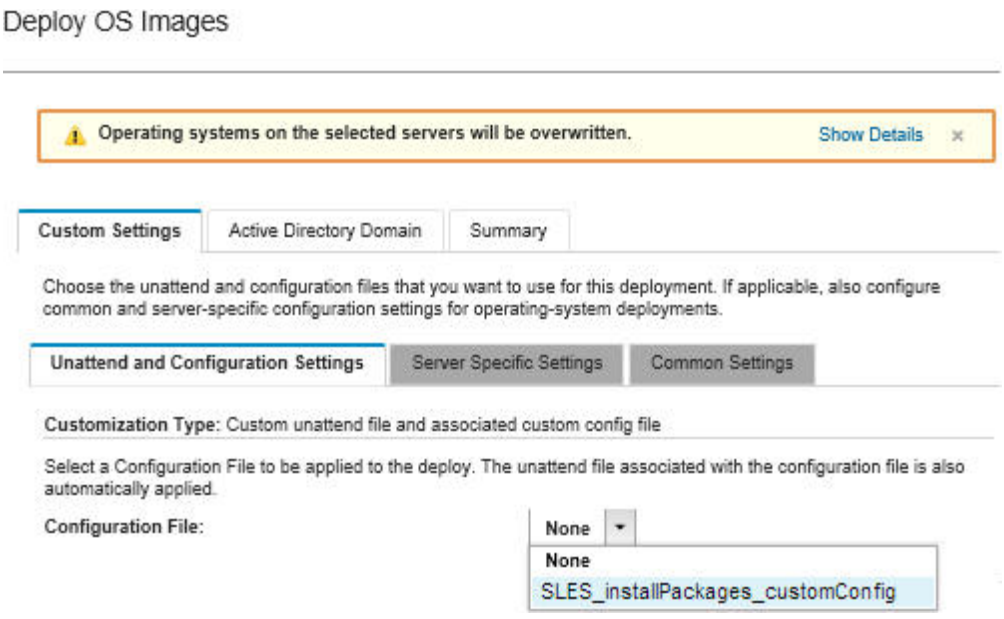
1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom SLES with optional packages`) from the drop-down list in the **Image to Deploy** column

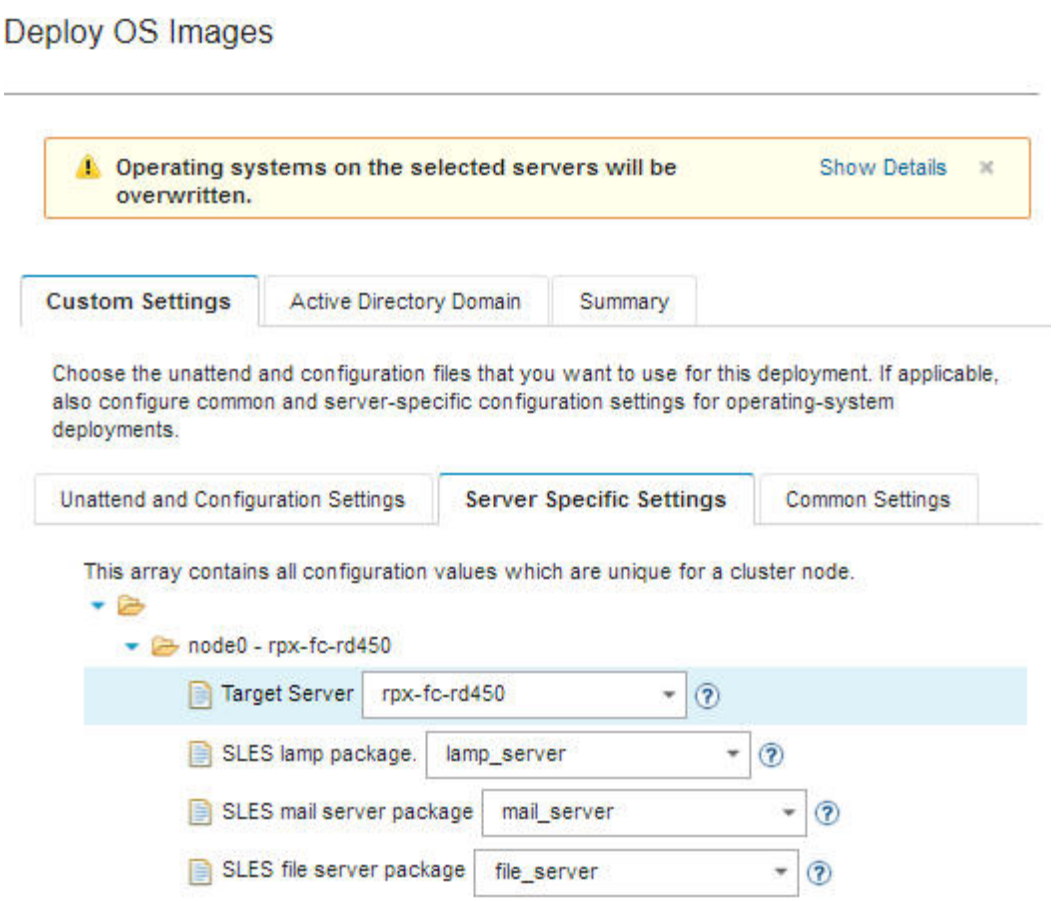
      Note: Ensure that all target servers use the same custom profile.
   d. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
   e. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom configuration-settings file (for example, `SLES_installPackages_customConfig`).

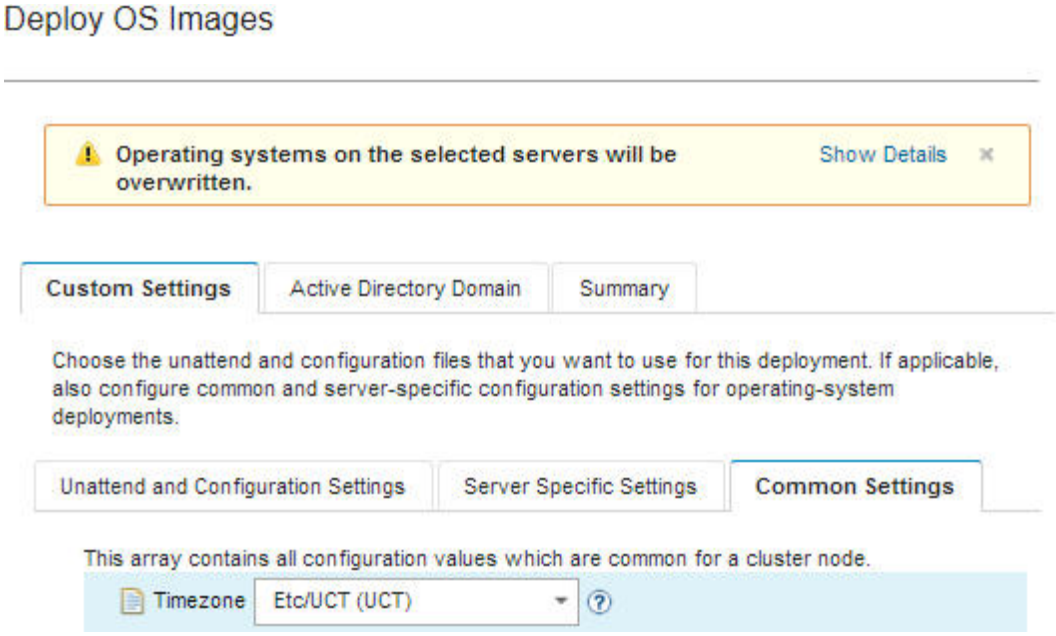
   Note: The associated custom unattend file is selected automatically.



5. On the **Server-Specific Settings** subtab, select the target server and the optional SLES packages that you want to deploy.



6. On the **Common Settings** subtab, select the time zone to set for all target servers.



7. On the **Summary** tab, review the settings.
8. Click **Deploy** to deploy the operating system.

Deploying SLES 12 SP3 with custom software

This scenario installs the SLES 12 SP3 operating system along with custom software (Java and Eclipse IDE). A custom profile is used that includes the custom software and post-installation scripts to install and configure the custom software. The custom software packages are copied to the host during the deployment and made available for the custom post-install script to use.

Before you begin

This scenario uses the following sample files.

- jre-8u151-linux-x64.tar.gz. This is the installation file for Java for Eclipse.
- eclipse-4.6.3-3.1.x86_64.tar.gz This is the installation file for Eclipse IDE.
- SLES_installSoftware_customScript.sh This post-installation script creates a user to launch Eclipse, and installs Eclipse IDE and Java.

Notes:

- SLES installation scripts can be in one of the following formats: Bash (.sh), Perl (.pm or .pl), Python (.py)
- Software files and installation scripts are installed from the custom data and files path that you specify during deployment. The default custom data and files path is `/home/lxca`.
- For SLES 12 SP3, the Eclipse IDE requires the GCC compiler, which is included in the predefined Basic profile. This scenario creates a custom OS-image profile using the predefined Basic profile as the base. If you choose to use another profile, you must ensure that the profile includes the GCC compiler.

Procedure

To deploy SLES 12 SP3 with custom software, complete the following steps.

Step 1. Download the base SLES 12 SP3 operating system from the SUSE website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the SLES 12 SP3 image to import (for example, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the custom software to the local system and import the files into the OS-images repository. For more information, see Importing custom software.

1. Click the **Software** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the software file to import (for example, `jre-8u151-linux-x64.tar.gz`).
6. Click **Import** to upload the file to the OS-images repository.

7. Click the **Import** icon () again.
8. Click **Local Import**.
9. Select `SLES` for the operating system.
10. Click **Browse** to find and select the software- file to import (for example, `eclipse-4.6.3-3.1.x86_64.tar.gz`).
11. Click **Import** to upload the file to the OS-images repository.

Step 3. Create a custom post-installation script, and import the file to the OS-images repository.

Add commands to create a user to launch eclipse to this file, for example:

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "Passw0rd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] && echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Add commands to install the software, for example:

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

Note that these commands use predefined macros for the HTTPS URL that XClarity Administrator uses for reporting status (**predefined.otherSettings.statusSettings.urlStatus**), for the Folder containing the certificates that are needed to access the urlStatus web service from the host OS on first boot (**predefined.otherSettings.statusSettings.certLocation**), and for the path to the extracted data and software files (**predefined.otherSettings.deployDataAndSoftwareLocation**).

You can also add commands to send custom messages to the jobs log in XClarity Administrator, as shown in the sample file. For more information, see Adding custom status reporting to installation scripts.

To import the custom installation script, complete these steps. For more information, see Importing custom installation scripts.

1. Click the **Installation Scripts** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the post-installation script to import (for example, `SLES_installSoftware_customScript.sh`).
6. Click **Import** to upload the file to the OS-images repository.

Step 4. Create a custom OS-image profile that includes the custom software and post-installation script. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.

2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon () to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom SLES with software`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **None** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, select the software installation files (for example `jre-8u151-linux-x64.tar.gz` and `eclipse-4.6.3-3.1.x86_64.tar.gz`), and click **Next**.
7. On the **Installation Scripts** tab, select the installation scripts (for example, `SLES_installSoftware_customScript.sh`), and click **Next**.
8. On the **Summary** tab, review the settings.
9. Click **Customize** to create the custom OS-image profile.

Step 5. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom SLES with software`) from the drop-down list in the **Image to Deploy** column

      Note: Ensure that all target servers use the same custom profile.
   d. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
   e. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon () to initiate the operating-system deployment.
4. On the **Summary** tab, review the settings.
5. Click **Deploy** to deploy the operating system.

Deploying SLES 12 SP3 with a configurable locale and NTP servers

This scenario installs the SLES 12 SP3 operating system with either English, Brazilian, or Japanese enabled for the keyboard and operating-system locales. It also configures the IP address for up to three NTP servers. A custom OS-image profile is used that includes an unattend file (with predefined and custom macros) and a configuration-settings file for selecting the locales and NTP-server settings. This custom profile can be selected on the Deploy OS Images page. Then, the locales and NTP-server settings can be selected on the **Custom Settings** tab. The specified values are substituted for the custom macros contain in the custom

unattend file, and the SLES autoyast installer uses those values in the unattend file to configure the operating system.

Before you begin

This scenario uses the following sample files.

- SLES_locale_customConfig.json. This custom configuration file prompts for the language to install for the OS local and keyboard for SLES and for the NTP server.
- SLES_locale_customUnattend.xml. This custom unattend file uses values in custom macros that are defined in the configuration file.

Procedure

To deploy SLES 12 SP3 using custom OS-image profile, complete the following steps.

Step 1. Download the base SLES operating system from the SUSE website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the SLES 12 SP3 image to import (for example, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete.

Step 2. Create a custom configuration-settings file, and import the file to the OS-images repository.

The configuration-settings file is a JSON file that describe the data that needs to be gathered dynamically during the OS deployment process. For this scenario, we want to specify the operating-system locale (en_US, ja_JP, pt_BR), the keyboard locale (english-us, Japanese, or portugese-br), and up to three NTP server IP addresses to use for each OS deployment. For more information about creating a configuration-settings file, see Custom macros.

To import the configuration-settings file, complete these steps. For more information, see Importing custom configuration settings.

1. Click the **Configuration Files** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the configuration-settings file to import (for example, `SLES_locale_customConfig.json`).
6. Click **Import** to upload the file to the OS-images repository

   Note: When you import a custom configuration-settings file, XClarity Administrator generates custom macros for each setting in the file. You can add those macros to the unattend file. During OS deployment, the macros are replaced with actual values.

Step 3. Modify the SLES unattend file to specify dynamic values for the operating-system locale, keyboard locale, and NTP server IP addresses, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

Just after the <profile> tag, add the NTP server and networking information. The following example includes tags for two NTP servers. The IP addresses will be added as macros in a later step.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

In the <general> section, add the OS and keyboard locale info, as shown in the following example. The keyboard and operating system locale settings will be added as macros in a later step.

```
<keyboard>
   <keymap></keymap>
</keyboard>
<language></language>
```

Note: When you use a custom unattend file, XClarity Administrator does not provide many of the normal convenience features that you get when you use a predefined unattend file. For example, the targets **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>**, and **<UserAccounts>** for Administrator, **<Interfaces>** for networking, and **<package>** list for installation features must be specified in the custom unattend file that is being uploaded.

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `SLES_locale_customUnattend.xml`).
6. Click **Import** to upload the file to the OS-images repository

Step 4. Associate the custom unattend file with the custom configuration-settings file, and add the required predefined and custom macros (settings) from the configuration-settings file to the unattend file. For more information, see Associating an unattend file with a configuration settings file and Injecting predefined and custom macros to an unattend file

Tip: You can optionally the custom unattend file with the custom configuration-settings file and add macros when importing the unattend file.

1. From the **Unattend Files** tab, select the custom attend file (for example, `SLES_locale_customUnattend.xml`).
2. Click the **Associate a Configuration File** icon ( ) to display the Associate an Unattend File dialog.
3. Select the configuration-settings file to associate with the unattend file (for example, `SLES_locale_customConfig`).
4. Add the required predefined macros to the unattend file.
   a. Select **Predefined** from the **Available Macros** drop-down list.
   b. Place the cursor in the unattend file anywhere after line 1 (after the **<xml>** tag).
   c. Expand the **predefined → unattendSettings** list in the list of available predefined macros.
   d. Click the **preinstallConfig** and **postinstallConfig** macros to add the macros.

   For example:

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

5. Add the custom macro for specifying the operating-system locale.
   a. Select **Custom** from the **Available Macros** drop-down list
   b. Place the cursor after the **<language>** tag.
   c. Expand **server-settings → node** in the list of available custom macros, and then click **locale** to add the OS-locale macro.

   For example:

```
<language>#server-settings.node.locale#</language>
```

6. Add the custom macro for specifying the keyboard locale.
   a. Place the cursor after the **<keymap>** tag.
   b. Expand **server-settings → node** in the list of available custom macros, and then click **keyboardLocale** to add the keyboard-locale macro.

   For example:

```
<keyboard>
   <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. Add the custom macro for specifying the NTP server IP addresses.

   In this scenario, the custom configuration-settings file uses a template to specify zero to three NTP servers. When using templates in the configuration-settings file, macros that are associated with template are not displayed in the Associate an Unattend File dialog. Instead, you must manually edit the unattend file and add the macros and appropriate tags.

   For example, to include three NTP servers, you would add the following tags and macros to the unattend file. These tags and macros already exist in the example unattend file for this scenario.

```
<ntp-client>
    <configure_dhcp config:type="boolean">false</configure_dhcp>
    <peers config:type="list">
      <peer>
        <address>#server-settings.ntpserver1#</address>
        <initial_sync config:type="boolean">true</initial_sync>
        <options></options>
```

```
      <type>server</type>
    </peer>
    <peer>
      <address>#server-settings.ntpserver2#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
    <peer>
      <address>#server-settings.ntpserver3#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
  </peers>
  <start_at_boot config:type="boolean">true</start_at_boot>
  <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. Click **Associate** to bind the files together and save the changes to the unattend file.

Step 5. Create a custom OS-image profile that includes the custom configuration-settings and unattend files. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom SLES for OS and keyboard locale and NTP server`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Associated unattend and configuration-settings files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, click **Next**.
7. On the **Unattend Files** tab, select the unattend file (for example, `SLES_locale_customUnattend.xml`), and click **Next**.

   The associated configuration-settings file is automatically selected.
8. On the **Installation Scripts** tab, click **Next**.
9. On the **Summary** tab, review the settings.
10. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target server. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.

c. Select the custom OS-image profile (for example, *<base_OS>*|*<timestamp>*_Custom SLES for OS and keyboard locale and NTP server) from the drop-down list in the **Image to Deploy** column

   Note: Ensure that all target servers use the same custom profile.

d. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

   Note: To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

e. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom configuration-settings file (for example, SLES_locale_customConfig).

   Note: The associated custom unattend file is selected automatically.



5. On the **Server-Specific Settings** subtab, select the target server, OS locale, and keyboard locale.
6. On the **Common Settings** subtab, click **Add** to specify the IP address of up to three NTP servers.
7. On the **Summary** tab, review the settings.
8. Click **Deploy** to deploy the operating system.

Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address

This scenario installs the VMware ESXi v6.7 with Lenovo Customization operating system to the local disk using the static IP address of the host server. A custom OS-image profile is used that includes an unattend file with predefined macros. This custom profile can be selected on the Deploy OS Images page. Known values are substituted for the predefined macros in the custom unattend file, and the VMware ESXi kickstart installer uses those values in the unattend file to configure the operating system.

Before you begin

This scenario uses the following sample files.

- ESXi_staticIP_customUnattend.cfg. This custom unattend file uses values in predefined macros.

Procedure

To deploy VMware ESXi v6.7 using custom OS-image profile, complete the following steps.

Step 1. Download the VMware vSphere® Hypervisor (ESXi) with Lenovo Customization operating system from the VMware Support – Downloads webpage website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the ESXi image to import (for example, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete.

Step 2. Modify the ESXi unattend (kickstart) file to add the required predefined macros and other predefined macros where applicable, such as the IP address, gateway, DNS and host name settings, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

For ESXi and RHEL only, XClarity Administrator provides the **#predefined.unattendSettings.networkConfig#** macro, which adds all network settings that are defined in the UI to the unattend file. Because this example specifies a setting (**--addvmportgroup**) that is not defined in the UI, the . **#predefinedunattendSettings.storageConfig#** macro is not used in the sample unattend file. Instead, network settings are individually added to the file, and the **#predefined.hostPlatforms.networkSettings.**<*setting*>**#** macros are used.

For ESXi and RHEL only, XClarity Administrator also provides the **#predefined.unattendSettings.storageConfig#** macro, which adds all storage settings that are defined in the UI to the unattend file. Because this example specifies settings (**--novmfsondisk** and **–ignoressd**) that are not defined in the UI, the **#predefinedunattendSettings.storageConfig#** macro is not used in the sample unattend file. Instead, storage settings are individually added and **--firstdisk=local** is hardcoded in the file.

Note: XClarity Administrator provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file. The example file already contains the required macros. Note that because the %firstboot section is included, the ordering of these predefined macros matters. For more information, see Importing custom unattend files.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

The example file already contains the required macros and additional predefined macros for dynamically specifying network settings for the target server. For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file.

For more information about available predefined macros, see Predefined macros.

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `ESXi` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `ESXi_staticIP_customUnattend.cfg`).
6. Click **Import** to upload the file to the OS-images repository

Step 3. Create a custom OS-image profile that includes the custom unattend. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Virtualization`).
3. Click **Create** icon () to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom ESXi using static IP`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Only unattend files** for the customization type.
   d. Click **Next**.
5. On the **Unattend Files** tab, select the unattend file (for example, `ESXi_staticIP_customUnattend.cfg`), and click **Next**.
6. On the **Summary** tab, review the settings.
7. Click **Customize** to create the custom OS-image profile.

Step 4. Deploy the custom OS-image profile to the target server. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip:

      - VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
      - The network settings that you specify on the Network Settings dialog are added to the unattend file at runtime using the **#predefined.hostPlatforms.networkSettings.** <*setting*>**#** macros.

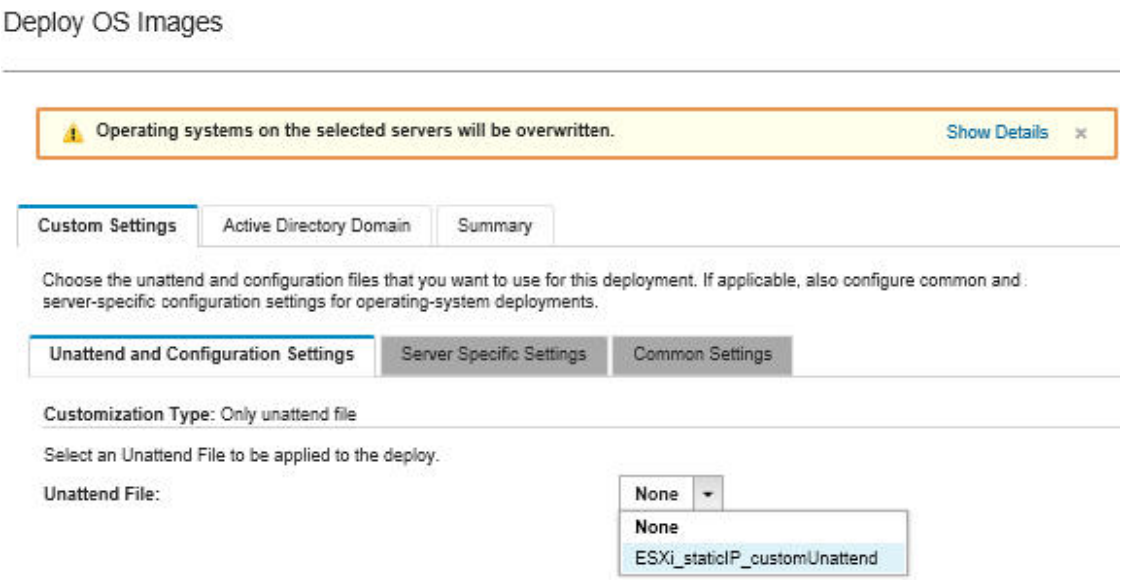
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom ESXi using static IP`) from the drop-down list in the **Image to Deploy** column

      Note: Ensure that all target servers use the same custom profile.

   d. (Optional) Click the **License Key** icon () and specify the license key to use to activate the operating system after it is installed.
   e. Verify that the deployment status for the selected server is **Ready**.

Note: Because **--firstdisk=local** is specified in the unattend file, you do not need to specify the preferred storage location in the **Storage** column. The setting in the UI is ignored.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom unattend file (for example, `ESXi_staticIP_customUnattend.cfg`).



5. On the **Summary** tab, review the settings.
6. Click **Deploy** to deploy the operating system.

Deploying VMware ESXi v6.7 with Lenovo Customization with a configurable locale and second-user credentials

This scenario installs the VMware ESXi v6.7 with Lenovo Customization operating system with a configurable language enabled for the keyboard locale and credentials for a second ESXi user. This example also uses basic network and storage settings that are defined in the UI. A custom OS-image profile is used that includes an unattend file (with predefined and custom macros) and a configuration-settings file for selecting the password. This custom profile can be selected on the Deploy OS Images page. Then, the password can be specified on the **Custom Settings** tab. The specified value is substituted for the custom macro in the custom unattend file, and the ESXi installer uses those values in the unattend file to configure the operating system.

Before you begin

This scenario uses the following sample files.

- ESXi_locale_customConfig.json. This custom configuration file prompts for the keyboard locale and credentials for the second ESXi user.
- ESXi_locale_customUnattend.cfg. This custom unattend file uses values in predefined macros and custom macros that are defined in the configuration file.

Procedure

To deploy VMware ESXi v6.7 using custom OS-image profile, complete the following steps.

Step 1. Download the VMware vSphere® Hypervisor (ESXi) with Lenovo Customization operating system from the VMware Support – Downloads webpage website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the ESXi image to import (for example, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete.

Step 2. Create a custom configuration-settings file, and import the file to the OS-images repository.

The configuration-settings file is a JSON file that describe the data that needs to be gathered dynamically during the OS deployment process. For this scenario, we want to choose keyboard locale and the user ID and password for a second ESXi user to use for each OS deployment. For more information about creating a configuration-settings file, see Custom macros.

To import the configuration-settings file, complete these steps. For more information, see Importing custom configuration settings.

1. Click the **Configuration Files** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `ESXi` for the operating system.
5. Click **Browse** to find and select the configuration-settings file to import (for example, `ESXi_locale_customConfig.json`).
6. Click **Import** to upload the file to the OS-images repository

   Note: When you import a custom configuration-settings file, XClarity Administrator generates custom macros for each setting in the file. You can add those macros to the unattend file. During OS deployment, the macros are replaced with actual values.

Step 3. Modify the ESXi unattend (kickstart) file to specify the operating-system locale and keyboard locale and user credentials for the second ESXi user, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

Add commands to set the keyboard locale, for example:

```
# Set the keyboard locale
keyboard ''
```

Add commands to create a second ESXi user. In the following example, *<user_id>* and *<password>* will be replaced with custom macros in the next step.

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.

2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `ESXi` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `ESXi_locale_customUnattend.cfg`).
6. Click **Import** to upload the file to the OS-images repository

Step 4. Associate the custom unattend file with the custom configuration-settings file, and add the required predefined and custom macros (settings) from the configuration-settings file to the unattend file. For more information, see Associating an unattend file with a configuration settings file and Injecting predefined and custom macros to an unattend file

Tip:

- You can optionally associate the custom unattend file with the custom configuration-settings file and add macros when importing the unattend file.
- XClarity Administrator provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file. The example file already contains the required macros. Note that because the %firstboot section is included, the ordering of these predefined macros matters. For more information, see Importing custom unattend files.
  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```
- XClarity Administrator also provides macros that inject all network and storage-location settings that are defined in the UI. These macros are useful when only basic settings are needed for the deployment. The example file already contains the required macros.
  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file. For more information about available predefined macros, see Predefined macros.

To associate the custom unattend file with the custom configuration-settings file, complete these steps.

1. From the **Unattend Files** tab, select the custom attend file (for example, `ESXi_locale_customUnattend.cfg`).
2. Click the **Associate a Configuration File** icon () to display the Associate an Unattend File dialog.
3. Select the configuration-settings file to associate with the unattend file (for example, `ESXi_locale_customConfig`).
4. Select **Custom** from the **Available Macros** drop-down list.
5. Add the custom macro for specifying the keyboard locale by placing the cursor between the single quotes after keyboard, and then clicking **keyboard_locale**.

   For example:

   ```
   # Set the keyboard locale
   keyboard '#keyboard_locale#'
   ```
6. Add the custom macro for specifying the second user's ID by placing the cursor at each location where you want to add the user ID, and then clicking **second_user_id**. In the example file, replace each occurrence of *<user_id>* with the custom macro.

For example:

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
```

7. Add the custom macro for specifying the second user's password by placing the cursor at the location where you want to add the password, and then clicking **second_user_password**. In the example file, replace <*password*> with the custom macro.

   For example:

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
```

8. Click **Associate** to bind the files together and save the changes to the unattend file.

Step 5. Create a custom OS-image profile that includes the custom configuration-settings and unattend files. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom ESXi using custom locale and second user credentials`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Associated unattend and configuration-settings files** for the customization type.
   d. Click **Next**.
5. On the **Unattend Files** tab, select the unattend file (for example, `ESXi_locale_customUnattend.cfg`), and click **Next**.

   The associated configuration-settings file is automatically selected.
6. On the **Summary** tab, review the settings.
7. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target server. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip:

      - VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
      - The network settings that you specify on the Network Settings dialog are added to the unattend file at runtime using the **#predefined.hostPlatforms.networkConfig#** macro.

   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom ESXi using custom locale and second user credentials`) from the drop-down list in the **Image to Deploy** column

Note: Ensure that all target servers use the same custom profile.

d. (Optional) Click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.

e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

Notes:

- To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
- The storage settings that you specify on the Storage Settings dialog are added to the unattend file at runtime using the **#predefined.hostPlatforms.storageConfig#** macro.

f. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom configuration-settings file (for example, `ESXi_locale_customConfig`).

Note: The associated custom unattend file is selected automatically.



5. On the **Server-Specific Settings** subtab, select the keyboard locale and credentials for the second ESXi user.
6. On the **Summary** tab, review the settings.
7. Click **Deploy** to deploy the operating system.

Deploying Windows 2016 with custom features

This scenario installs the Windows 2016 operating system and several additional features. A custom profile is used that includes a custom unattend file. The custom profile can then be selected on the Deploy OS Images page.

Before you begin

This scenario uses the following sample files.

- Windows_installFeatures_customUnattend.xml. This custom unattend file installs the WindowsMediaPlayer and BitLocker features, and uses predefined macros for dynamic values.

Procedure

To deploy Windows 2016 with custom features, complete the following steps.

Step 1. Download the Japanese Windows 2016 operating system to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the bundle file for Windows 2016 to the local system, and import the image to the OS-images repository. For more information, see Importing device drivers.

The bundle file contains the latest device drivers and WinPE boot files that you can add to your custom OS-images profiles. This scenario uses a custom boot file, so the boot file in the bundle will not be used.

1. Click the **Driver Files** tab.
2. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the bundle file for Windows 2016 to the local system.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `bundle_win2016_20180126130051.zip`).
6. Click **Import** to upload the file to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 3. Modify the Windows unattend file to install the additional features (such as WindowsMediaPlayer and BitLocker), and import the custom file to the OS-images repository.

In the “servicing” section of the Windows unattend file, add the Windows features to install, for example

```
<servicing>
   <package action="configure">
      <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
                        processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
                        language=""></assemblyIdentity>
      <selection name="Microsoft-Hyper-V" state="true"></selection>
      <selection name="MultipathIo" state="true"></selection>
      <selection name="FailoverCluster-PowerShell" state="true"></selection>
      <selection name="FailoverCluster-FullServer" state="true"></selection>
      <selection name="FailoverCluster-CmdInterface" state="true"></selection>
      <selection name="FailoverCluster-AutomationServer" state="true"></selection>
```

```
      <selection name="FailoverCluster-AdminPak" state="true"></selection>
      <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
      <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
      <selection name="ServerManager-Core-RSAT" state="true"></selection>
      <selection name="WindowsMediaPlayer" state="true"></selection>
      <selection name="BitLocker" state="true"></selection>
   </package>
</servicing>
```

Notes:

- These tags are in the sample unattend file.
- When you use a custom unattend file, XClarity Administrator does not provide many of the normal convenience features that you get when you use a predefined unattend file. For example, the targets `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>`, and `<UserAccounts>` for Administrator, `<Interfaces>` for networking, and `<package>` list for installation features must be specified in the custom unattend file that is being uploaded.

To import the custom unattend file, complete these steps. For more information, see Importing custom unattend files.

1. Click the **Unattend Files** tab.
2. Click **Import** icon ( ).
3. Click **Local Import**.
4. Select `Windows` for the operating system.
5. Click **Browse** to find and select the custom unattend file (for example, `Windows_installFeatures_customUnattend.xml`).
6. Click **Import** to upload the file to the OS-images repository.

XClarity Administrator provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, and custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

The example file already contains the code for installing the additional features, required macros, and other macros that are needed for dynamic input. For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file.

For more information about available predefined macros, see Predefined macros.

Step 4. Create a custom OS-image profile that includes the unattend file. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select the profile to customize (for example, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom Windows with features`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Only unattend files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.

6. On the **Boot Options** tab, and click **Next**. The predefined WinPE boot file is selected by default.
7. On the **Software** tab, click **Next**.
8. On the **Unattend Files** tab, select custom unattend file (for example, `Windows_installFeatures_customUnattend.xml`), and click **Next**.
9. On the **Installation Scripts** tab, click **Next**.
10. On the **Summary** tab, review the settings.
11. Click **Customize** to create the custom OS-image profile

Step 5. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, subnet mask, gateway, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom Windows with features`) from the drop-down list in the **Image to Deploy** column.

      Note: Ensure that all target servers use the same custom profile.
   d. (Optional) Click the **License Key** icon () and specify the license key to use to activate the operating system after it is installed.
   e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment
   f. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon () to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom unattend file (for example, `Windows_installFeatures_customUnattend.xml`).
5. (Optional) On the **Active Directory Domain** tab, specify information to join an Active Directory domain as part of a Windows image deployment (see Integrating with Windows Active Directory).
6. On the **Summary** tab, review the settings.
7. Click **Deploy** to deploy the operating system.

Deploying Windows 2016 with custom software

This scenario installs the Windows 2016 operating system along with custom software (Java and Eclipse IDE). A custom profile is used that includes the custom software and post-installation scripts to install and configure the custom software. The custom software packages are copied to the host during the deployment and made available for the custom post-install script to use.

Before you begin

This scenario uses the following sample files.

- jre-8u151-windows-x64-with-configfile.zip. This is the installation file for Java for Eclipse.
- eclipse-java-oxygen-1a-win32-x86_64.zip This is the installation file for Eclipse IDE.
- Windows_installSoftware_customScript.ps1 This post-installation script creates a user to launch Eclipse, and installs Eclipse IDE and Java.

Notes:

- Windows installation scripts can be in one of the following formats: Command file (.cmd), PowerShell (.ps1)
- Software files and installation scripts are installed from the custom data and files path that you specify during deployment. The default custom data and files path is `C:\lxca`.

Procedure

To deploy Windows 2016 with custom software, complete the following steps.

Step 1. Download the Japanese Windows 2016 operating system to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the bundle file for Windows 2016 to the local system, and import the image to the OS-images repository. For more information, see Importing device drivers.

The bundle file contains the latest device drivers and WinPE boot files that you can add to your custom OS-images profiles. This scenario uses a custom boot file, so the boot file in the bundle will not be used.

1. Click the **Driver Files** tab.
2. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the bundle file for Windows 2016 to the local system.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `bundle_win2016_20180126130051.zip`).
6. Click **Import** to upload the file to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 3. Download the custom software to the local system and import the files into the OS-images repository. For more information, see Importing custom software.

1. Click the **Software** tab.

2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `Windows` for the operating system.
5. Click **Browse** to find and select the configuration-settings file to import (for example, `jre-8u151-windows-x64-with-configfile.zip`).
6. Click **Import** to upload the file to the OS-images repository.
7. Click the **Import** icon () again.
8. Click **Local Import**.
9. Select `Windows` for the operating system.
10. Click **Browse** to find and select the configuration-settings file to import (for example, `eclipse-java-oxygen-1a-win32-x86_64.zip`).
11. Click **Import** to upload the file to the OS-images repository.

Step 4. Create a custom post-installation script, and import the file to the OS-images repository.

Add commands to install the software, for example:

```
Write-Output "Install Java...."
Invoke-Command -ScriptBlock
        {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
        [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
        /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
        "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
        -DestinationPath $eclipseDir
```

Note that these command use the predefined macro for the path to the extracted data and software files (**predefined.otherSettings.deployDataAndSoftwareLocation**).

You can also add commands to send custom messages to the jobs log in XClarity Administrator, as shown in the sample file. For more information, see Adding custom status reporting to installation scripts.

To import the custom installation script, complete these steps. For more information, see Importing custom installation scripts

1. Click the **Installation Scripts** tab.
2. Click the **Import** icon ().
3. Click **Local Import**.
4. Select `Windows` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `Windows_installSoftware_customScript.ps1`).
6. Click **Import** to upload the file to the OS-images repository.

Step 5. Create a custom OS-image profile that includes the custom unattend file. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Datacenter virtualization`).

3. Click **Create** icon () to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom Windows with software`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **None** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Boot Options** tab, and click **Next**. The predefined WinPE boot file is selected by default.
7. On the **Software** tab, select the software installation files (for example `jre-8u151-windows-x64-with-configfile.zip` and `eclipse-java-oxygen-1a-win32-x86_64.zip`), and click **Next**.
8. On the **Installation Scripts** tab, select the installation scripts (for example, `Windows_installSoftware_customScript.ps1`), and click **Next**.
9. On the **Summary** tab, review the settings.
10. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom Windows with software`) from the drop-down list in the **Image to Deploy** column

      Note: Ensure that all target servers use the same custom profile.
   d. (Optional) Click the **License Key** icon () and specify the license key to use to activate the operating system after it is installed.
   e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
   f. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon () to initiate the operating-system deployment.
4. On the **Summary** tab, review the settings.
5. Click **Deploy** to deploy the operating system.

Deploying Windows 2016 for Japanese

This scenario installs the Windows 2016 operating system to multiple servers with Japanese enabled for the keyboard and operating-system locales. A custom profile is used that includes a custom WinPE boot file and unattend file. The custom profile can then be selected on the Deploy OS Images page.

Before you begin

This scenario uses the following sample files.

- `WinPE_64_ja.zip`. This custom Windows boot (WinPE) file installs the Japanese locale.
- Windows_locale_customUnattend.xml. This custom unattend file uses the WinPE file to install Japanese.

Notes: The sample custom unattend file assumes the following:

- The server only has one visible disk (disk 0) and does not already have a system partition on it.
- Static IPv4 mode is used and sets a static IP (which gets used in the custom unattend as a predefined macro).

Procedure

To deploy Japanese Windows 2016 to target servers using a custom OS-image profile, complete the following steps.

Step 1. Download the Japanese Windows 2016 operating system to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the bundle file for Windows 2016 to the local system, and import the image to the OS-images repository. For more information, see Importing device drivers.

The bundle file contains the latest device drivers and WinPE boot files that you can add to your custom OS-images profiles. This scenario uses a custom boot file, so the boot file in the bundle will not be used.

1. Click the **Driver Files** tab.
2. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the bundle file for Windows 2016 to the local system.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `bundle_win2016_20180126130051.zip`).
6. Click **Import** to upload the file to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 3. Optional: Create a custom WinPE boot file that uses the Japanese locale during the WinPE install, and import the file to the OS-images repository.

XClarity Administrator uses a predefined Windows PreInstallation (WinPE) boot file to install the Windows operating system. The locale that is used with this predefined boot file is English (en-US). If you want to change the locale that is used during Windows Setup, you can create a custom WinPE boot file with the desired locale and assign that custom boot file to your custom profile.

For information about injecting locales into WinPE, see the Windows WinPE: Add packages webpage.

Important: Specifying a non-English locale in the WinPE boot file does not change the locale of the final OS being deployed. It only changes the locale that is shown during Windows install and setup.

To create a custom WinPE boot file that includes the Japanese locale, complete these steps. For more information, see Creating a boot (WinPE) file.

1. Using a user ID with administrator authority, run the Windows ADK command "Deployment and Imaging Tools Environment." A command session is displayed.
2. From the command session, change to the directory where the **genimage.cmd** and **starnet.cmd** files were downloaded (for example, `C:\customwim`).
3. Ensure that no previously mounted images are on the host by running the following command:
   `dism /get-mountedwiminfo`

   If there are mounted images, discard them by running the following command:

   `dism /unmount-wim /MountDir:C:\<mount_path> /Discard`
4. If you are adding in-box device drivers to a customized Windows profile, copy the raw device-driver files, in .inf format, to the host system in the `C:\drivers` directory.
5. Run the following command to generate the boot file, in .wim format, and then wait a few minutes for the command to complete.
   `genimage.cmd amd64 <ADK_Version>`

   Where *<ADK_Version>* is one of the following values.

   - **8.1**. For Windows 2012 R2
   - **10**. For Windows 2016

   This command creates a boot file named `C:\WinPE_64\media\Boot\WinPE_64.wim`.
6. Mount the boot file by running the following command:
   `DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount`
7. If you are adding out-of-box device drivers directly to the boot file, complete the following steps.
   a. Create the following directory structure, where *<os_release>* is `2012R2`, or `2016`
      `drivers\<os_release>\`
   b. Copy the device drivers, in .inf format, to a directory inside that path, for example:
      `drivers\<os_release>\<driver1>\<driver1_files>`
   c. Copy the `drivers` directory to the mount directory, for example:
      `C:\WinPE_64\mount\drivers`
8. **Optional:** Make additional customizations to the boot file, such as adding folders, files, startup scripts, language packs, and apps. For more information about customizing boot files, see the WinPE: Mount and Customize website.
9. Add the Japanese packages, for example.

10. View installed packages to ensure that the Japanese-specific packages are installed.
    ```
    Dism /Add-Package /Image:"C:\WinPE_64\mount"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
    and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
    ```
11. Review the International Settings in the image.
    ```
    Dism /Get-Packages /Image:"C:\WinPE_64\mount"
    ```
12. Unmount the image by running the following command.
    ```
    DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
    ```
13. Compress the contents of the `C:\WinPE_64\media` directory into a zip file called `WinPE_64_ja.zip`.
14. Import the .zip file into XClarity Administrator (see Importing boot files).
    a. Click the **Boot Files** tab.
    b. Click **Import** icon ().
    c. Click **Local Import**.
    d. Select `Windows` for the operating system.
    e. Click **Browse** to find and select the custom boot file (for example, `WinPE_64_ja.zip`).
    f. Click **Import** to upload the file to the OS-images repository.

Step 4. Modify the Windows unattend file to specify that Japanese is included in the OS image, and import the custom file to the OS-images repository.

In the “windowsPE” pass of the Windows install, add the Japanese as the operating-system language and the locale, for example:

```
<settings pass="windowsPE">
   <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
              publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
              xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
         <UILanguage>ja-JP</UILanguage>
      </SetupUILanguage>
      <SystemLocale>ja-JP</SystemLocale>
      <UILanguage>ja-JP</UILanguage>
      <UserLocale>ja-JP</UserLocale>
      <InputLocale>0411:00000411</InputLocale>
   </component>
</settings>
```

Note: When you use a custom unattend file, XClarity Administrator does not provide many of the normal convenience features that you get when you use a predefined unattend file. For example, the targets `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>`, and `<UserAccounts>` for Administrator, `<Interfaces>` for networking, and `<package>` list for installation features must be specified in the custom unattend file that is being uploaded.

XClarity Administrator provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

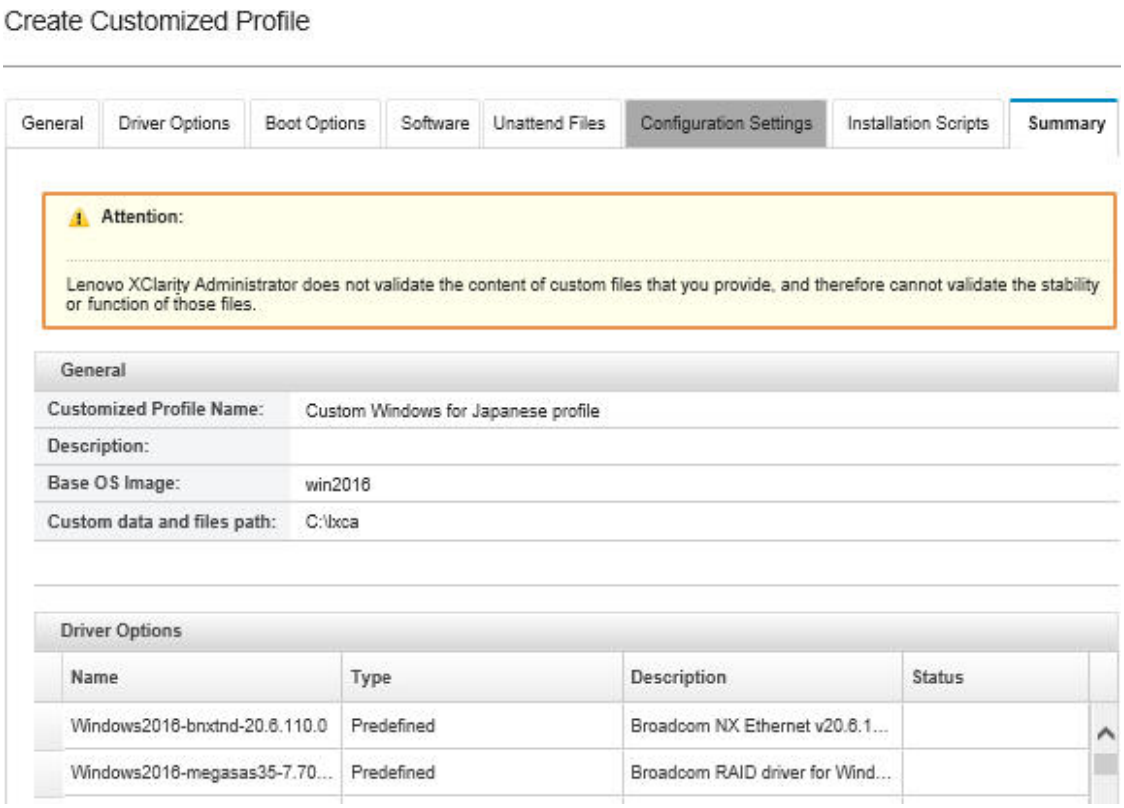
The example file already contains the required macros. For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file. For more information about available predefined macros, see Predefined macros.

To import the custom unattend file, complete these steps. For more information, see Importing custom unattend files.

1. Click the **Unattend Files** tab.
2. Click **Import** icon ( ).
3. Click **Local Import**.
4. Select `Windows` for the operating system.
5. Click **Browse** to find and select the custom unattend file (for example, `Windows_locale_customUnattend.xml`).
6. Click **Import** to upload the file to the OS-images repository.

Step 5. Create a custom OS-image profile that includes the custom boot (WinPE) file and unattend file. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select the profile to customize (for example, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom Windows for Japanese profile`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Only unattend files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Boot Files** tab, select custom boot file (for example, `WinPE_64_ja`), and click **Next**.
7. On the **Software** tab, click **Next**.
8. On the **Unattend Files** tab, select custom unattend file (for example, `Windows_locale_customUnattend.xml`), and click **Next**.
9. On the **Installation Scripts** tab, click **Next**.
10. On the **Summary** tab, review the settings.



11. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

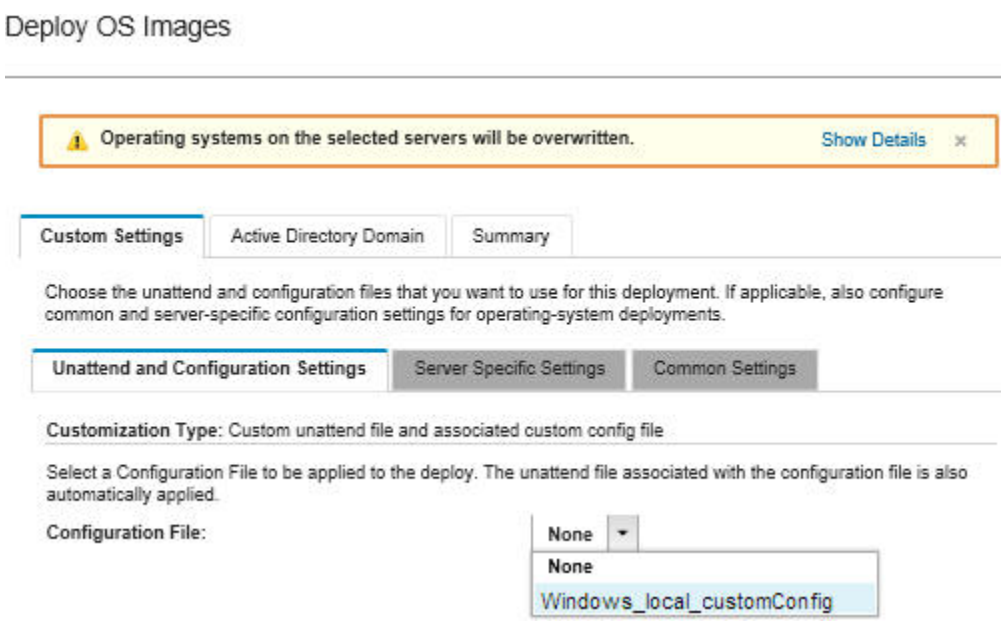
1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, subnet mask, gateway, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom Windows for Japanese profile`) from the drop-down list in the **Image to Deploy** column.

      Note: Ensure that all target servers use the same custom profile.
   d. (Optional) Click the **License Key** icon () and specify the license key to use to activate the operating system after it is installed.
   e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
   f. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom unattend file (for example, `Windows_locale_customUnattend.xml`).



5. (Optional) On the **Active Directory Domain** tab, specify information to join an Active Directory domain as part of a Windows image deployment (see Integrating with Windows Active Directory).
6. On the **Summary** tab, review the settings.
7. Click **Deploy** to deploy the operating system.

   The Windows installation dialog is displayed in Japanese.



   After installation is complete, the Windows login page also displayed in Japanese.


Administrator
パスワード
パスワードのリセット

Chapter 15. End-to-end scenarios for setting up new devices

Use these end-to-end scenarios describe how to help you use Lenovo XClarity Administrator to set up new devices in a way that is consistent and easily repeatable.

Deploying ESXi to a local hard drive

Use these procedures to deploy VMware ESXi 5.5 to a locally installed hard drive on a Flex System x240 Compute Node. It illustrates how to learn a server pattern from an existing server, modify the extended UEFI-settings category pattern for that server pattern, and how to install VMware ESXi.

VMware ESXi 5.5 requires memory-mapped I/O (MMIO) space to be configured within the initial 4 GB of the system. Depending on the configuration, certain systems attempt to use memory higher than 4 GB, which might cause a failure. To resolve the issue, you can increase the value of the MM Config option to 3 GB through the Setup utility for each server on which VMware ESXi 5.5 is going to be installed.

An alternative is to deploy a server pattern that contains one of the predefined extended UEFI category patterns that is related to virtualization, which sets the MM Config option and disables the PCI 64-bit resource allocation.

Deploying a predefined virtualization pattern

A category pattern defines specific firmware settings that can be reused by multiple server patterns. To deploy a predefined virtualization pattern, you create a server pattern and then apply a predefined extended UEFI pattern to that server pattern. That server pattern can then be applied to multiple servers of the same type, such as the Flex System x240 Compute Node or the Flex System x880 X6 Compute Node.

About this task

When creating a server pattern, you can choose to complete the configuration yourself or learn the pattern attributes from an existing server that has already been set up. When you learn a new pattern from an existing server, most of the pattern attributes are already defined.

For more information about server patterns and category patterns, see Working with server patterns.

Procedure

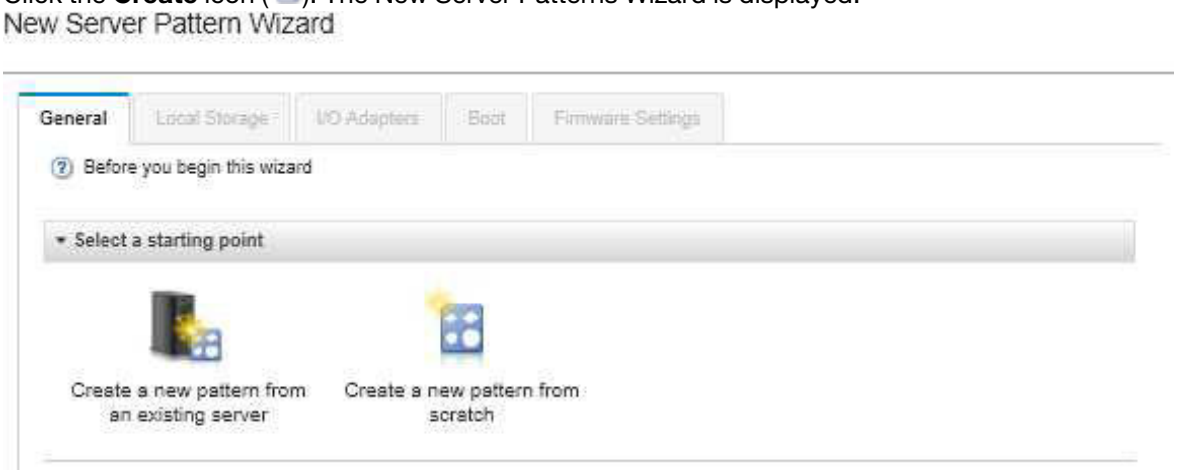
To learn a new pattern from an existing server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

© Copyright Lenovo 2015, 2021

Step 3. Click the **Create** icon ( ). The New Server Patterns Wizard is displayed.



Step 4. Click **Create a new pattern from an existing server**. You can choose to create a pattern from scratch, but it is typically more efficient to create a pattern from an existing server that has the desired configuration.

When you create a server pattern from an existing server, XClarity Administrator learns the settings from a managed server (including the extended port, UEFI, and baseboard management controller settings) and dynamically creates category patterns for those settings. If the server is brand new, XClarity Administrator learns the manufacturing settings. If the server is in use, XClarity Administrator learns the customized settings. You can then modify the settings specifically for the server to which this pattern is to be deployed.

Step 5. Select the server to use as a base configuration when creating the pattern.

Note: Remember that the server that you choose must be the same model as the servers to which you intend to deploy the server pattern. This scenario is based on choosing a Flex System x240 Compute Node.

Step 6. Enter the name of the new pattern, and provide a description.

For example:

- Name: **x240_ESXi_deployment**
- Description: **Pattern with extended UEFI settings that are appropriate for the deployment of VMware ESXi**

Step 7. Click **Next** to load the information from the selected server.

Step 8. On the **Local Storage** tab, select **Specify storage configuration**, and choose one of the storage types. Then click **Next**.

For more information about the local-storage settings, see Defining local storage.

Step 9. On the **I/O adapters** tab, enter information about the adapters that are in the servers on which you intend to install VMware ESXi.

Any adapters that were present in the server used as a base are displayed.

If all Flex System x240 Compute Nodes in your installation have the same adapters, you do not need to modify any settings on this tab.

For more information about the I/O adapters settings, see Defining I/O adapters.

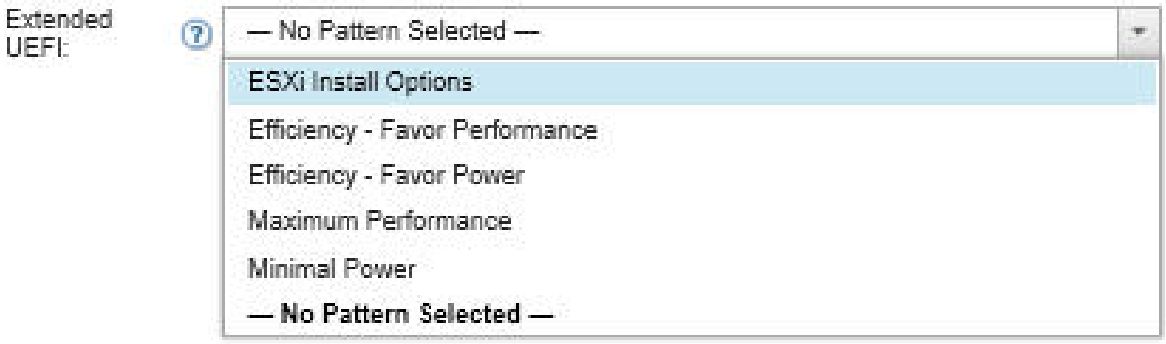
Step 10. Click **Next** to continue.

Step 11. On the **Boot** tab, configure settings for legacy-only boot environment and SAN boot environments. Unless you are using one of these environments, accept the default, which is **UEFI Only Boot**, and click **Next**.

For more information about the boot settings, see Defining boot options.

Step 12. On the **Firmware Settings** tab, specify the management controller and UEFI firmware settings that are to be used for target servers when this pattern is deployed (for example, select **x240 Virtualization**).

On this tab, you can choose one of the predefined extended UEFI patterns:



For more information about the firmware settings, see Defining firmware settings.

Step 13. Click **Save and Deploy** to save the pattern to XClarity Administrator and deploy it to the servers on which you intend to install VMware ESXi.

What to do next

After the server pattern has been deployed to all servers, you can install the operating system on those servers.

Deploying VMware ESXi to a Flex System x240 Compute Node

Use this procedure as an example flow to illustrate the process for deploying the ESXi operating system to a Flex System x240 Compute Node.

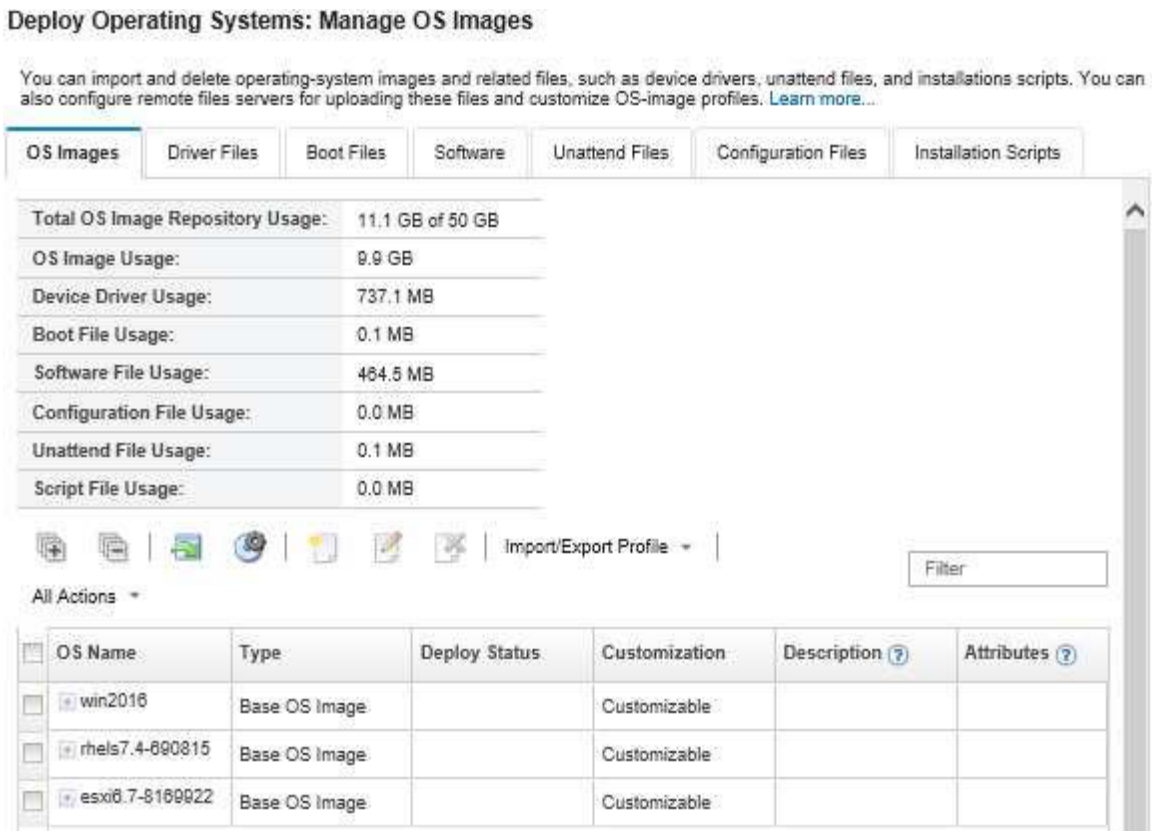
Before you begin

Before you begin this procedure, ensure that Lenovo XClarity Administrator is managing the chassis in which the Flex System x240 Compute Node is installed.

Procedure

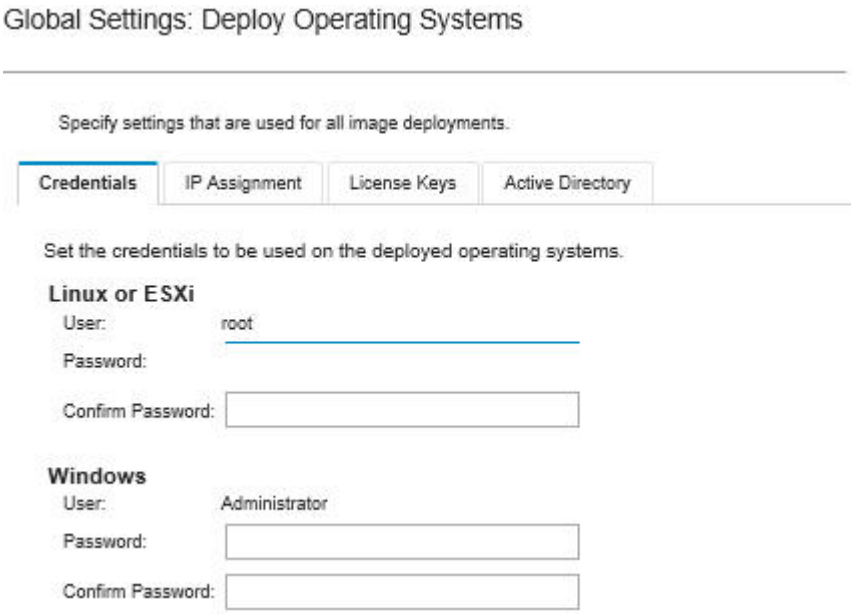
Complete the following steps to deploy the ESXi operating system to an Flex System x240 Compute Node.

Step 1. Ensure that the image to be deployed is already loaded into the OS images repository by click **All actions → Manage OS images** to display a list of all available images.



Step 2. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Deploy OS images**. The Deploy OS Images page is displayed.

Step 3. Set global settings that are to be used as defaults for all image deployments by clicking **All actions → Global Settings** to display the Global Settings dialog.



a. On the **Credentials** tab, enter the password that is to be used by the administrator account to log in to the operating system.

b. On the **IP Assignment** tab, specify how the IP address for the operating system will be assigned to the server.

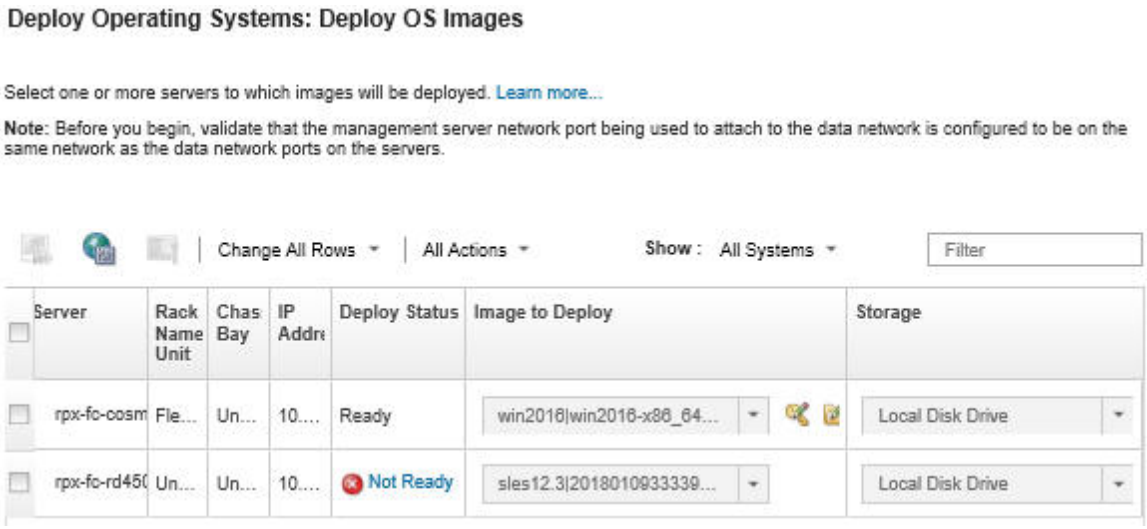
   If you choose **Use Dynamic Host Configuration Protocol (DHCP)** to assign IP addresses, the IP address information is not displayed on the Edit Network Settings dialog (see step Step 8 9 on page 565). If you choose **Assign static IP address (IPv4)**, you can specify an IP address, subnet, and gateway for each deployment.

c. On the **License Keys** tab, enter a mass-activation license key, if desired.

d. Click **OK** to close the dialog.

Step 4. Ensure that the server is ready for operating system deployment. by selecting the server to which the operating system is to be deployed. Initially, the deployment status might be shown as Not Ready. The deployment status must be Ready before you can deploy an operating system to a server.

Tip: You can choose multiple servers in multiple Flex System chassis if you intend to deploy the same operating system to all servers. You can choose up to 28 server.



Step 5. Click in the **Image to Deploy** column, and select VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Step 6. In that same column, click the **License Key** icon ( ) to enter the license key for this deployment.

Tip: You can also choose to use a mass-activation key that you entered in the Global Settings dialog.

Step 7. Ensure that **Local Disk** is selected in the Storage column.

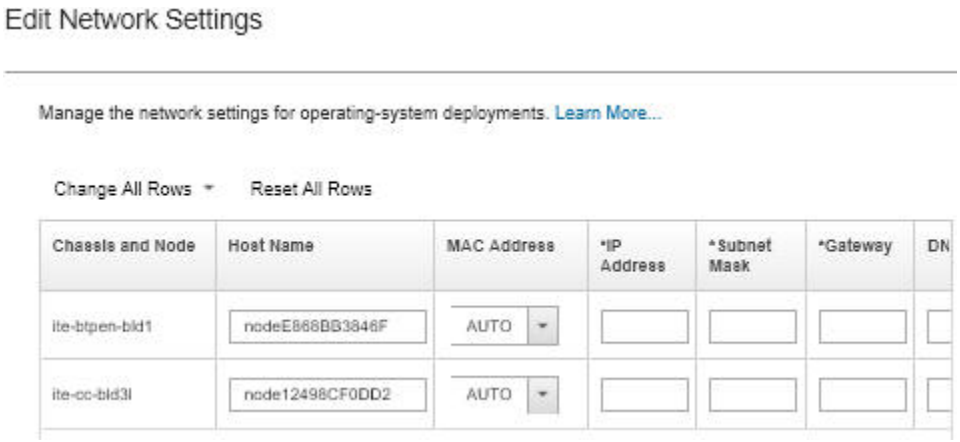
Step 8. Click **Edit** in the **Network Settings** column of the server row to configure the network settings that are to be used for this deployment. The Edit Network Settings page is displayed.

Fill in the following fields:

- Hostname
- MAC address of the port on the host where the operating system is to be installed
- Domain name system (DNS) servers, if required
- maximum transmission unit (MTU) speed

Notes: If you chose **Assign static IP address (IPv4)** from the Global Settings dialog (see step Step 3 4 on page 564), also enter the following information:

- IPv4 address
- Subnet mask
- Gateway



Step 9. Click **OK** to close the dialog.

From the Deploy OS images page, ensure that the server shows a Deploy Status of Ready.

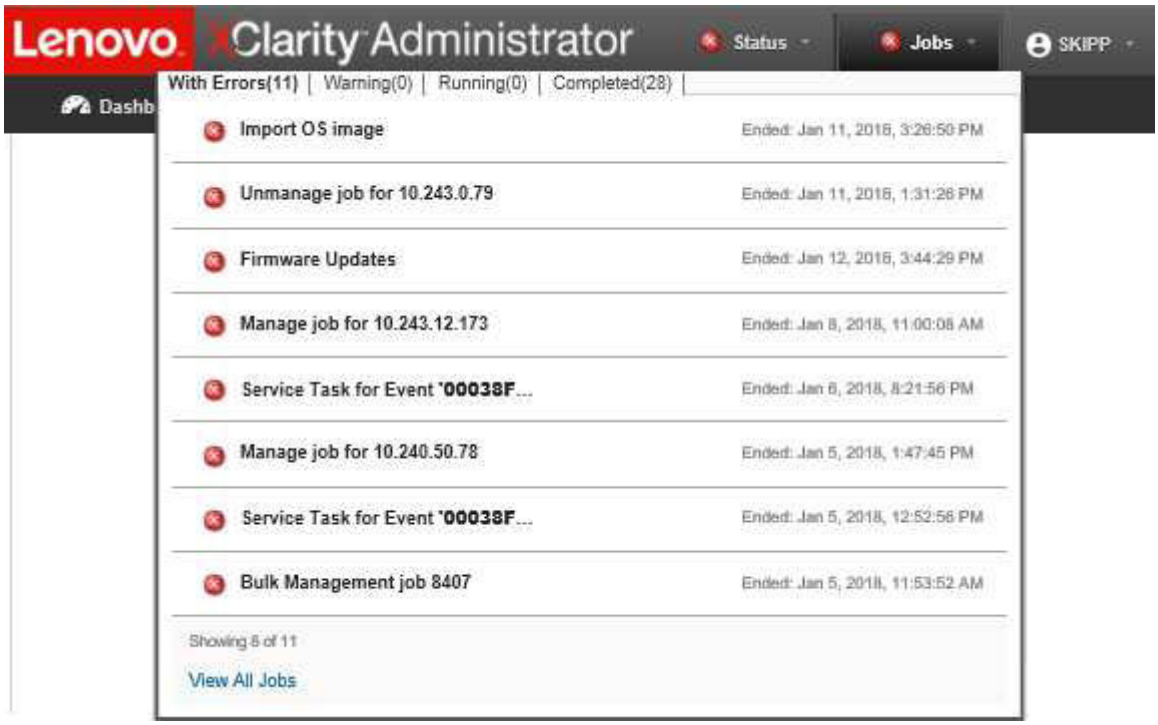
Step 10. Deploy the operating system by clicking **All actions → Deploy images**.

Step 11. From the confirmation page, click **Deploy** to deploy the image.

If the server currently has an operating system installed, you are warned about the fact that deploying the image will overwrite the current operating system.

Tip: You can set up a Remote Control session to watch the installation as it progresses. Click **All actions → Remote Control** to start a Remote Control session with the server.

When you deploy the operating system, Lenovo XClarity Administrator starts a job to track the deployment. To view the status of the deployment job, click **Jobs** from the Lenovo XClarity Administrator menu bar. Then, click the **Running** tab.

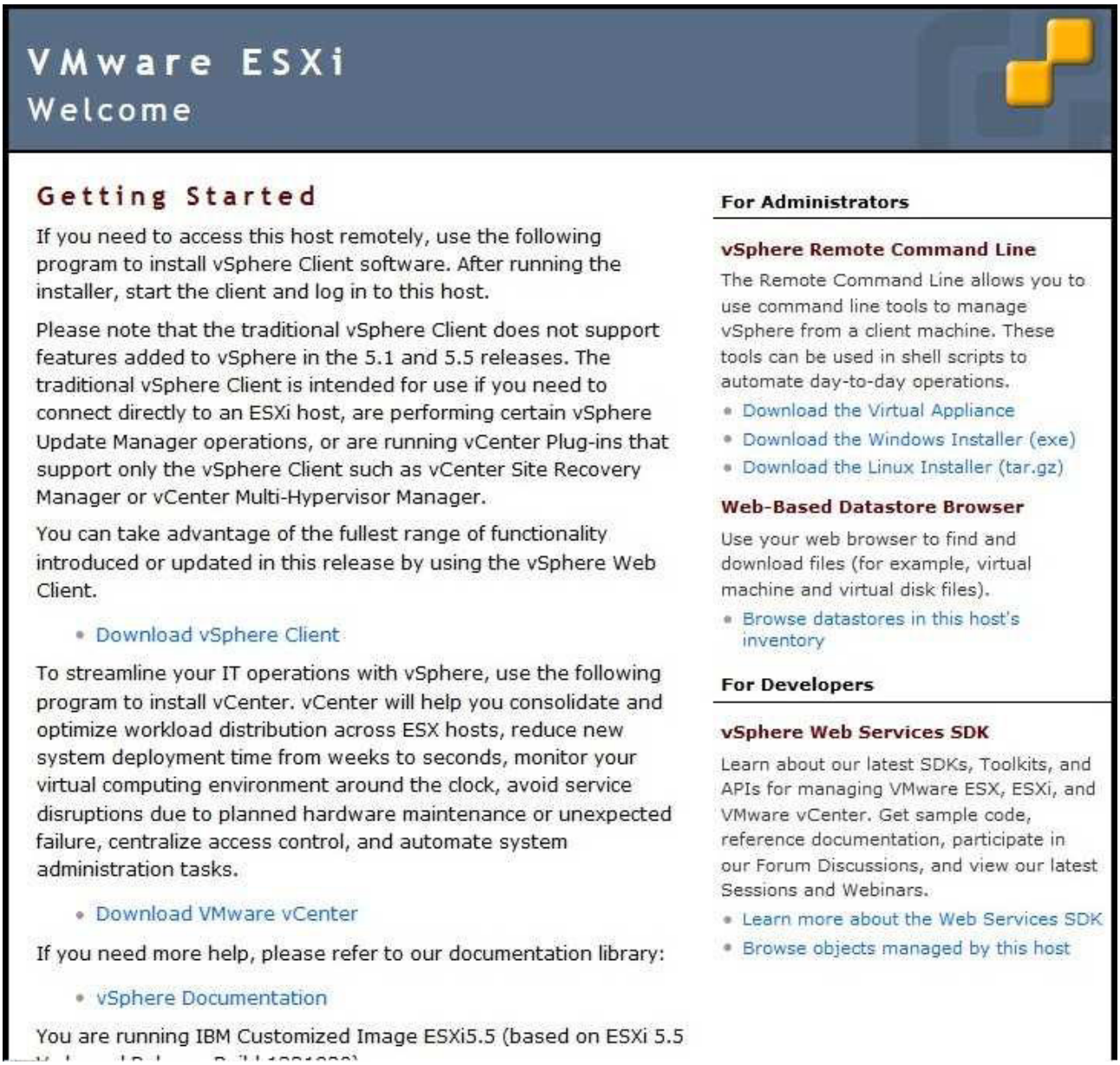


Hover over the running job to see the details, such as the percentage of the job that is complete.

Results

After the operating system deployment has completed, log in to the IP address that you specified on the Edit Network Settings page to continue with the configuration process.

Note: The license provided with the image is a 60-day free trial. You are responsible for meeting all VMware licensing requirements.



Deploying ESXi to SAN storage

Use these procedures to deploy VMware ESXi 5.5 to SAN volumes that are attached to servers.

When you deploy an operating system to a SAN, the operating system is deployed to the first SAN boot target that is configured through a server pattern. In addition, a local hard drive cannot be enabled in the server that will be booting from SAN. It must be disabled or removed if a hard drive is present.

Deploying a server pattern to support SAN boot

When you create and deploy a server pattern to support booting a system from SAN, ensure that you identify the SAN boot target and the adapters that are part of the server.

Procedure

To create and deploy a server pattern that supports the deployment of the operating system on SAN storage, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

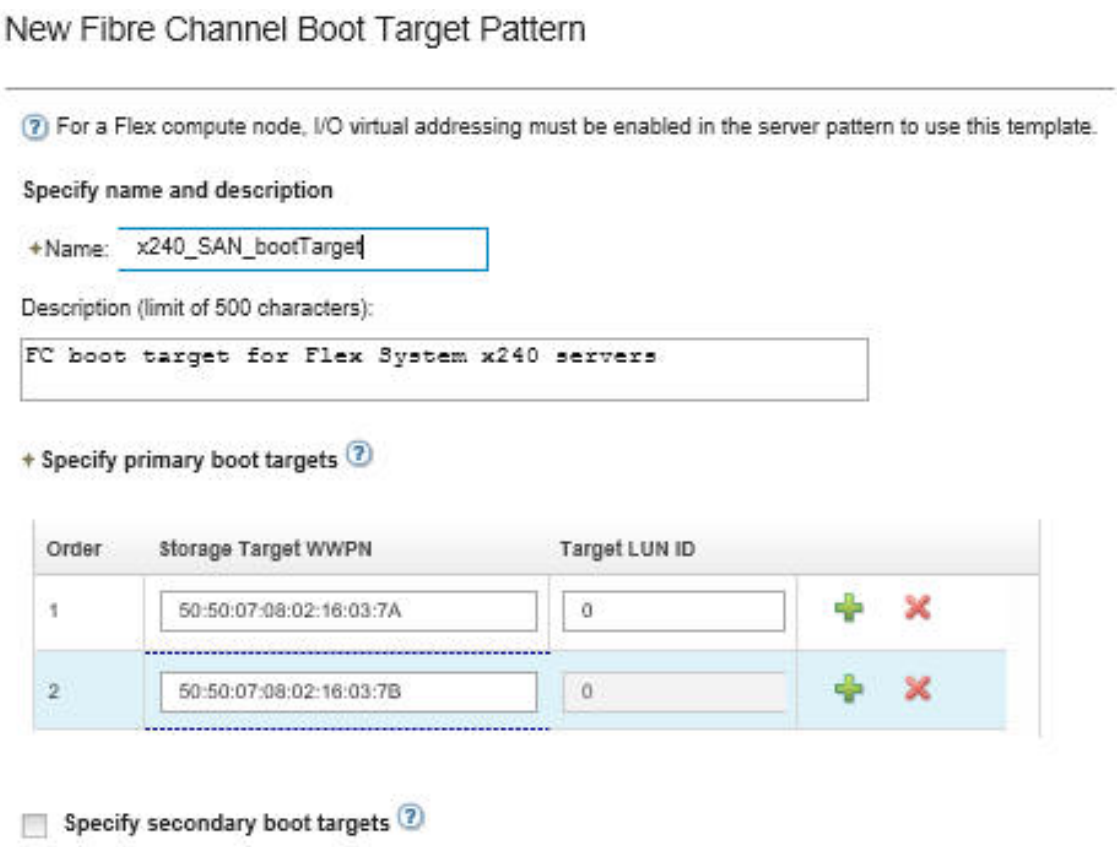
Step 2. To identify the WWPN and LUN IDs of the storage volumes where the operating system is to be deployed, create a category pattern.

a. Click the **Category Patterns** tab.

b. Click **Fibre Channel Boot Target Patterns**, and then click the **Create** icon ( ).

c. Enter the WWPN of the storage target.

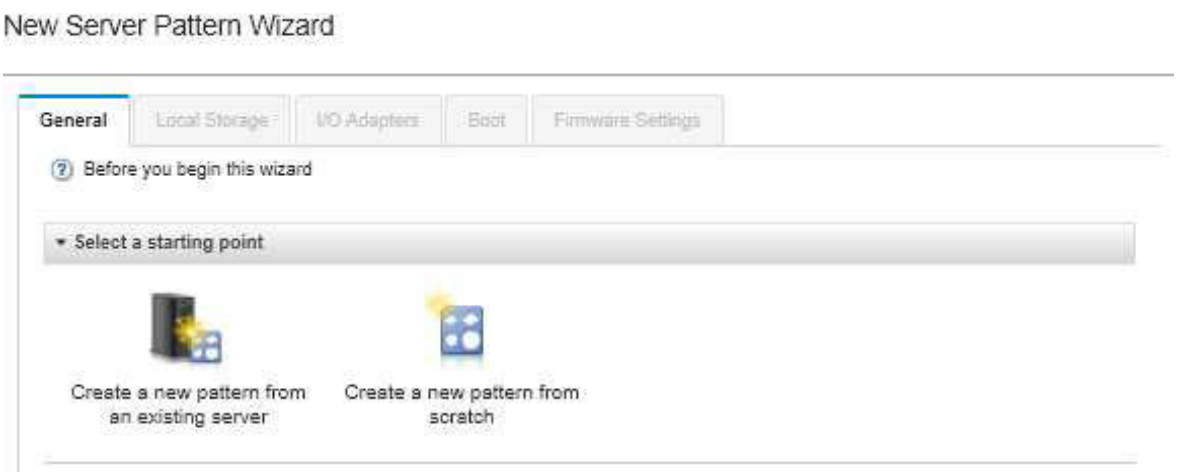
Note: Click **Allow Multiple LUN Identifiers** to assign multiple target LUN identifiers to the same storage volumes.



d. Click **Create** to create the pattern. The target is displayed in the list of Fibre Channel boot target patterns.

Step 3. Click the **Server Patterns** tab to create a pattern.

Step 4. Click the **Create** icon ( ). The New Server Patterns Wizard is displayed.



Step 5. Click **Create a new pattern from scratch**.

Step 6. On the **General** tab:

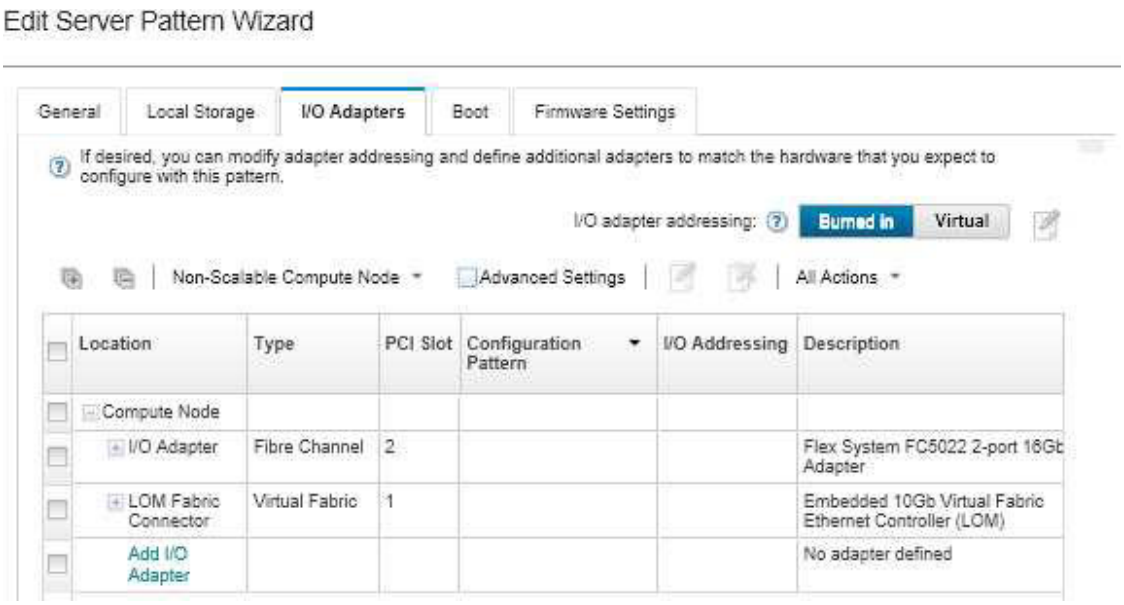
- Select **Flex Compute Node** for the form factor.
- Specify a pattern name (**x240_san_boot**) and description.
- Click **Next**.

Step 7. On the **Local Storage** tab, consider disabling the local storage adapter if you are using a diskless system to improve boot times that are related to scanning for local drives. Then, click **Next**.

Step 8. On the **I/O Adapters** tab, add the Ethernet and Fibre Channel cards. Ensure that they are in the appropriate PCI slots.

a. For each card, click **Add I/O Adapter**, choose the PCI slot where the card is located, and select the card.

Note: Ensure that you specify an Ethernet card and a Fibre Channel card.



b. Ensure that I/O adapter addressing is set to **Virtual**. Then click the **Edit** icon to specify the configuration to be used for Ethernet (MAC) virtual addressing and Fibre Channel (WWN) virtual addressing.

Note: From the Edit Virtual Addressing page, you can choose to use the burned-in MAC address for the Ethernet card by disabling the virtual addressing. However, to select and use a Fibre Channel boot-target pattern, you must use virtual addressing for the Fibre Channel adapter.

c. Click **Next**.

Step 9. On the **Boot** tab, add the SAN boot target pattern that you created earlier.

a. On the **SAN Boot** tab, choose the boot target pattern that you defined.

b. Click **Next**.

Step 10. On the **Firmware Settings** tab, define any additional category patterns that are to be included in this server pattern. You can define the following category patterns.

- **System information** (see Defining system-information settings)
- **Management interface** (see Defining management-interface settings
- **Device and I/O ports** (see Defining devices and I/O ports settings
- **Extended BMC**. You can choose from baseboard management controller settings that have been learned previously (see Defining extended management-controller settings).
- **Extended UEFI**. You can choose from predefined settings or from UEFI settings that have been learned previously (see Defining extended UEFI settings).

Step 11. Click **Save and Deploy** to save the pattern to Lenovo XClarity Administrator, and deploy it to the servers on which you intend to install VMware ESXi.

What to do next

Consider the following steps after the server pattern has been deployed to all servers.

1. Take the virtualized WWPN addresses that were created, and add them to the storage zone so that the server can reach the defined storage LUNs.

   Tip: After you deploy the server profile, you can find the virtualized WWPN addresses by viewing the server profile.

   a. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server profiles**.

   b. Click the deployed server profile (for example, **x240_SAN_boot**). The **Virtual Address Mapping** tab displays the list of addresses.

2. Deploy the operating system to the server.

Deploying VMware ESXi to SAN storage

Use this procedure as an example flow to illustrate the process for deploying the ESXi operating system to SAN storage that is connected to a server.

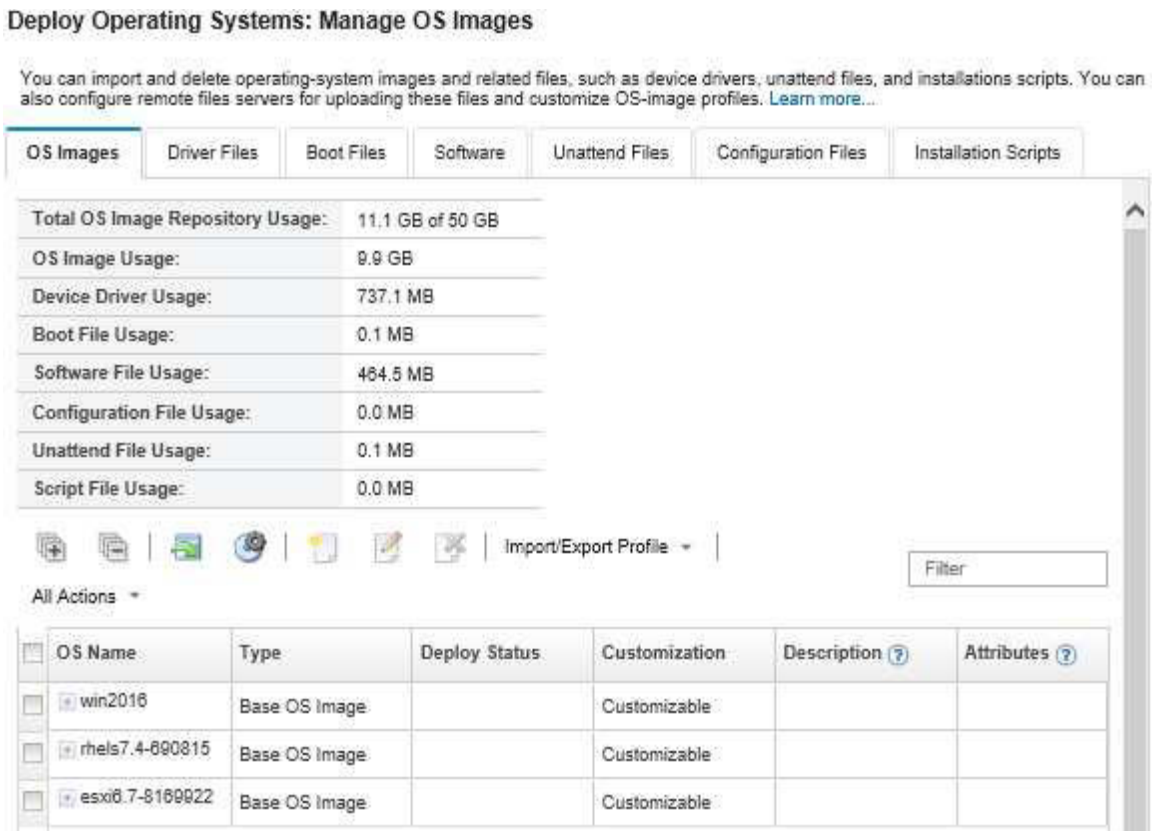
Before you begin

Before you begin this procedure, ensure that Lenovo XClarity Administrator is managing the chassis in which the Flex System x220 Compute Node is installed.

Procedure

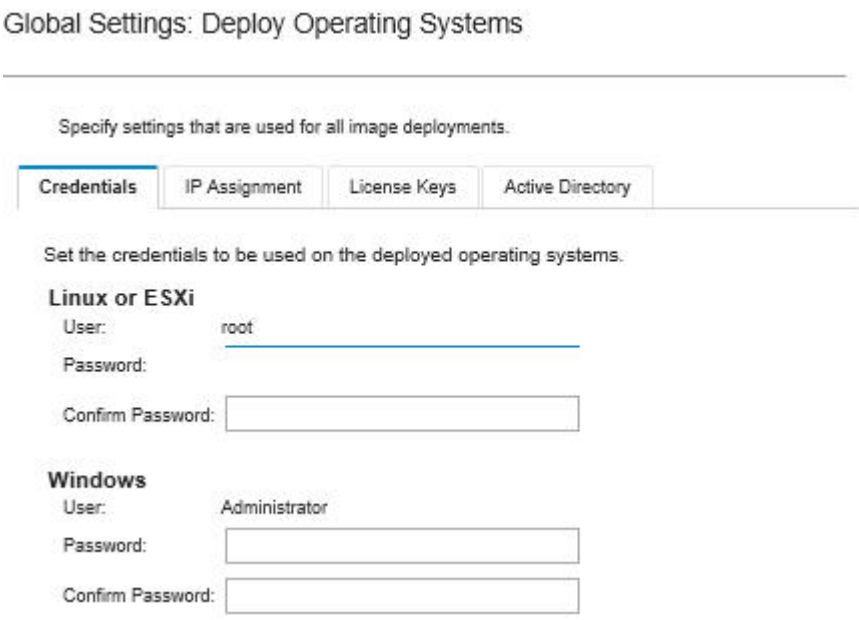
Complete the following steps to deploy the ESXi operating system to an Flex System x222 Compute Node.

Step 1. Ensure that the image to be deployed is already loaded into the OS images repository by clicking **All actions → Manage OS images**.



Step 2. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Deploy OS images**

Step 3. Set global settings that are to be used as a default for all image deployments by clicking **All actions → Global Settings** to display the Global Settings: Deploy Operating Systems dialog.



a. On the **Credentials** tab, enter the password that is to be used by the administrator account to log in to the operating system.

b. On the IP **Assignment** tab, specify how the IP address for the operating system is to be assigned to the server.

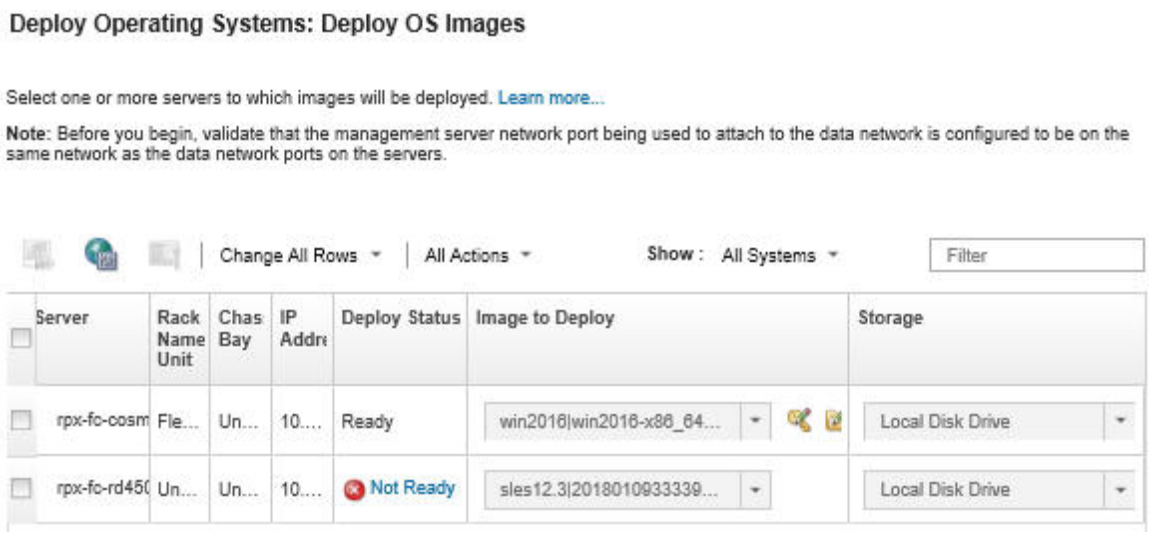
If you choose **Use Dynamic Host Configuration Protocol (DHCP)** to assign IP addresses, the IP address information will not be displayed on the Edit Network Settings dialog (see step Step 8 9 on page 573). If you choose **Assign static IP address (IPv4)**, you can specify an IP address, subnet, and gateway for each deployment.

c. On the **License Keys** tab, enter a mass-activation license key, if desired.

d. Click **OK** to close the dialog.

Step 4. Ensure that the server is ready for operating-system deployment by selecting server to which the operating system is to be deployed. Initially, the deployment status might be shown as Not Ready. The deployment status must be Ready before you can deploy an operating system to a server.

Tip: You can choose multiple servers from multiple Flex System chassis if you intend to deploy the same operating system to all servers. You can choose up to 28 servers.



Step 5. Click in the **Image to Deploy** column, and select VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Step 6. In that same column, click the **License Key** icon ( ) to enter the license key for this deployment.

Tip: You can also choose to use a mass-activation key that you entered in the Global Settings: Deploy Operating Systems dialog.

Step 7. In the **Storage** column, select the SAN storage to which the operating system is to be deployed.

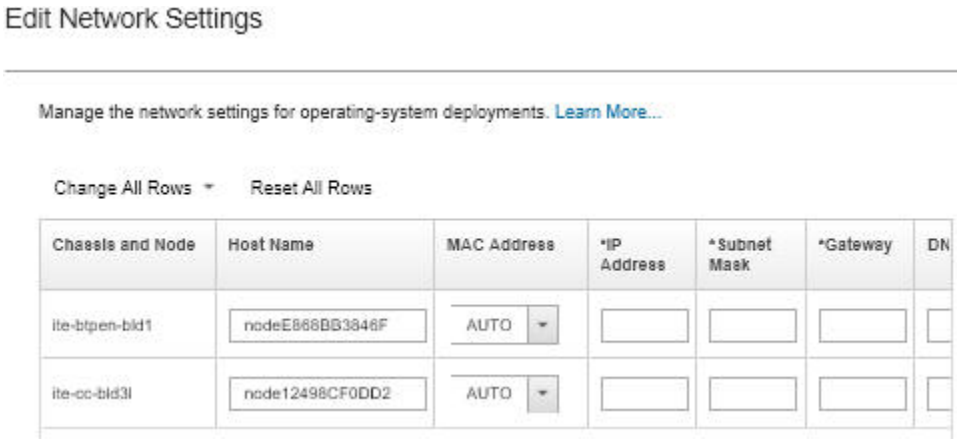
The storage is listed as:
`LUN: <LUN VALUE>  WWPN: <WWPN_VALUE>`

Step 8. Click **Edit** in the **Network Settings** column of the server row to configure the network settings that is to be used for this deployment. The Edit Network Settings page is displayed.

Fill in the following fields:
- Hostname
- MAC address of the port on the host where the operating system will be installed
- Domain name system (DNS) serveres, if required
- Maximum transmission unit (MTU) speed

Notes: If you chose **Assign static IP address (IPv4)** from the Global Settings: Deploy Operating Systems dialog (step Step 3 4 on page 572), also enter the following information:
- IPv4 address
- Subnet mask

- Gateway



Step 9. Click **OK** to close the dialog.

From the Deploy OS images page, the server now shows a deployment status of Ready.

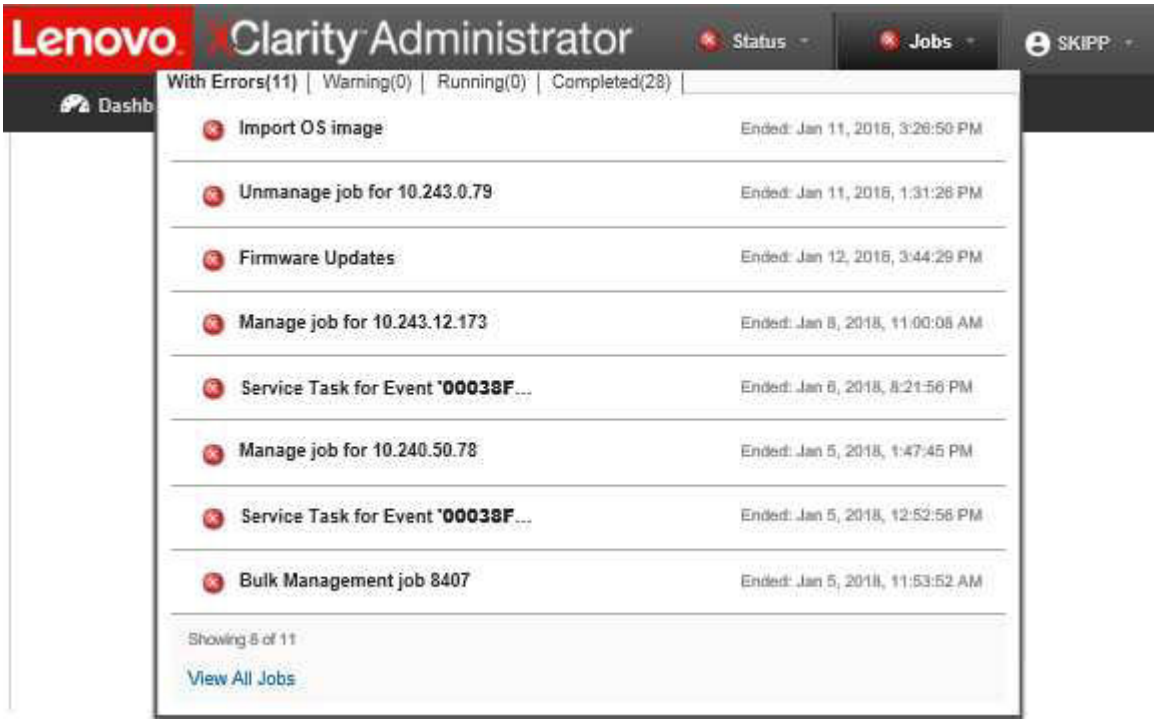
Step 10. Deploy the operating system by clicking **All actions → Deploy images**.

Step 11. From the confirmation page, click **Deploy** to deploy the image.

If the server currently has an operating system installed, you are warned about the fact that deploying the image will overwrite the current operating system.

Tip: You can set up a remote-control session to watch the installation as it progresses. Click **All actions → Remote Control** to start a remote-control session with the server.

When you deploy the operating system, Lenovo XClarity Administrator starts a job to track the deployment. To view the status of the deployment job, click **Jobs** from the Lenovo XClarity Administrator menu bar. Then, click the **Running** tab.

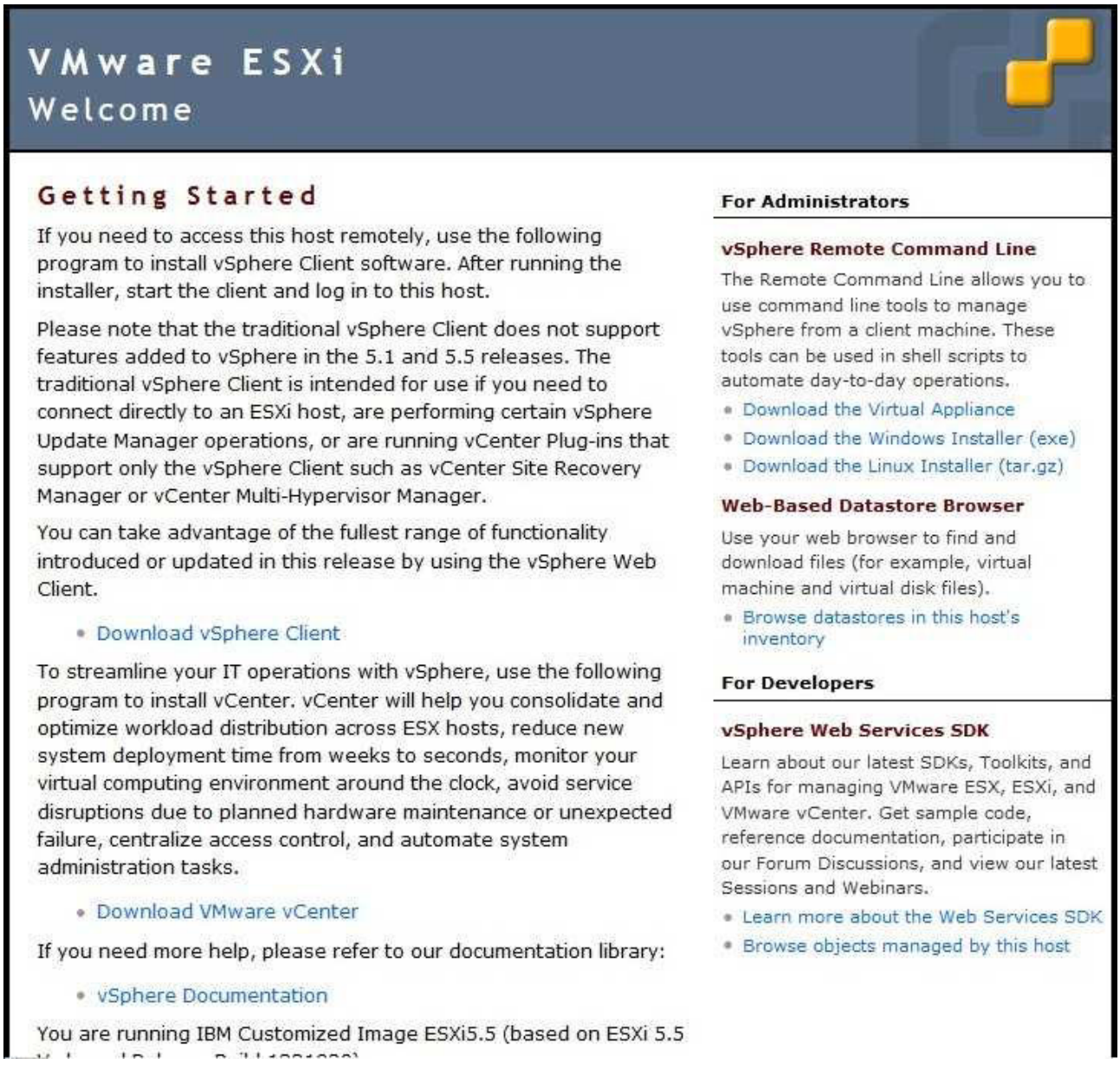


Hover over the running job to see the details, such as the percentage of the job that is complete.

Results

After the operating-system deployment has completed, log in to the IP address that you specified on the Edit Network Settings page to continue with the configuration process.

Note: The license provided with the image is a 60-day free trial. You are responsible for meeting all VMware licensing requirements.



Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

LENOVO, SYSTEM, NEXTSCALE, SYSTEM X, THINKSERVER, THINKSYSTEM, and XCLARITY are trademarks of Lenovo.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, Windows Server, Windows PowerShell, Hyper-V, Internet Explorer, and Active Directory are registered trademarks of the Microsoft group of companies.

Mozilla and Firefox are registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Nutanix is a trademark and brand of Nutanix, Inc. in the United States, other countries, or both.

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.

SUSE is atrademark of SUSE IP Development Limited or its subsidiaries or affiliates.

VMware vSphere is a registered trademark of VMware in the United States, other countries, or both.

All other trademarks are the property of their respective owners.


Lenovo

Lenovo

Lenovo XClarity Provisioning Manager V3 User Guide



Second Edition (March 2021)

© Copyright Lenovo 2020, 2021.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Chapter 1. Overview 1

Lenovo XClarity Provisioning Manager V3 introduction 1

Lenovo XClarity Provisioning Manager V3 startup . . 1

Main interface 3

Buttons on the LXPM V3 interfaces 3

Keyboard navigation 4

Downloading useful information 5

Chapter 2. Using LXPM V3 7

Getting started 7

Configuring network settings 9

System Summary 10

RAID Setup 12

OS Installation 14

Effortless Installation 15

Guided installation 20

Manual installation 40

Firmware Update 42

UEFI Setup 44

Cloning 48

Exporting response files 48

Importing response files 49

Diagnostics 50

Effortless diagnostic 50

Running diagnostics 51

Collecting service data 56

Effortless Reset 56

Chapter 3. Troubleshooting 61

Appendix A. Notices 63

Trademarks 64

© Copyright Lenovo 2020, 2021

Chapter 1. Overview

This chapter provides an overview of the Lenovo® XClarity Provisioning Manager V3 program (hereinafter referred to as LXPM V3). This chapter contains information about the program introduction, program startup, main interface, buttons displayed on the program interfaces, keyboard navigation, and how to download useful information.

Lenovo XClarity Provisioning Manager V3 introduction

LXPM V3 combines the functions of configuring Unified Extensible Firmware Interface (UEFI), configuring Redundant Array of Independent Disks (RAID), and updating applications and firmware. It also enables you to install the supported operating systems and associated device drivers, run diagnostics, and collect service data.

Lenovo XClarity Provisioning Manager has the following features:

- Easy-to-use, language-selectable interface
- Integrated help system
- Automatic hardware detection
- Ability to install an operating system and device drivers in an unattended mode or manually
- Ability to clone the settings in one server to other similarly configured Lenovo servers
- Supports RAID setup
- Supports firmware and applications update
- Supports UEFI setup
- Contains diagnostic utility
- Permanently erase all data on storage devices, clear all system logs, and reset the whole system to factory default

Note: When you are using LXPM V3, do not restart Lenovo XClarity Controller (also known as BMC).

Lenovo XClarity Provisioning Manager V3 startup

To start LXPM V3, do the following:

1. Turn on the server. Press F1 as soon as you see the logo screen.
2. If you have set a password, enter the correct password.
3. Wait for several seconds. LXPM V3 opens.

   Note: If the text-based interface for UEFI Setup opens instead of the LXPM V3, go to **System Settings → <F1> Start Control** and select **Tool Suite**. Then, restart the server and repeat step 1 to step 3 to open LXPM V3.

4. Click  on the top right corner of the interface and select the language in which you want to view the program. Then, you can start to use the program.

Notes:

- When LXPM V3 opens, if there is any system error or warning, a window will be displayed. Follow the guidance of the window to go to the Diagnostics interface to see the detailed information for the error or warning.

© Copyright Lenovo 2020, 2021

- After disabling **USB Mass Storage Driver Support** in **UEFI Setup → System Settings → Device and I/O Ports → USB Configuration**, text-based interface will replace LXPM V3 for UEFI Setup.

Main interface

The LXPM V3 main interface is divided into two panes. Click the tabs in the left pane to enter corresponding interfaces in the right pane.

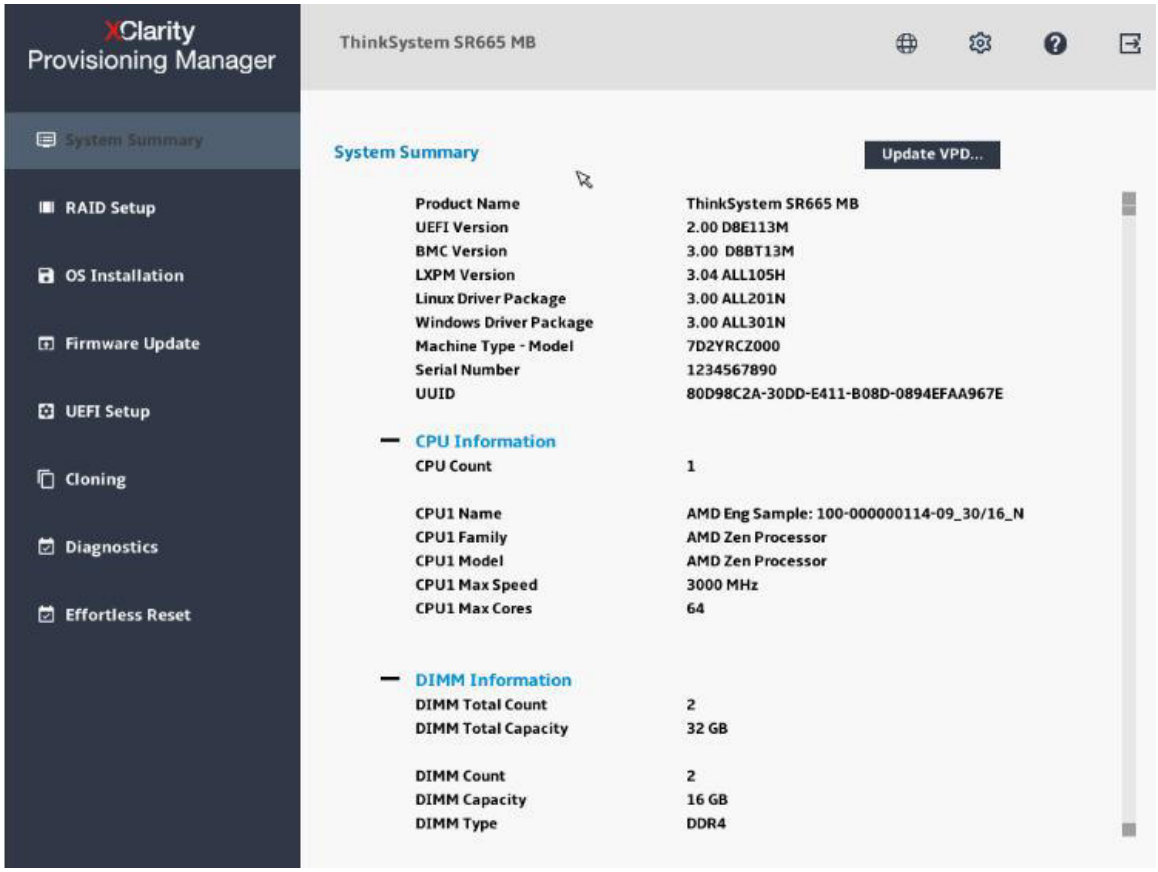


Figure 1. LXPM V3 main interface

Tabs in the left pane of the main interface

The following list provides information about each tab in the left pane of the LXPM V3 main interface:

- **System Summary**: View basic information about your server, such as CPU, DIMM, and PCI devices.
- **RAID Setup**: Configure RAID and disk settings.
- **OS Installation**: Follow the wizard to install an operating system and associated device drivers.
- **Firmware Update**: Update applications, firmware, and drivers for your server.
- **UEFI Setup**: View and change the UEFI settings of your server.
- **Cloning**: Export UEFI, RAID, and BMC settings to response files and import UEFI, RAID, BMC, and operating system installation settings from response files.
- **Diagnostics**: Collect service data and run diagnostics.
- **Effortless Reset**: Erase data, clear system logs, reset system to factory default.

Buttons on the LXPM V3 interfaces

The following table provides information about the buttons appear on the LXPM V3 interfaces.

Button	Description
	Select the language to be displayed. **Note:** LXPM V3 only supports English before June 2020.
	Display the Network Settings window. For details, refer to “Configuring network settings” on page 9.
	Click this button to display the following items: • **Help**: View context-sensitive help information for each interface. • **HotKey**: View keyboard navigation information. • **Getting Started**: View a brief introduction to LXPM V3, do some basic system settings and management network settings, and modify the Lenovo XClarity Controller credentials. • **License Agreement**: View Lenovo license agreement. • **Third-party Licenses**: View the third-party licenses. • **About**: View the LXPM V3 version, copyright, and trademark information.
	Exit LXPM V3.
	Return to the previous interface.
	Save changes.
	Discard changes and load previous values.
	Load the optimized default values.
	Return to the previous step.
	Go to the next step.

Keyboard navigation

Note: Only United States layout keyboard is applicable in LXPM V3 user interface.

LXPM V3 supports navigation by using either mouse or keyboard. The following are the keys used for keyboard navigation:

- Ctrl+Tab: Switch between the left pane and the right pane.
- Tab: Move forward to the next selectable item in the active pane.
- Shift+Tab: Move backward to the previous selectable item in the active pane.
- Space: Same as a click when a button is active.
- Up arrow: Scroll up.
- Down arrow: Scroll down.

For UEFI Setup, the following keys can be used for keyboard navigation:

- Enter: Select.
- +: Increase the value.
- –: Decrease the value.
- Esc: Return to the previous interface.
- F1: Display the help information.
- F2: Load the previous values.
- F3: Load the optimized default values.
- F4: Save and exit UEFI Setup.

Downloading useful information

Lenovo releases firmware, applications, and device drivers in bundles called UpdateXpress System Packs (UXSPs). To download the UXSPs, go to:
http://datacentersupport.lenovo.com

Chapter 2. Using LXPM V3

This chapter provides information about using LXPM V3.

Getting started

Click ? on the top right corner of the LXPM V3 main interface; then, click **Getting Started**. The following interface is displayed.

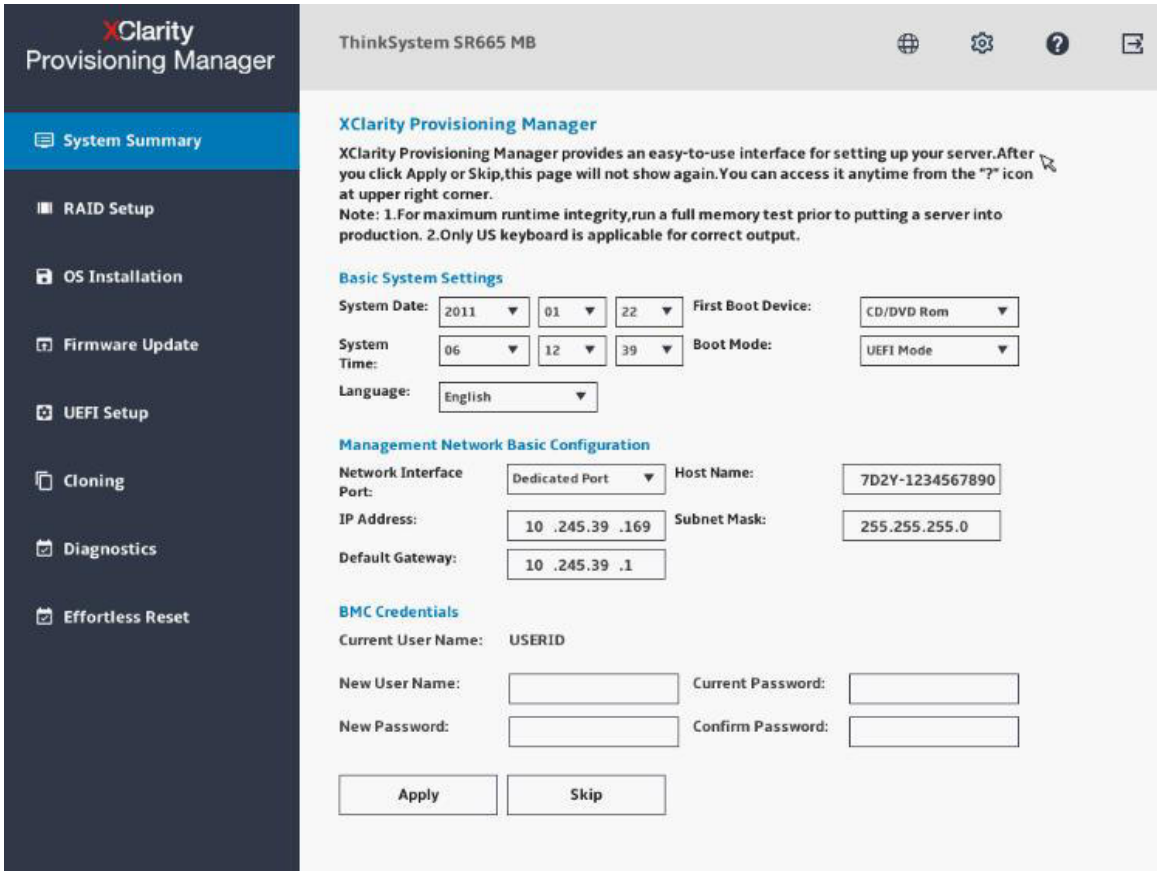


Figure 2. Getting Started interface

In this interface, you can do the following:

- View a general introduction to LXPM V3.
- Configure basic settings for the server, including system date, system time, language, first boot device, and boot mode.
- Configure the Lenovo XClarity Controller basic settings, including network interface port, IP address, default gateway, hostname, and subnet mask.
- Modify the Lenovo XClarity Controller credentials.

Modifying Lenovo XClarity Controller credentials

To modify the Lenovo XClarity Controller credentials, do one of the following:

© Copyright Lenovo 2020, 2021

- To modify the user name, input the new user name and the current password, and click **Apply**.
- To modify the password, input the current password and the new password, input the new password again, and click **Apply**.
- To modify the user name and password at the same time, input the new user name, current password, and new password, input the new password again, and click **Apply**.

Configuring network settings

To configure the network settings, do the following:

1. Click on the top right corner of the LXPM V3 main interface. The following Network Settings window is displayed.

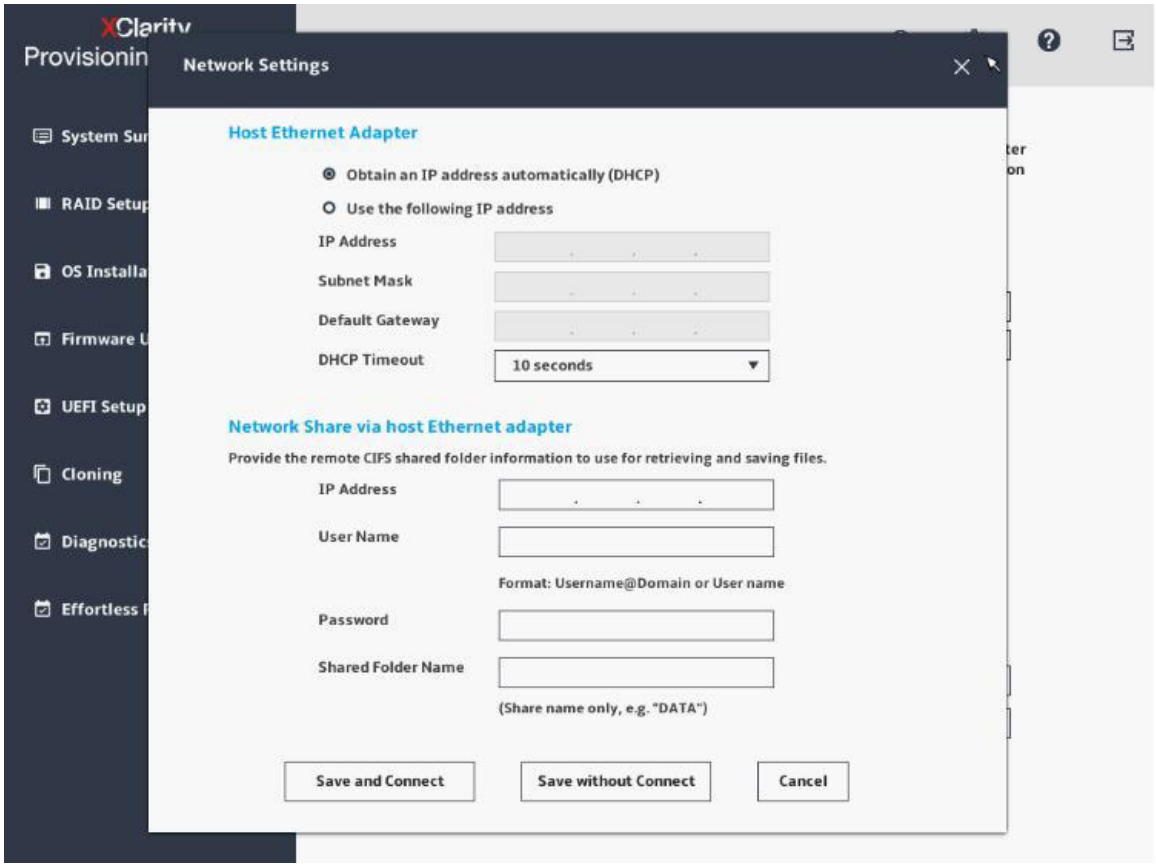


Figure 3. Network Settings window

2. Follow the instructions on the screen to configure the network settings.
3. After configuring the network settings, click one of the following buttons according to your needs:
   - **Save and Connect**: Save the settings and connect to the shared network. If the network cannot be connected, an error message will be displayed.
   - **Save without Connect**: Save the settings without connecting to the shared network. When you click the button, a confirmation window is displayed. Click **Continue** to save the settings without connecting, or click **Cancel** to go back to the Network Settings window.
   - **Cancel**: Discard the changes and exit the Network Settings window.

System Summary

Click the **System Summary** tab in the left pane to view the following system information in the right pane:

- Product name
- UEFI, BMC, and LXPM V3 version information
- Machine type and serial number
- Universally Unique Identifier (UUID)
- Operating system driver package information
- CPU information
- DIMM information
- PCI device information
- Disk drive information
- Partition information

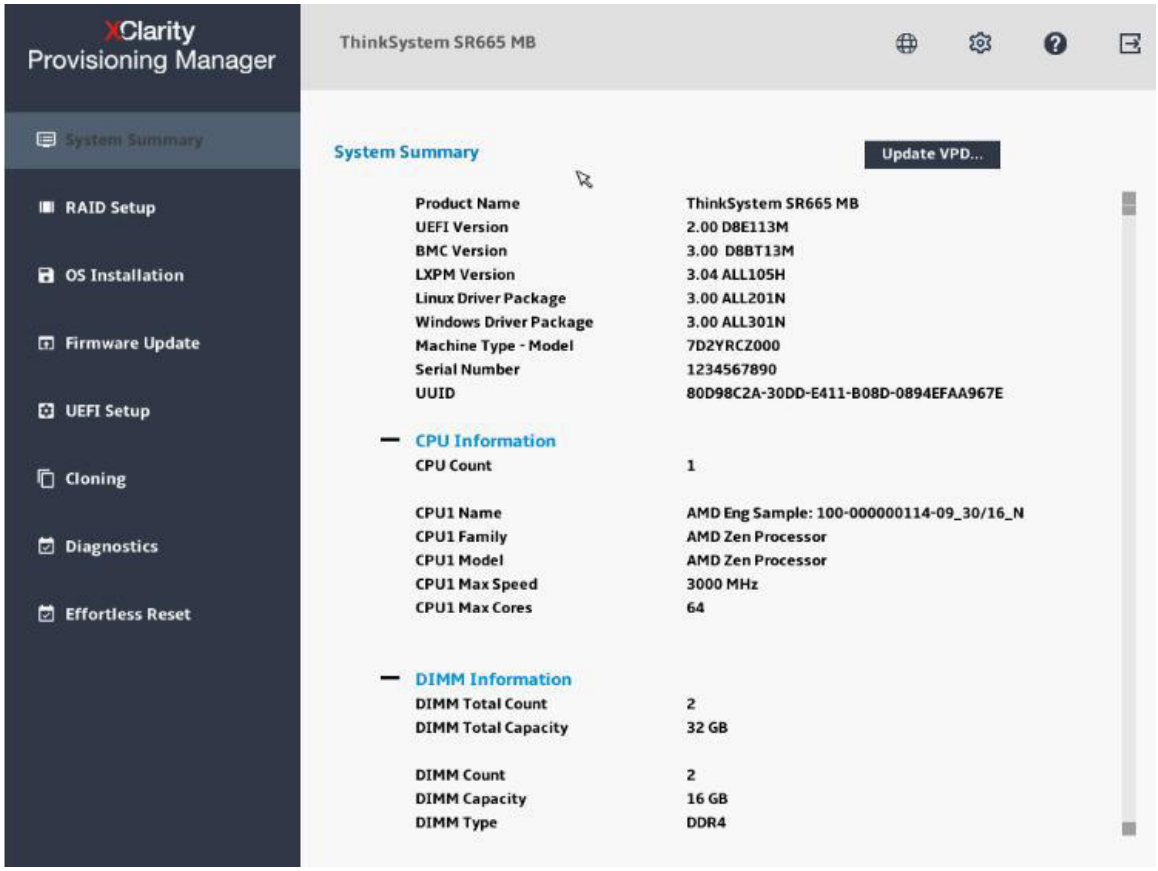


Figure 4. System Summary interface

You can click **Update VPD...** to enter the Update VPD interface to update some Vital Product Data (VPD), such as asset tag and UUID. You also can check or configure the TPM/TCM policy in the Update VPD interface.

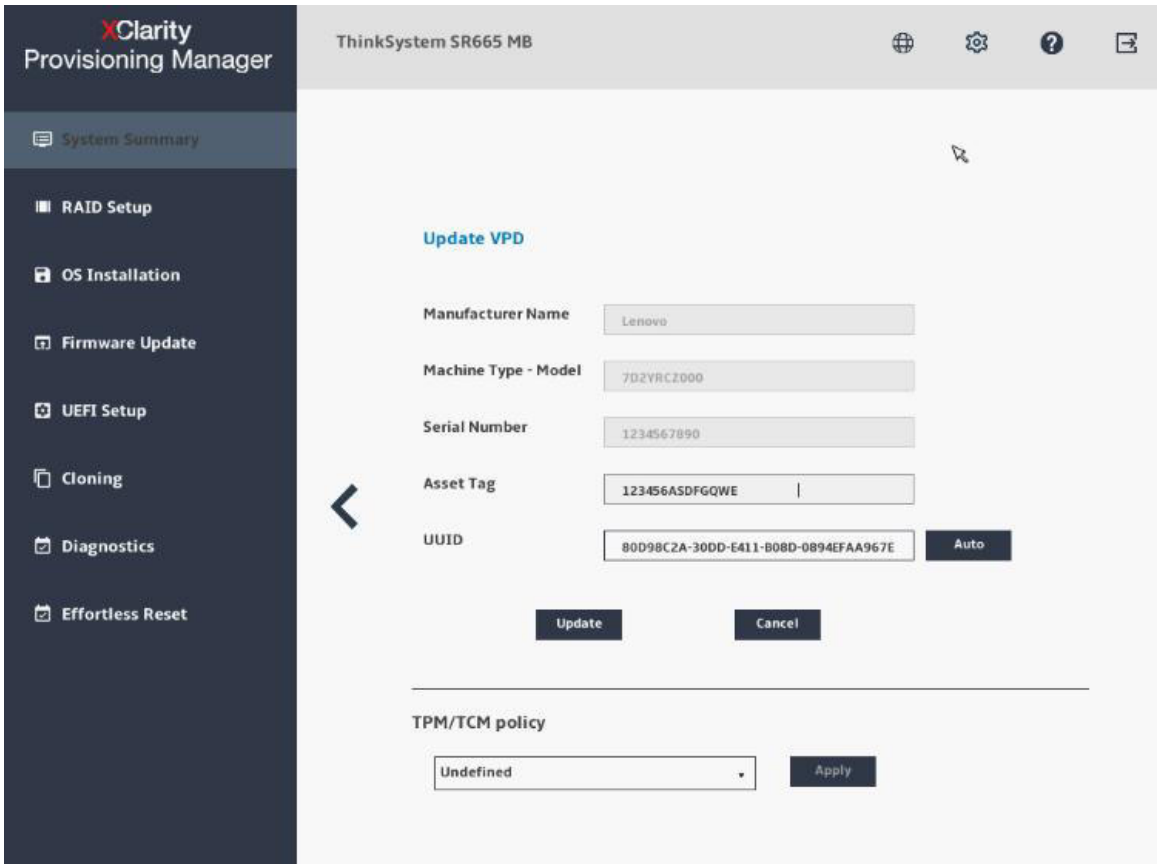


Figure 5. Update VPD

Notes:

- The Non-Volatile Memory express (NVMe) SSDs are recognized as PCIe devices and listed in the PCI device information section.

  Note: This is for servers with AMD processors only.
- For a running server, device changes will not be displayed in the System Summary interface in real time. To view the latest device information, you should restart the server.
- When **Legacy BIOS** is set to **Disable** in the UEFI Setup interface, all hard disk drives will be displayed in the disk drive information section. When **Legacy BIOS** is set to **Enable**, the hard disk drives connected to the RAID adapters will not be displayed.

RAID Setup

Click the **RAID Setup** tab in the left pane to enter the wizard for configuring RAID and disk settings for the installed RAID adapters. The following is the first interface for the wizard.

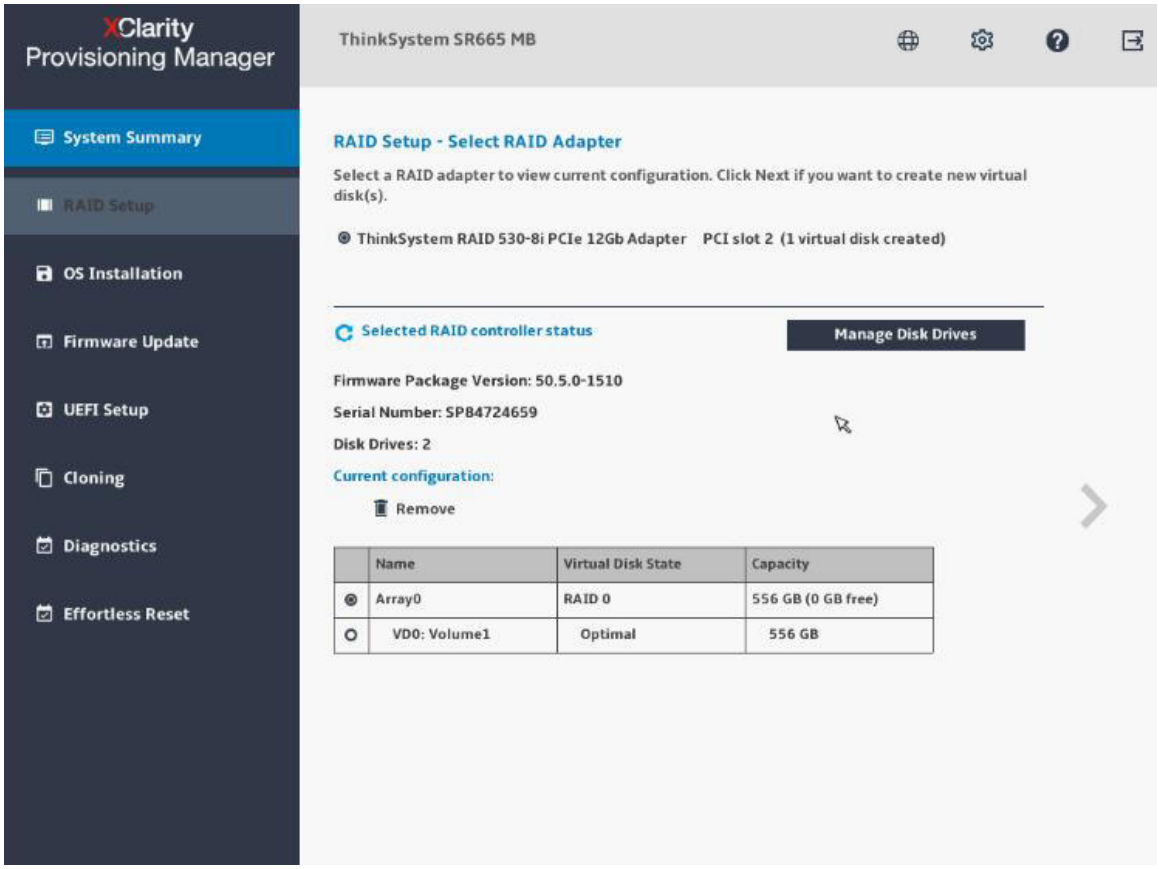


Figure 6. RAID Setup - Select RAID Adapter interface

To configure RAID and disk settings, follow the wizard to do the following:

1. Select the RAID adapter you want to configure. The basic information and current configuration for the selected RAID adapter will be displayed.
2. If you want to delete a disk array or a virtual disk for the selected RAID adapter, select the disk array or virtual disk you want to delete and click **Remove**. Then, follow the instructions on the screen to delete it.
3. If you want to view or change the drive status for the selected RAID adapter, click **Manage Disk Drives** to enter the Manage Disk Drives interface. In this interface, all the drives connected to the selected RAID adapter are listed. You can change the drive status according to your needs. Then, click > and confirm to save changes and return to the “RAID Setup - Select RAID Adapter” interface or click < to discard changes and return to the “RAID Setup - Select RAID Adapter” interface.

   Note: If you are configuring the ThinkSystem™ M.2 with Mirroring Enablement Kit, you cannot change the drive status, but only can view the drive status in the Manage Disk Drives interface.

4. Click > or click **Start** to enter the “RAID Setup - Select RAID configuration type” interface and do one of the following:

- Select **Simple configuration** and go to step 5.
- Select **Advanced configuration** and select **Create new disk array and virtual disk** in the drop-down list box. Then, go to step 6.
- Select **Advanced configuration** and select **Use free capacity on the existing disk array** in the drop-down list box. Then, go to step 7.

5. Click  to enter the “RAID Setup - Set RAID level and hot spare” interface. Select the RAID level and choose to select or clear the **Add Hot Spare Drive** check box. If the check box is selected, one of the drives is assigned for dedicated hot spare function. Then, go to step 9.

   Notes:

   - If you are configuring the ThinkSystem M.2 with Mirroring Enablement Kit, you can choose RAID 0 or RAID 1 as the RAID level. Choose RAID 1 to implement mirroring.
   - If you are configuring integrated software RAID or ThinkSystem M.2 with Mirroring Enablement Kit, the **Add Hot Spare Drive** check box will not be displayed.

6. Click  to enter the “RAID Setup - Select RAID Level and Select Drives” interface. Select the RAID level and the drives for the new disk array, and set the role for each drive. Then, go to step 8.
7. Click  to enter the “RAID Setup - Select Disk Array” interface. All the disk arrays that have free space will be displayed. Select a disk array for the new virtual disk.
8. Click  to enter the “RAID Setup - Create and Edit Virtual Disk” interface. You can create new virtual disks. Then, you can edit or remove the new virtual disks. Follow the instructions on the screen to do the configuration.
9. Click  to enter the “RAID Setup - Verify settings” interface. Double check the settings and click  . A confirmation window is displayed.
10. Click **Yes** to enter the “RAID Setup - Creating Virtual Disk(s)” interface. The virtual disk creation result is displayed.
11. Click  to return to the first interface of the wizard and view the current configuration of the selected RAID adapter.

OS Installation

Click the **OS Installation** tab in the left pane to enter the OS Installation interface. The OS Installation interface provides a configuration wizard for installing an operating system.

Note: If you want to configure RAID settings before installing an operating system, it is recommended to do the configuration in the RAID Setup interface. If you do the configuration in UEFI Setup, you must restart your server before installing the operating system to ensure that the RAID configuration takes effect.

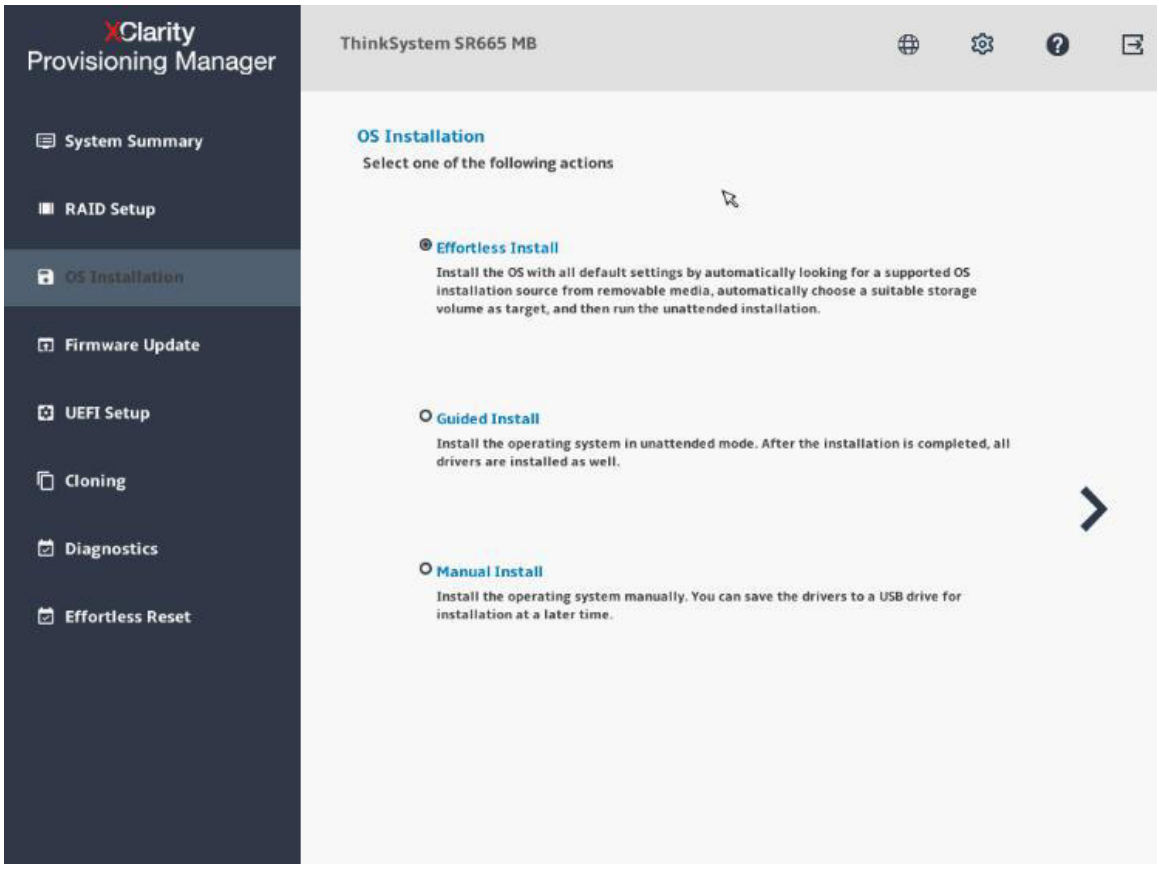


Figure 7. OS Installation interface

There are three types of installation for your selection:

- **Effortless Install**: Automatically detect, choose, and install an operating system and device drives with all default settings in an unattended mode.
- **Guided Install**: Install an operating system and device drivers in an unattended mode.
- **Manual Install**: Install an operating system and device drivers manually.

Note: The device drivers installed with the operating system are not complete. To view the complete list of the supported device drivers, refer to the readme files included in the Windows® Driver Bundle update package and Linux® Driver Bundle update package. To download the update packages, go to: http://datacentersupport.lenovo.com.

Effortless Installation

Prerequisites

Ensure that the minimum space of the target storage device for installing the OS meets the following requirements:

- For Windows/VMware OS, the minimum space should be 10 GB.
- For Red Hat Enterprise Linux (RHEL)/SUSE Linux Enterprise Server (SLES) OS, the minimum space should be 24 GB.

Before performing effortless installation:

- Ensure that the boot mode is preset by doing one of the following:
  - Click  on the top right corner of the LXPM V3 main interface and click **Getting Started**. Set the boot mode to be **UEFI Mode**.
  - Go to **UEFI Setup → Boot Manager → Boot Modes → System Boot Mode** and select **UEFI Mode**.
- Ensure that operating system installation files are prepared in one of the following:
  - CD or DVD

    Note: Ensure that the disc is clean and the version and architecture of the operating system are correct.
  - USB storage drive

    To create a USB installation medium, refer to the documentation at: http://cn.download.lenovo.com/ibmdl/pub/pc/pccbbs/thinkservers/how_to_create_usb_os_installation_media.pdf
  - Shared network based on management network

    Note: Ensure that the Ethernet connector for system management is active and can connect to the specified IP address.

    If the shared network is connected, you can prepare the operating system installation files through Lenovo XClarity Controller.

Performing effortless installation

In the OS Installation interface, select **Effortless Install** and click  . Refer to one of the following to install an operating system:

- “Installing a Windows operating system” on page 16
- “Installing an RHEL operating system” on page 18
- “Installing an SLES operating system” on page 19
- “Installing a VMware operating system” on page 20

Notes:

- The default Administrator password for installing a Windows operating system is “PASSW0RD”.
- The default root password for installing an RHEL/SLES/VMware operating system is “1234567”.
- Users should reset the password when logging in to the operating system for the first time.

Installing a Windows operating system

The wizard provides a step by step guidance for installing an operating system. Follow the instructions on the screen and the tips listed below to install a Windows operating system.

Note: For the information about the operating system compatibility, refer to https://lenovopress.com/osig.

1. Verify that the installation settings are correct, and click .

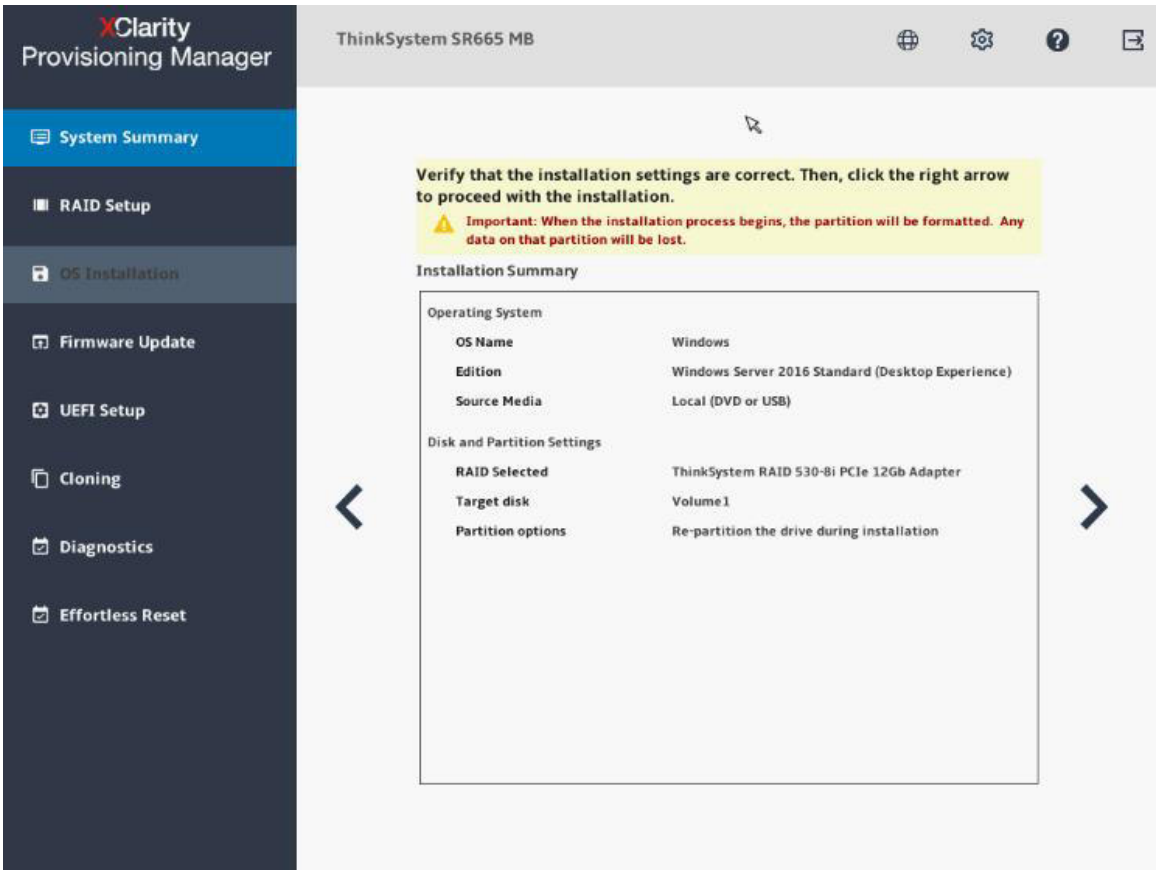


Figure 8. Installation Summary

2. Wait for several minutes, the Windows Setup window is displayed. Do one of the following based on your needs:

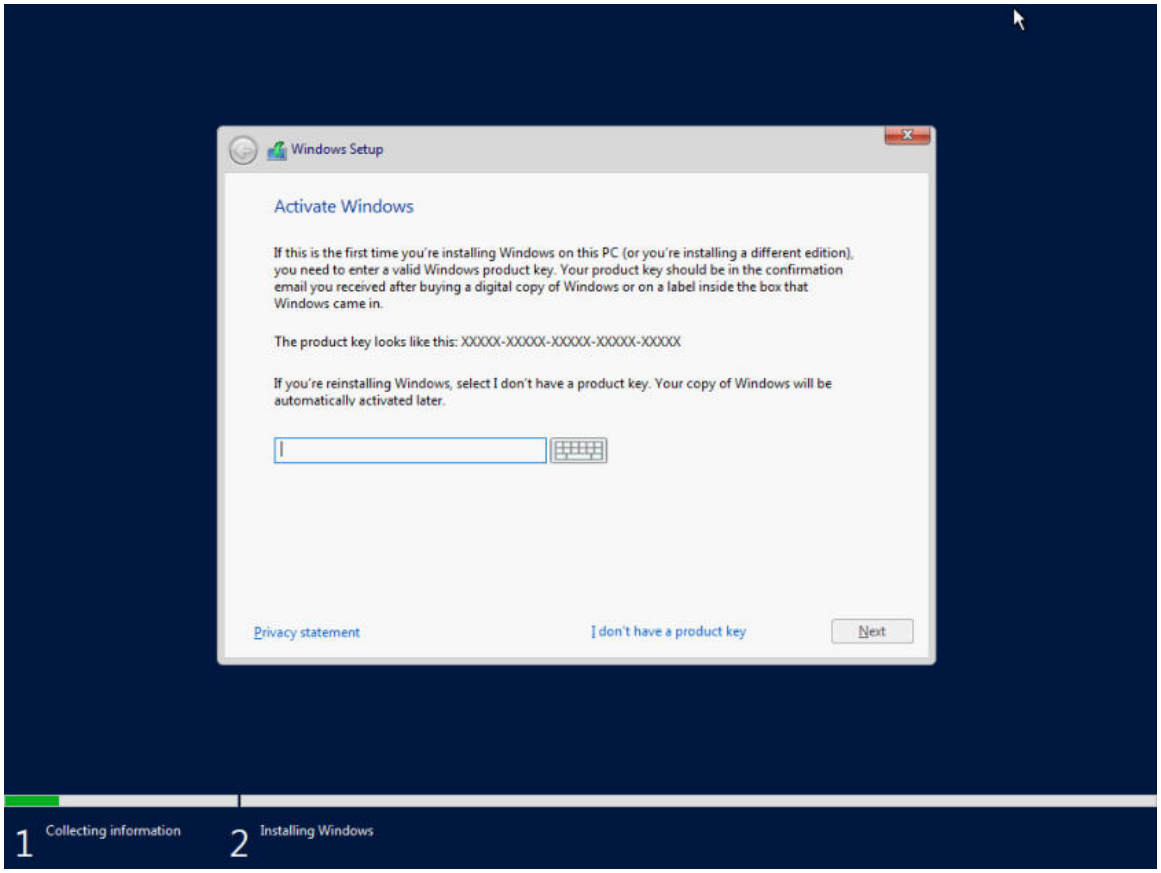


Figure 9. Activate Windows

- If you have a valid Windows product key, input the product key and click **Next** to start installation.
- If you don't have a valid Windows product key, click **I don't have a product key** to start installation.

3. After the installation procedure is completed, wait for several minutes, LXPM will be automatically restarted to make all installed drivers take effect.

Installing an RHEL operating system

The wizard provides a step by step guidance for installing an operating system. Follow the instructions on the screen and the tips listed below to install an RHEL operating system.

1. Verify that the installation settings are correct, and click ❯ to start installation.

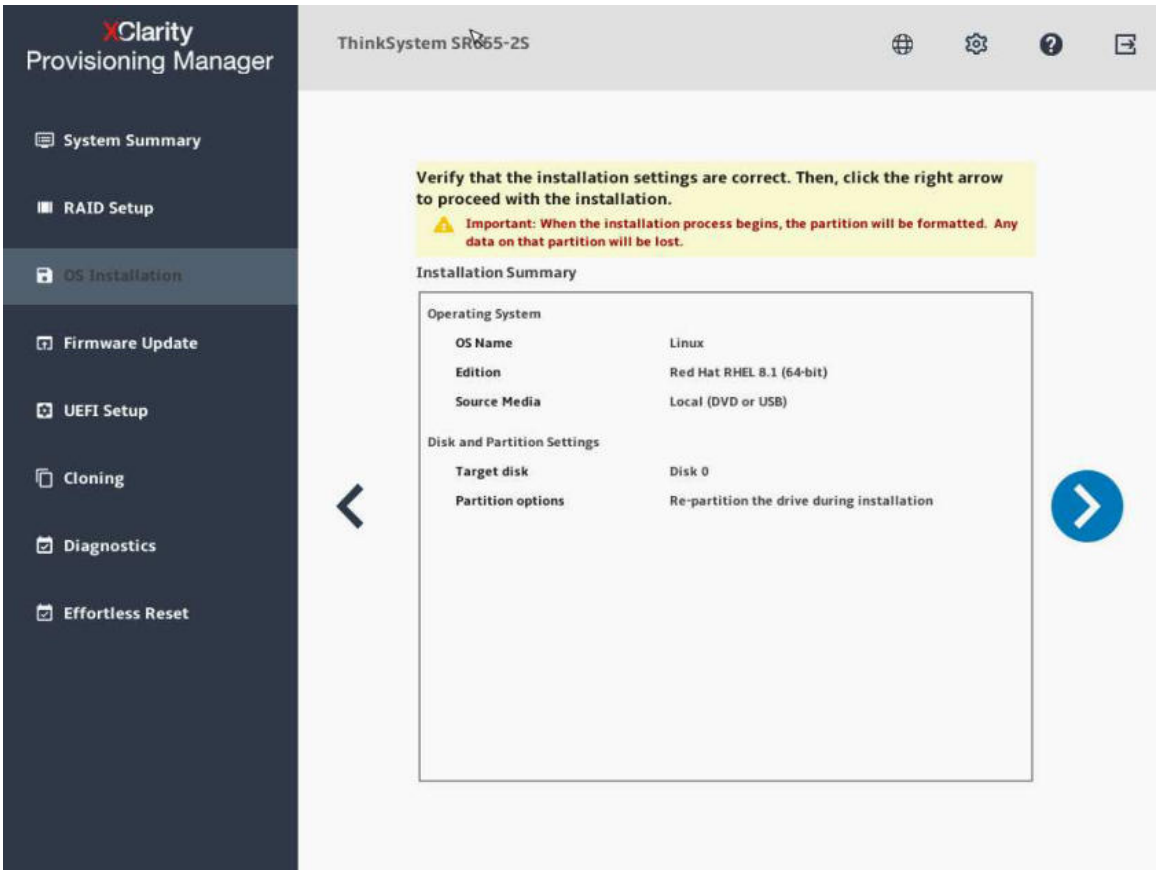


Figure 10. Installation Summary

2. Wait for several minutes until the installation procedure is completed. LXPM will be automatically restarted to make all installed drivers take effect.
3. Input user name and password, and click **Sign in** to enter into RHEL.

Installing an SLES operating system

The wizard provides a step by step guidance for installing an operating system. Follow the instructions on the screen and the tips listed below to install a SLES operating system.

1. Verify that the installation settings are correct, and click › to start installation.

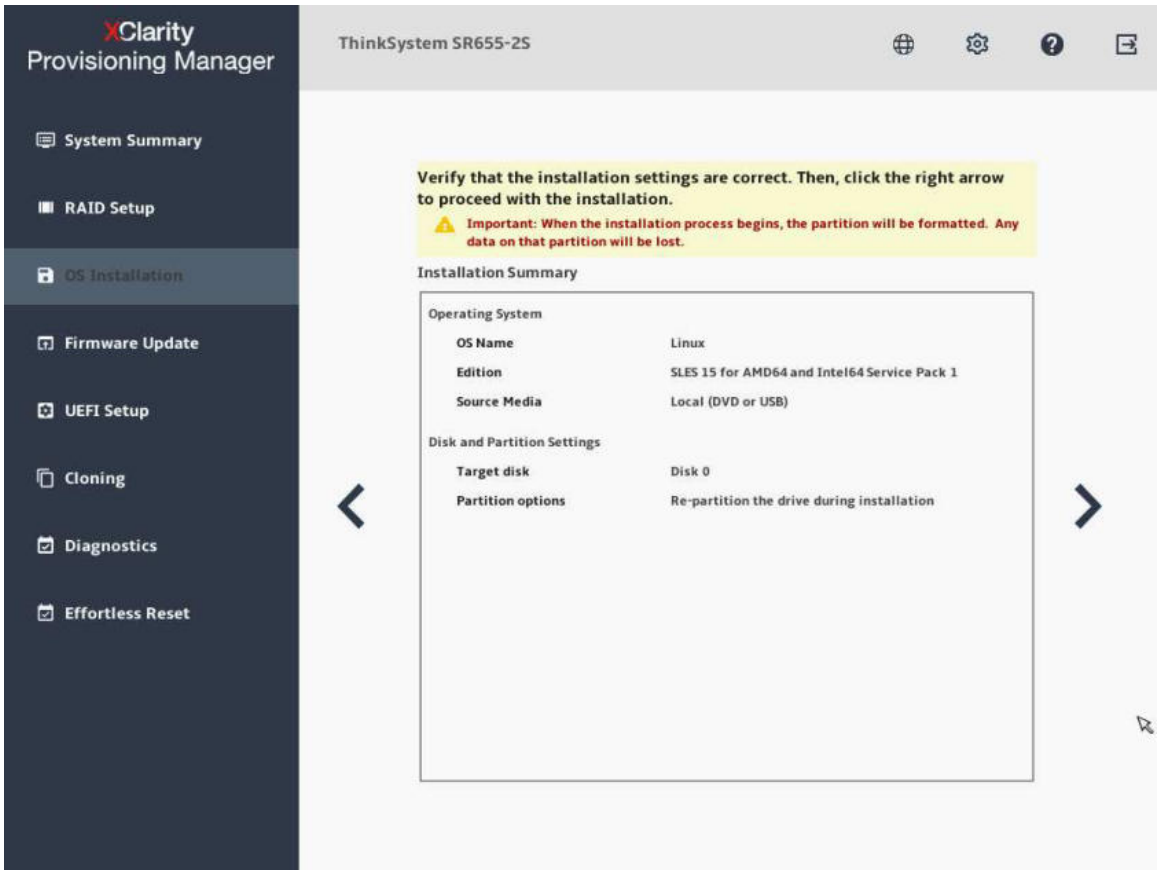


Figure 11. Installation Summary

2. Wait for several minutes until the installation procedure is completed. LXPM will be automatically restarted to make all installed drivers take effect.
3. Input user name and password, and click **Sign in** to enter into SLES.

Installing a VMware operating system

The wizard provides a step by step guidance for installing an operating system. Follow the instructions on the screen and the tips listed below to install a VMware operating system.

1. Verify that the installation settings are correct, and click ❯ to start installation.

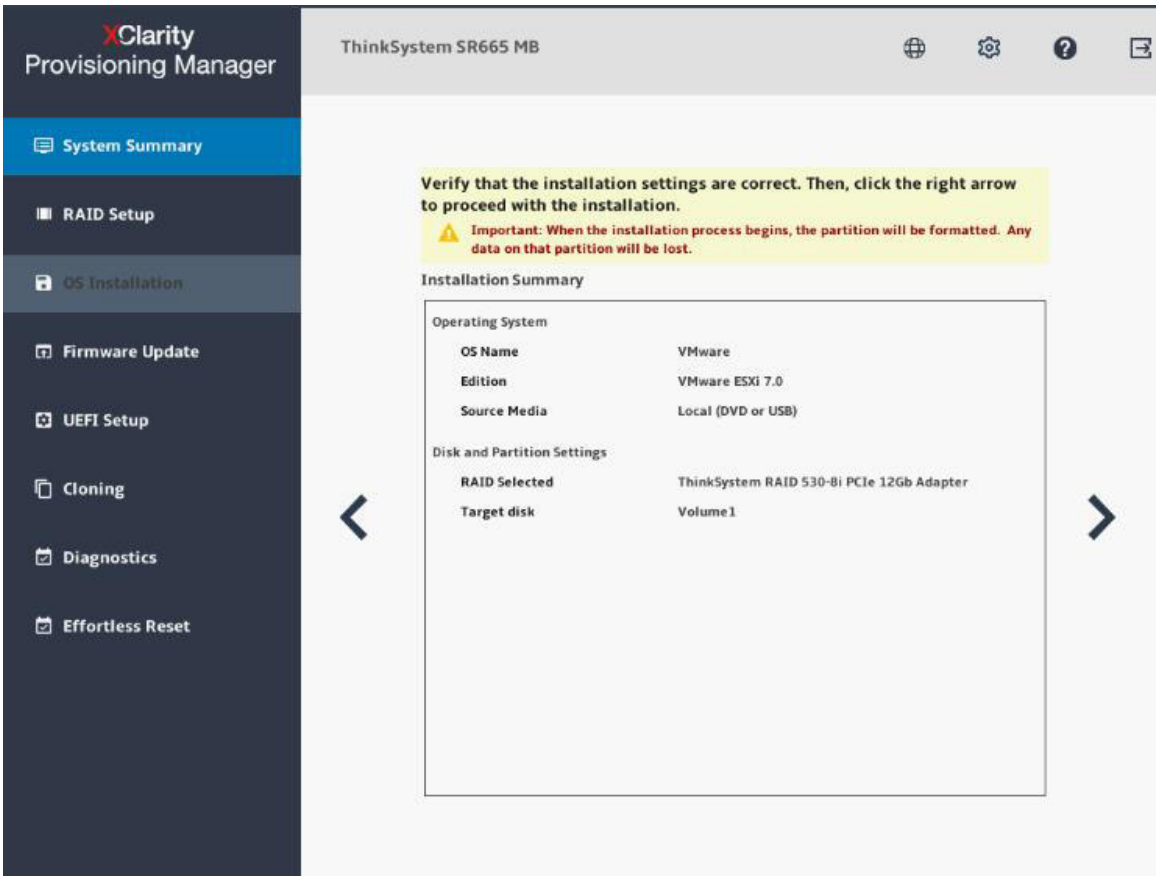


Figure 12. Installation Summary

2. Wait for several minutes until the installation procedure is completed. LXPM will be automatically restarted to make all installed drivers take effect.

   Note: If a warning window is displayed, press Enter to continue or just wait for several minutes and the installation will continue automatically.

3. When the VMware interface is displayed, press F2, input the authorized login name and password for local host, and press Enter to enter into VMware.

Guided installation

Prerequisites

Before performing guided installation:

- Ensure that the boot mode is preset by doing one of the following:
  - Click ? on the top right corner of the LXPM V3 main interface and click **Getting Started**. Set the boot mode to be **UEFI Mode**.

  - Go to **UEFI Setup → Boot Manager → Boot Modes → System Boot Mode** and select **UEFI Mode**.
- Ensure that operating system installation files are prepared in one of the following:
  - CD or DVD

    Note: Ensure that the disc is clean and the version and architecture of the operating system are correct.
  - USB storage drive

    To create a USB installation medium, refer to the documentation at: http://cn.download.lenovo.com/ibmdl/pub/pc/pccbbs/thinkservers/how_to_create_usb_os_installation_media.pdf
  - Shared network based on management network

    Note: Ensure that the Ethernet connector for system management is active and can connect to the specified IP address.

    If the shared network is connected, you can prepare the operating system installation files through Lenovo XClarity Controller. If the shared network is a CIFS server based on Linux Samba, the Samba configuration file "/etc/samba/smb.conf" shall have "ntlm auth = yes" in the "[global]" section.

Performing guided installation

In the OS Installation interface, select **Guided Install** and click  . Refer to one of the following to install an operating system:

- “Installing a Windows operating system” on page 22
- “Installing a Linux operating system” on page 29
- “Installing a VMware operating system” on page 36

Device drivers will be automatically installed during guided installation. It's recommended to reboot the OS after the guided installation is completed to make all drivers take effect. You also can export the operating system installation settings to a response file. For more information, refer to “Exporting an operating-system-installation response file” on page 40.

Installing a Windows operating system

The wizard provides a step by step guidance for installing an operating system. Follow the instructions on the screen and the tips listed below to install a Windows operating system.

Note: For the information about the operation system compatibility, refer to https://lenovopress.com/osig.

1. **Drive Selection**

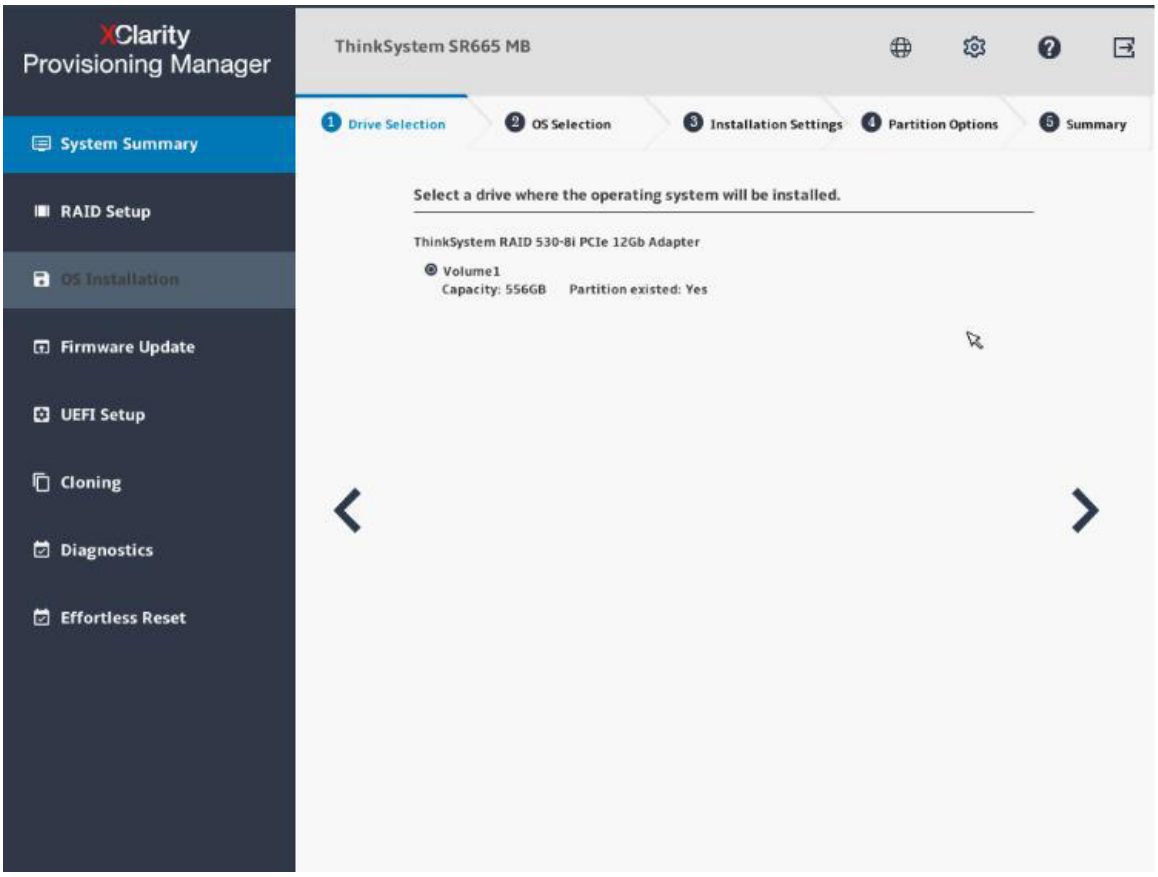


Figure 13. Drive Selection step (for Windows)

Attention: The selected drive will be formatted during the installation. Back up all data on it before the installation.

Note: The drivers will be installed automatically after the OS installation. It is recommended to restart your server to ensure that all installed drivers take effect.

2. **OS Selection**

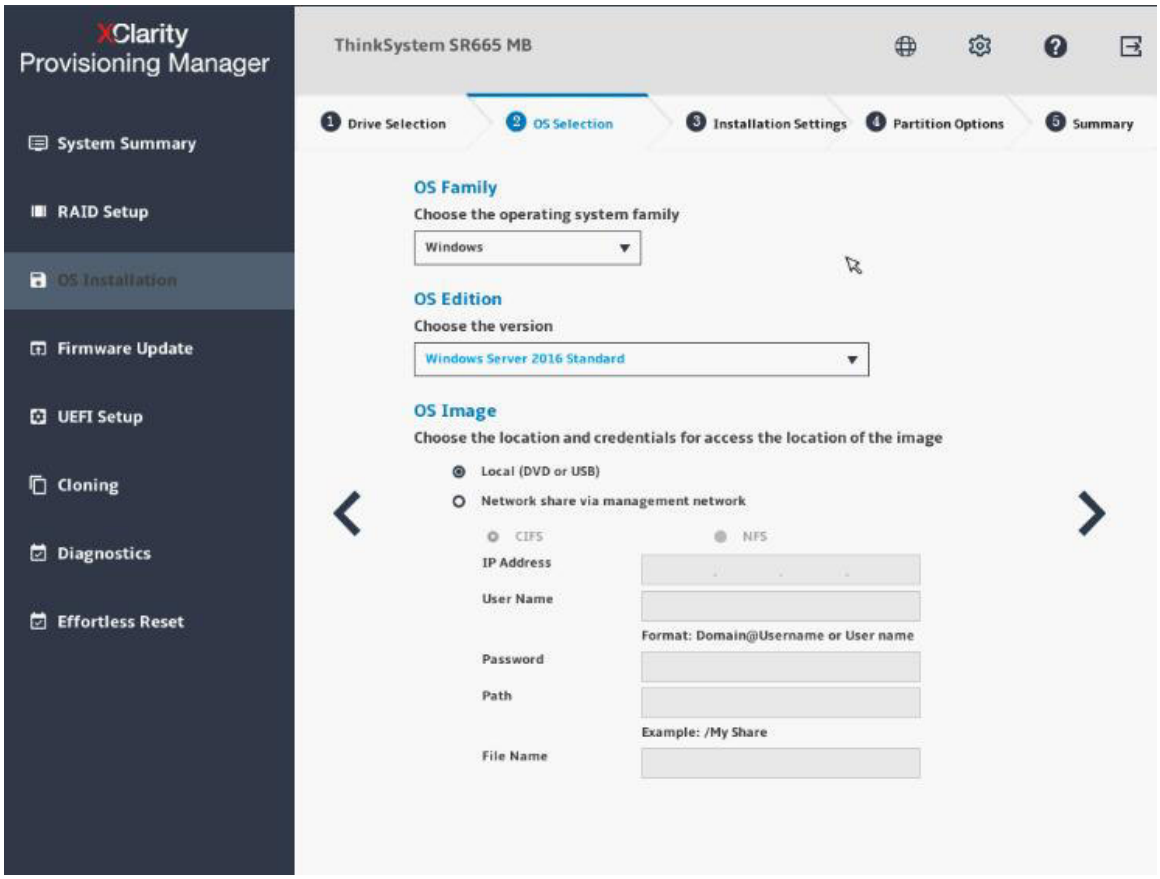


Figure 14. OS Selection step (for Windows)

The IP address is made up of four parts separated by dots. The following table lists the valid value range for each part.

IP Address	Part 1	Part 2	Part 3	Part 4
Valid values	1 – 223	0 – 255	0 – 255	0 – 255

3. **Installation Settings**

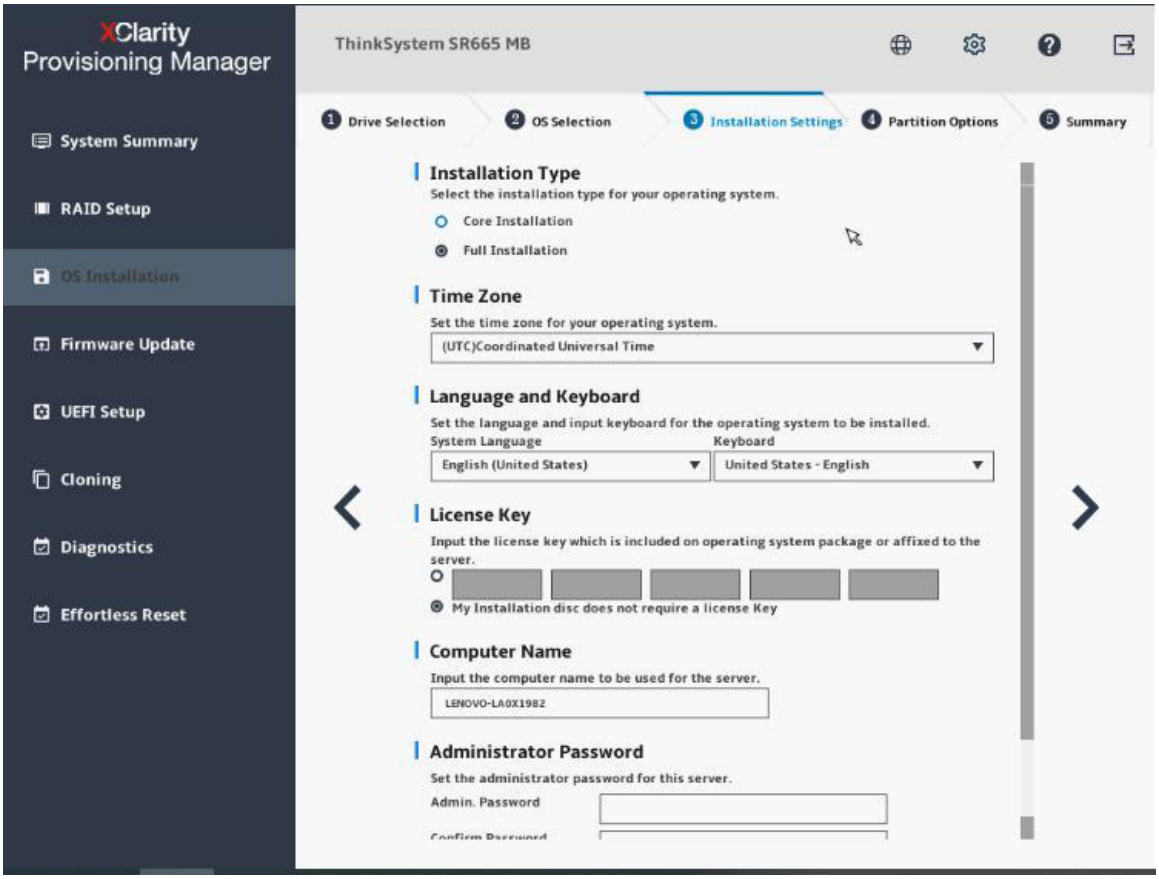


Figure 15. Installation Settings step – 1 (for Windows)

Administrator Password: You can change your administrator password later from the operating system.

If you want to do advanced configurations, expand the list by clicking the arrow icon next to **Advanced**.

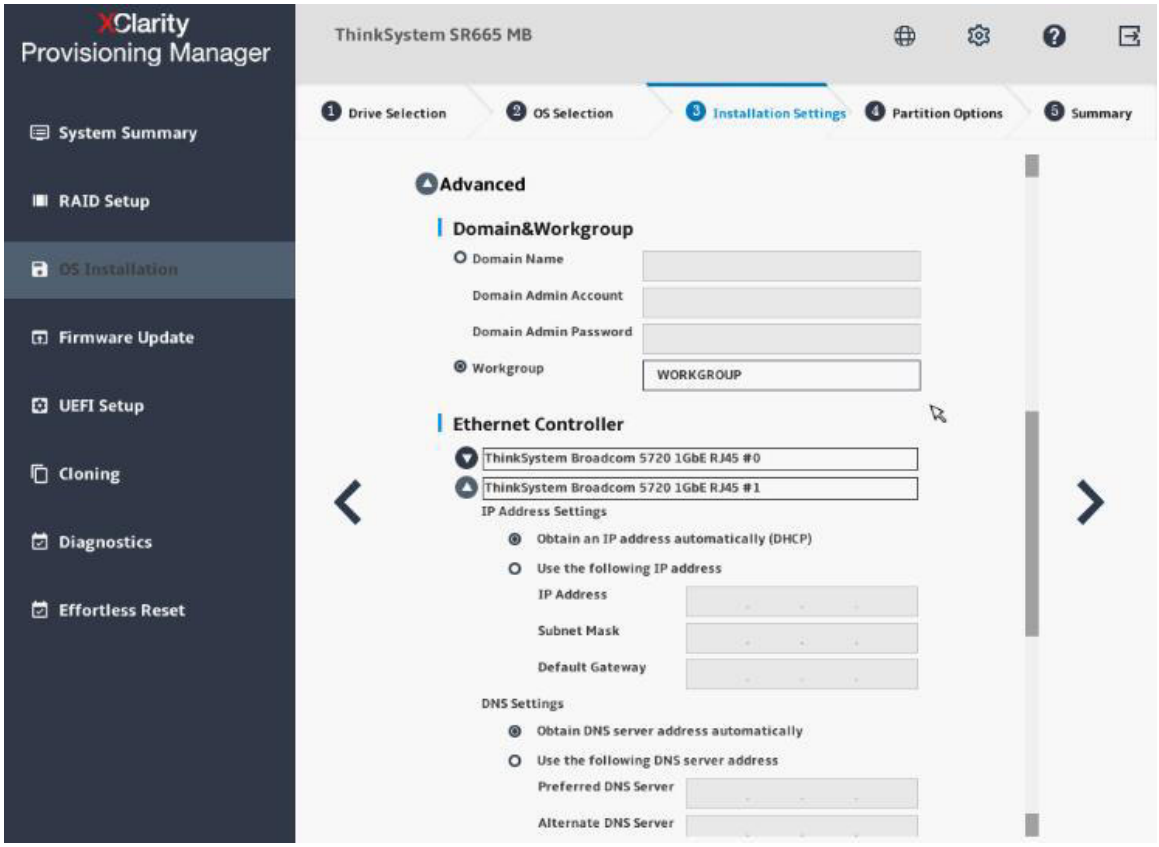


Figure 16. Installation Settings step – 2 (for Windows)

Refer to the following table for the valid values when you type the required address information.

Address	**Part 1**	**Part 2**	**Part 3**	**Part 4**
IP Address	1 – 126; 128 – 223	0 – 255	0 – 255	1 – 254
Subnet Mask	0 – 255	0 – 255	0 – 255	0 – 255
Default Gateway	0 – 255	0 – 255	0 – 255	0 – 255
Preferred DNS Server	1 – 126; 128 – 223	0 – 255	0 – 255	0 – 255
Alternate DNS Server	1 – 126; 128 – 223	0 – 255	0 – 255	0 – 255

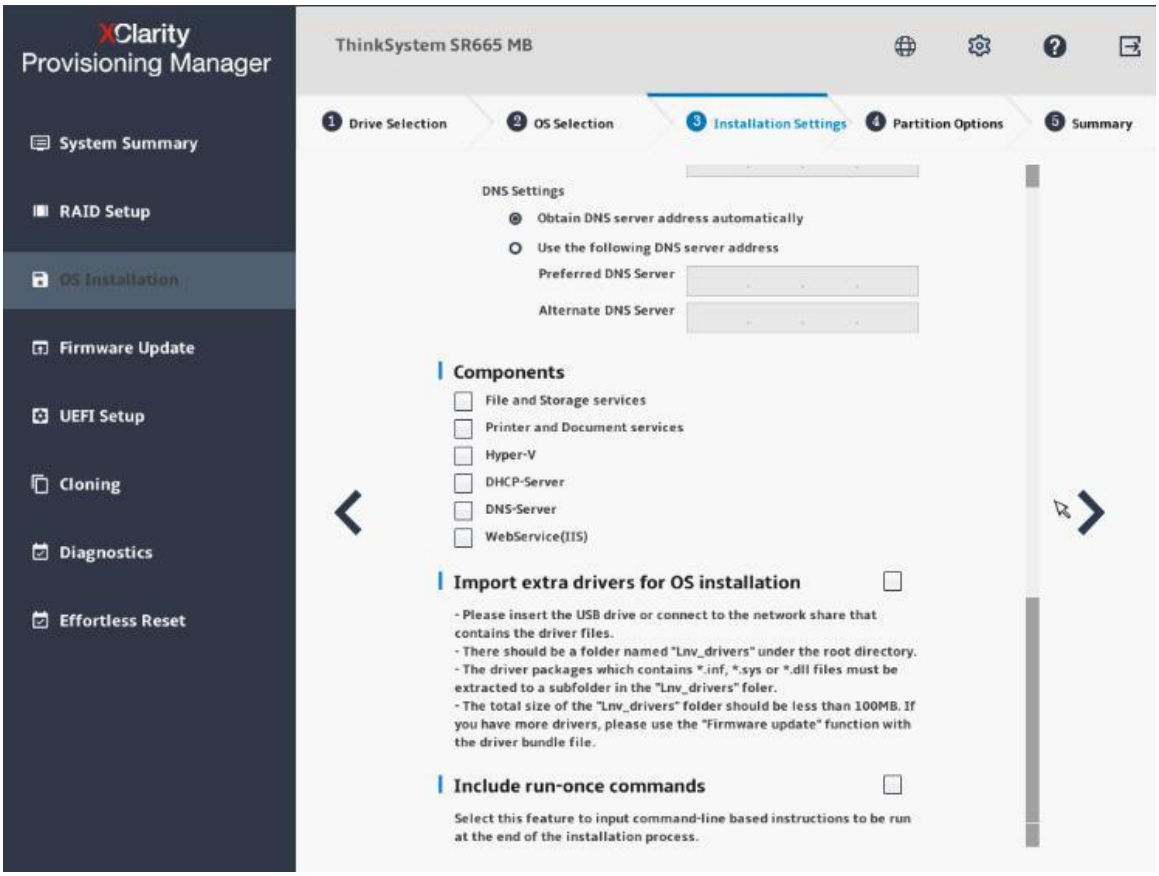


Figure 17. Installation Settings step – 3 (for Windows)

Components: You can select one or more components for installation according to your requirements.

Include run-once commands: If you want to run specified commands at the end of the installation process, select the check box. A command-type area is displayed. Input one command and click **Add**. The command is added to the command list. You can add five commands at most. If you want to remove a certain command, select it and click **Remove**. The commands in the command list will be run one time only and in the order you type them.

4. **Partition Options**

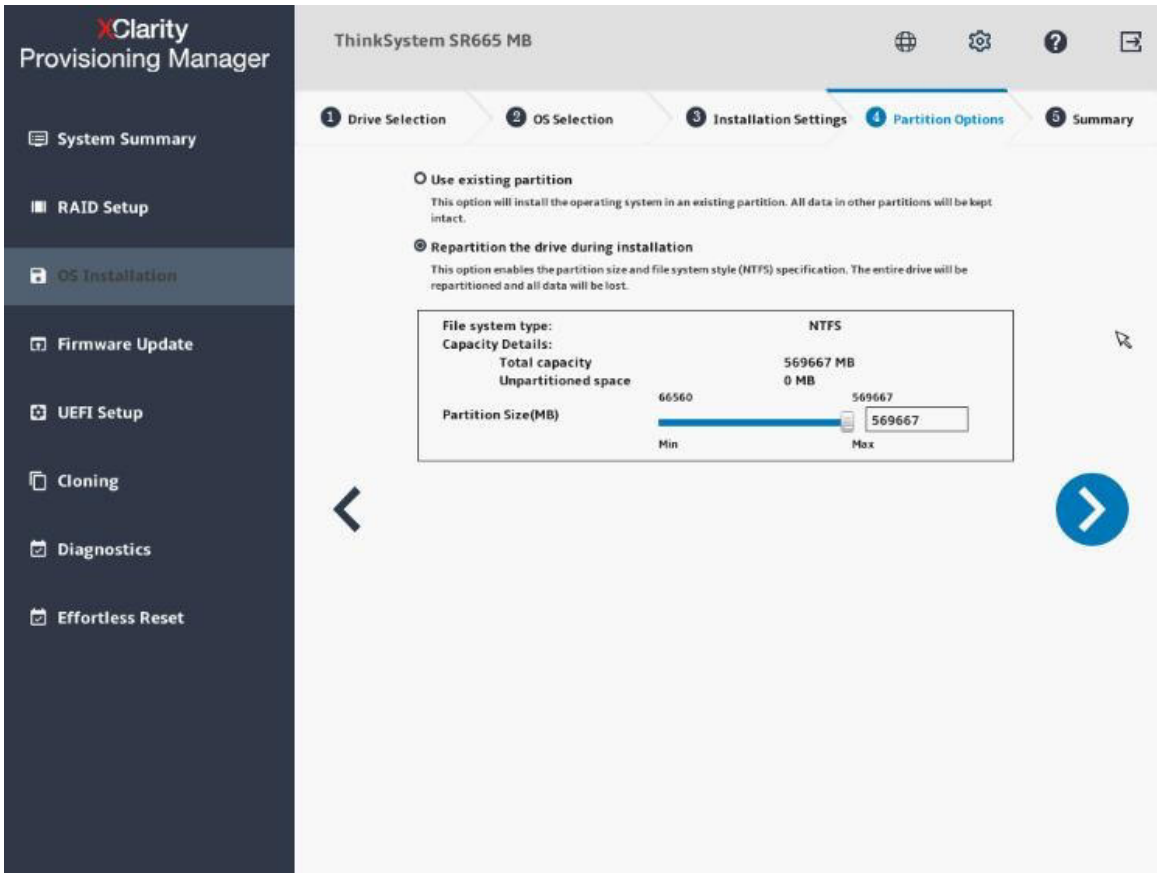


Figure 18. Partition Options step (for Windows)

If no existing partition is detected on the drive, select **Repartition the drive during installation**.

5. **Summary**

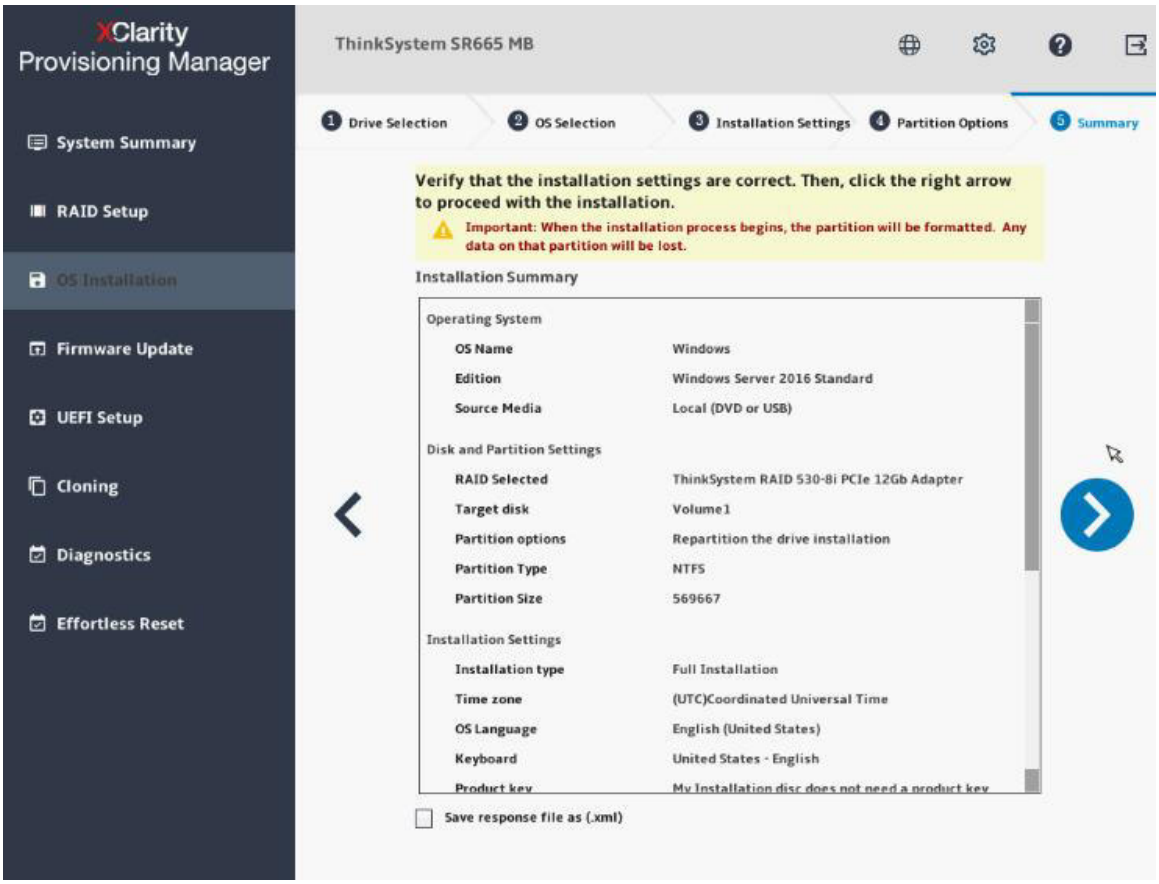


Figure 19. Summary step (for Windows)

If you want to change some settings, click < until you return to the page where you can make the changes.

If you want to export the operating system installation settings to a response file, refer to “Exporting an operating-system-installation response file” on page 40.

Click >. The license agreement page for the operating system is displayed. Read and accept the license agreement. Click **Next**. The installation process starts. Wait until the installation is completed.

Installing a Linux operating system

The wizard provides a step by step guidance for installing an operating system. Follow the instructions on the screen and the tips listed below to install a Linux operating system.

Notes:

- For the information about the operating system compatibility, refer to https://lenovopress.com/osig.
- The CentOS Linux operating systems can be installed on the server successfully. However, Lenovo servers provide only hardware-level support for CentOS.

For servers with AMD processors, if installed with SUSE Linux Enterprise Server 15.1 operating system, two image files are included: `Installer DVD` and `Packages DVD`. The image files are: `SLE-15-SP1-Installer-DVD-x86_64-GM-DVD1.iso` and `SLE-15-SP1-Packages-x86_64-GM-DVD1.iso`.

If **Core Installation** is selected, only the Installer DVD image file is required. If **Full Installation** is selected, both image files are required at the same time. To prepare two image files, you can use one of the following forms:

- Two discs (physical or virtual)
- Two USB storage drives
- One disc (physical or virtual) and one USB storage drive
- One USB storage drive including both image files

  To create a USB storage device including both image files, do the following:

  1. Prepare a USB storage drive with an FAT32 partition and a minimum of 8 GB of free storage space.
  2. Extract the Installer DVD image file to the root folder of the USB storage drive.
  3. Create a `packages` sub folder in the root folder.
  4. Extract the Package DVD image file to the `packages` sub folder.

1. **Drive Selection**

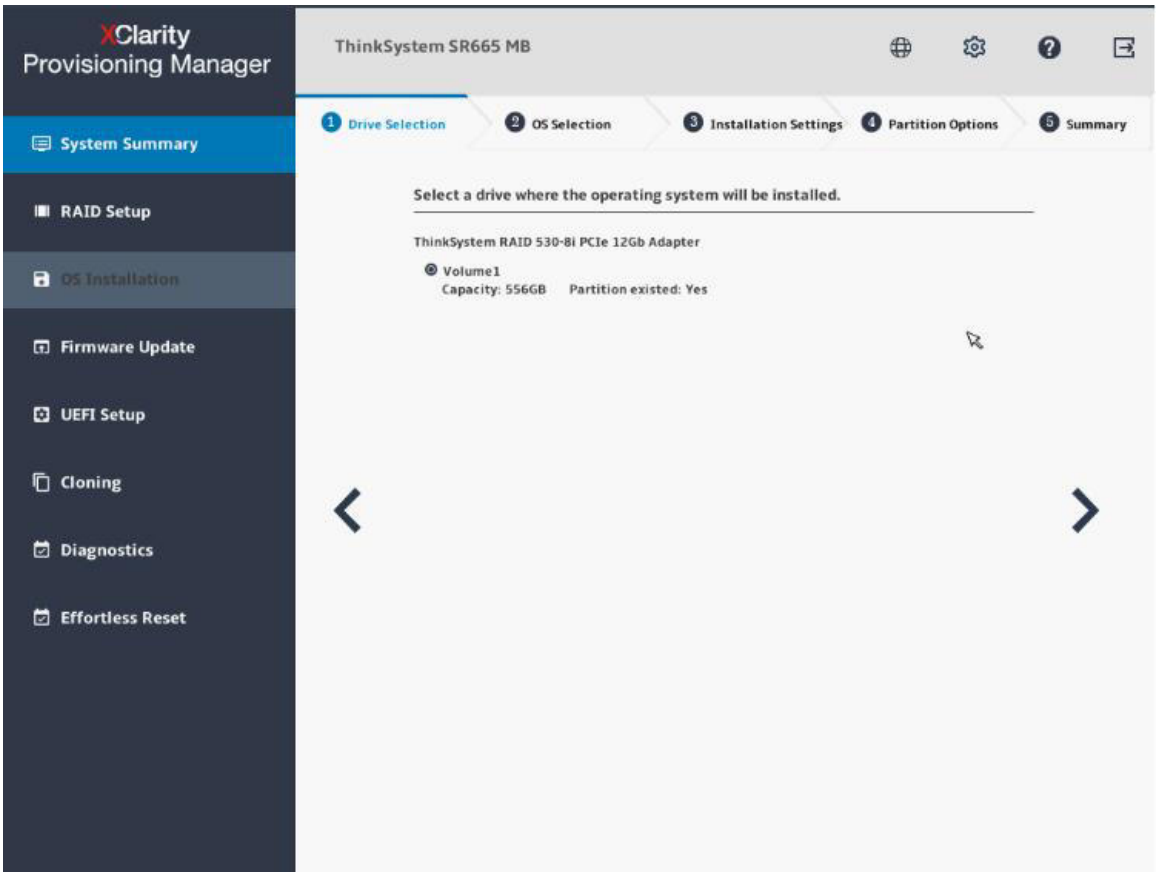


Figure 20. Drive Selection step (for Linux)

Attention: The selected drive will be formatted during the installation. Back up all data on it before the installation.

Note: The drivers will be installed automatically after the OS installation. It is recommended to restart your server to ensure that all installed drivers take effect.

2. **OS Selection**

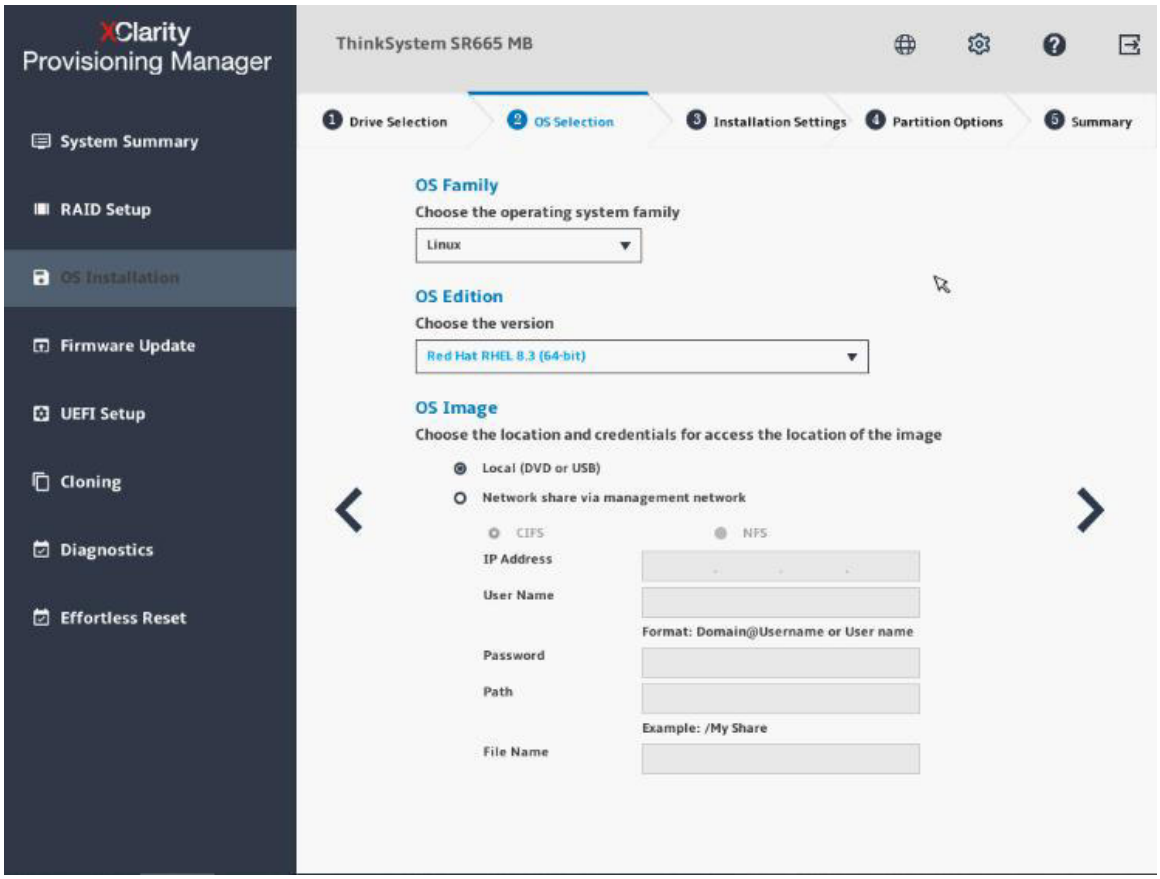


Figure 21. OS Selection step (for Linux)

The IP address is made up of four parts separated by dots. The following table lists the valid value range for each part.

IP Address	Part 1	Part 2	Part 3	Part 4
Valid values	1 – 223	0 – 255	0 – 255	0 – 255

3. **Installation Settings**

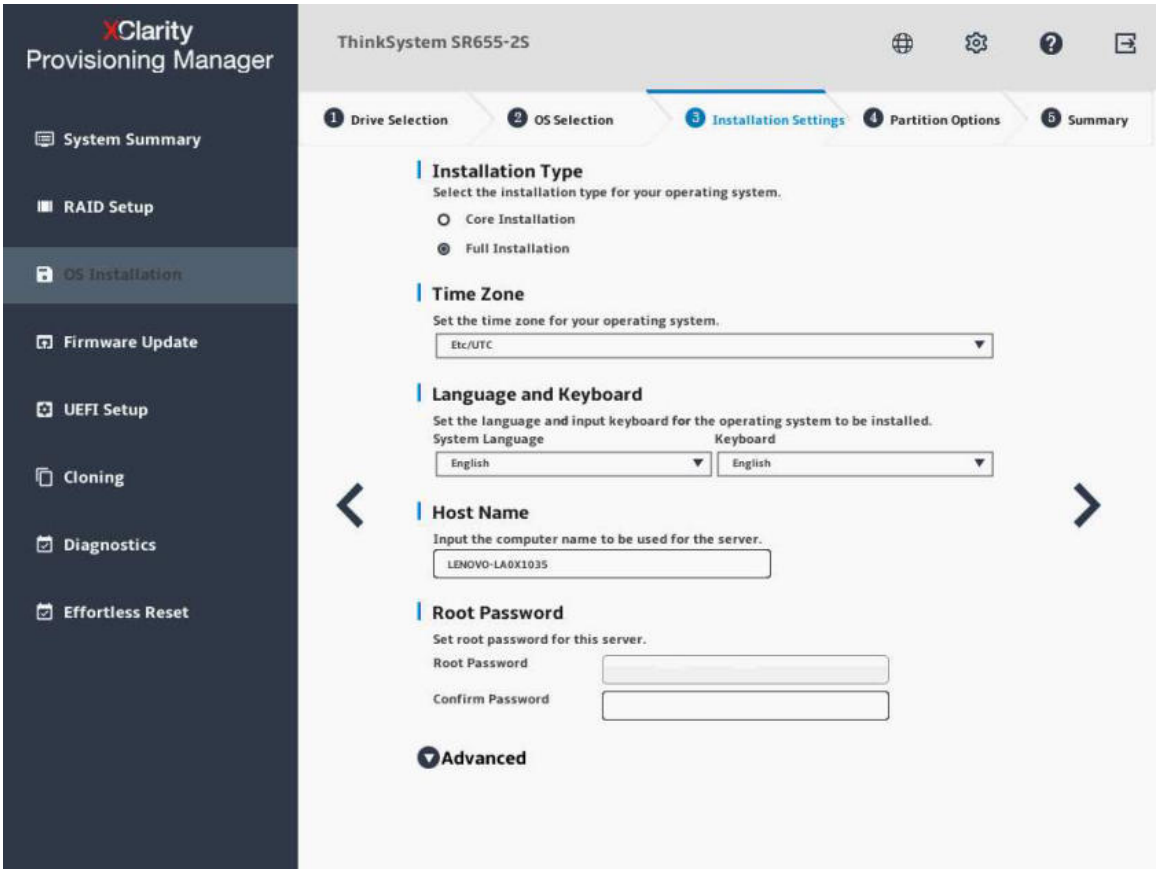


Figure 22. Installation Settings step – 1 (for Linux)

Root Password: You can change your root password later from the operating system.

If you want to do advanced configurations, expand the list by clicking the arrow icon next to **Advanced**.

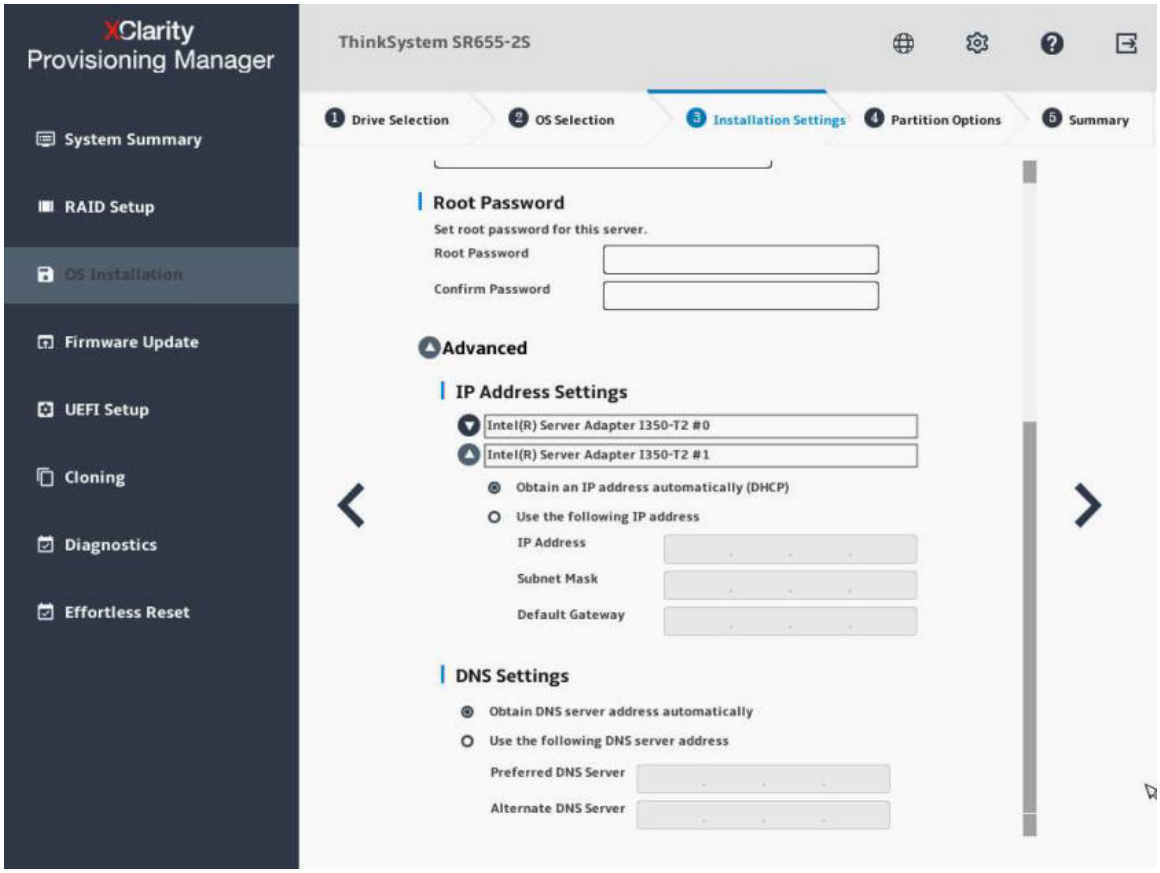


Figure 23. Installation Settings step – 2 (for Linux)

Refer to the following table for the valid values when you type the required address information.

Address	Part 1	Part 2	Part 3	Part 4
IP Address	1 – 126; 128 – 223	0 – 255	0 – 255	1 – 254
Subnet Mask	0 – 255	0 – 255	0 – 255	0 – 255
Default Gateway	0 – 255	0 – 255	0 – 255	0 – 255
Preferred DNS Server	1 – 126; 128 – 223	0 – 255	0 – 255	0 – 255
Alternate DNS Server	1 – 126; 128 – 223	0 – 255	0 – 255	0 – 255

4. **Partition Options**

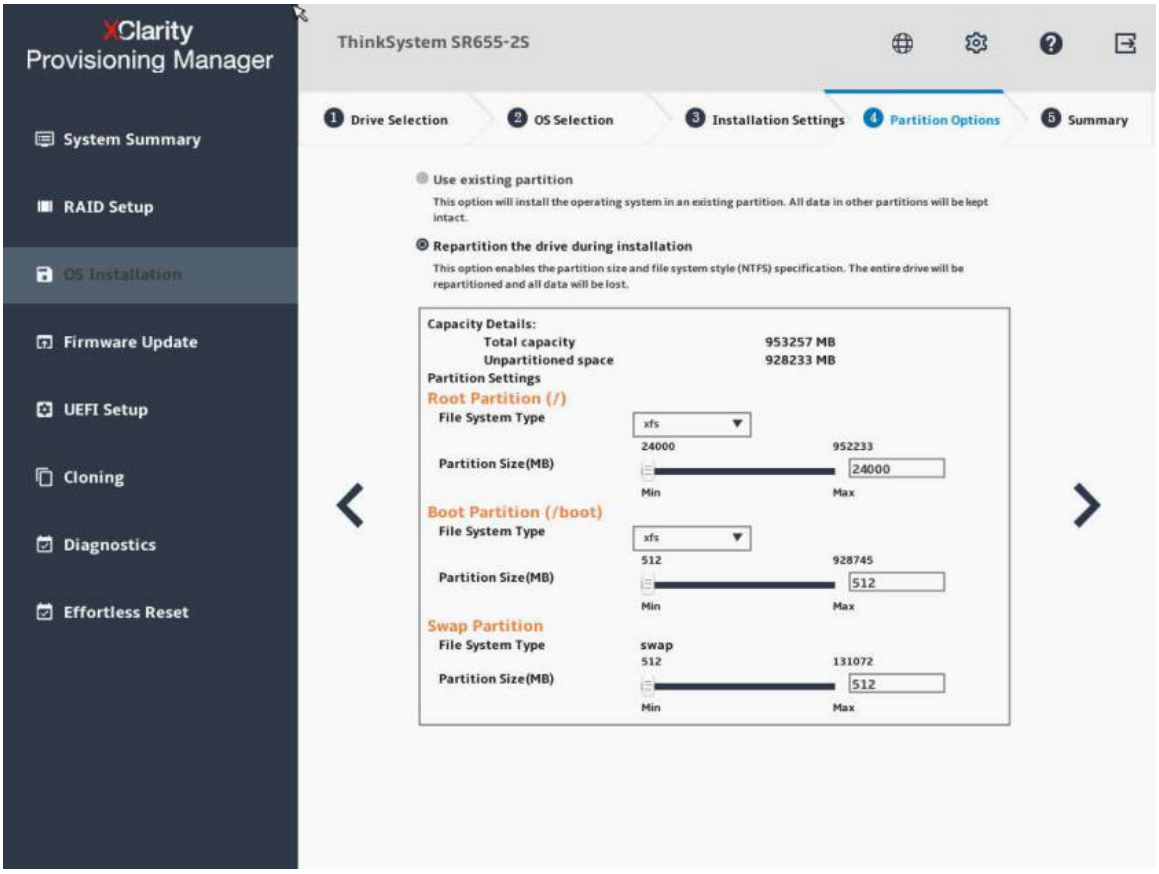


Figure 24. Partition Options step (for Linux)

If no existing partition is detected on the drive, select **Repartition the drive during installation**.

Root Partition: The root partition size depends on the space required for the operating system and applications.

Boot Partition: This partition contains files required to start the operating system.

Swap Partition: Swap partition is the virtual memory in Linux. When the Random Access Memory (RAM) is full, data will be stored on the swap partition temporarily. Although swap partition can be used to store data, it should not be considered as a replacement for RAM. It is on hard disk drives, and has slower access speed than RAM.

5. **Summary**

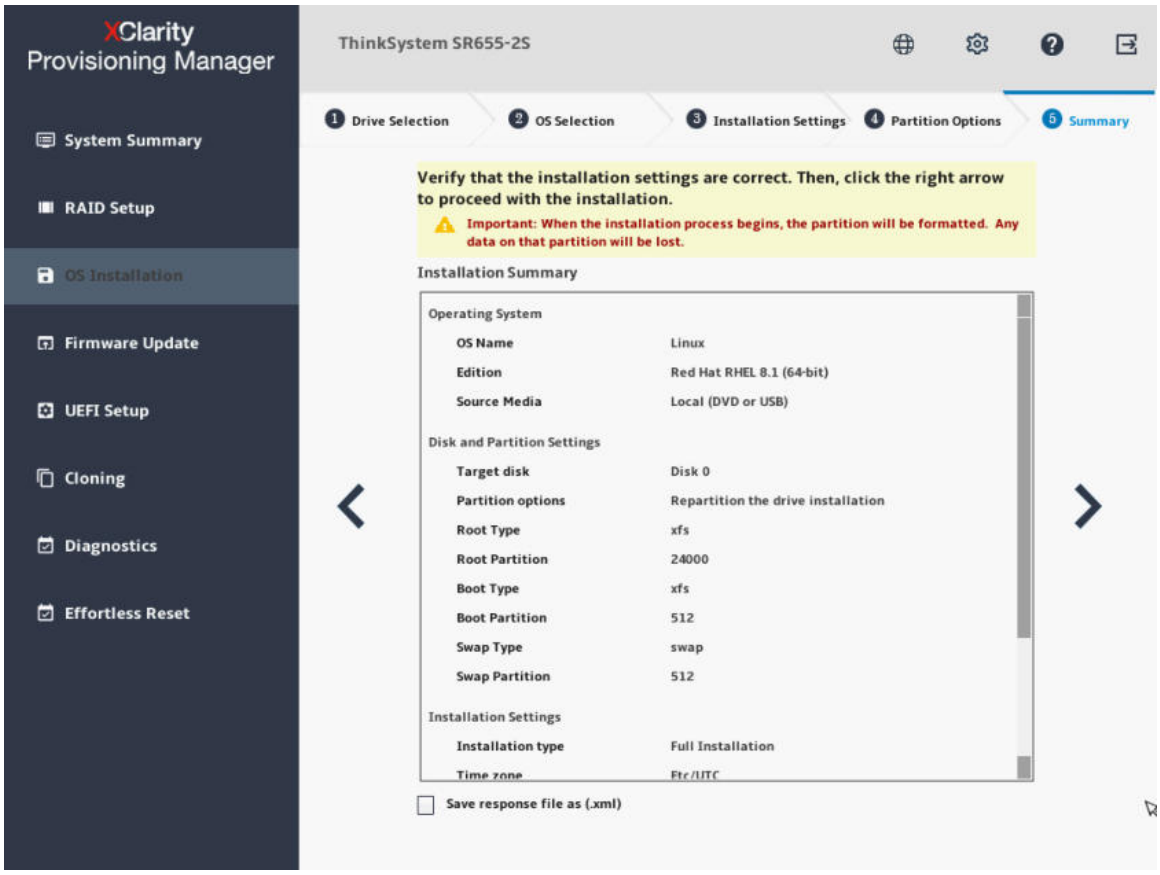


Figure 25. Summary step (for Linux)

If you want to change some settings, click  until you return to the page where you can make the changes.

If you want to export the operating system installation settings to a response file, refer to “Exporting an operating-system-installation response file” on page 40.

Click  . The installation process starts. Wait until the installation is completed.

Installing a VMware operating system

The wizard provides a step by step guidance for installing an operating system. Follow the instructions on the screen and the tips listed below to install a VMware operating system.

1. **Drive Selection**

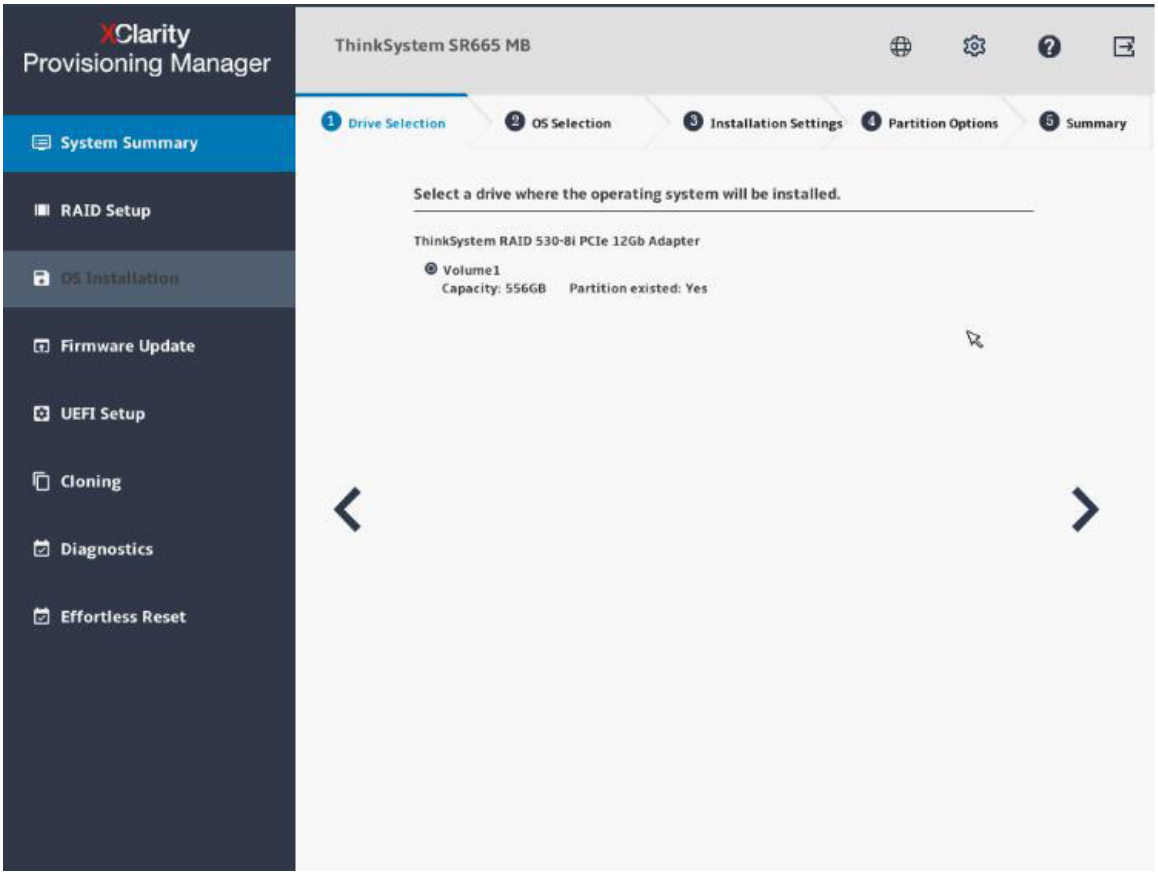


Figure 26. Drive Selection step (for VMware)

Attention: The selected drive will be formatted during the installation. Back up all data on it before the installation.

Note: The drivers will be installed automatically after the OS installation. It is recommended to restart your server to ensure that all installed drivers take effect.

2. **OS Selection**

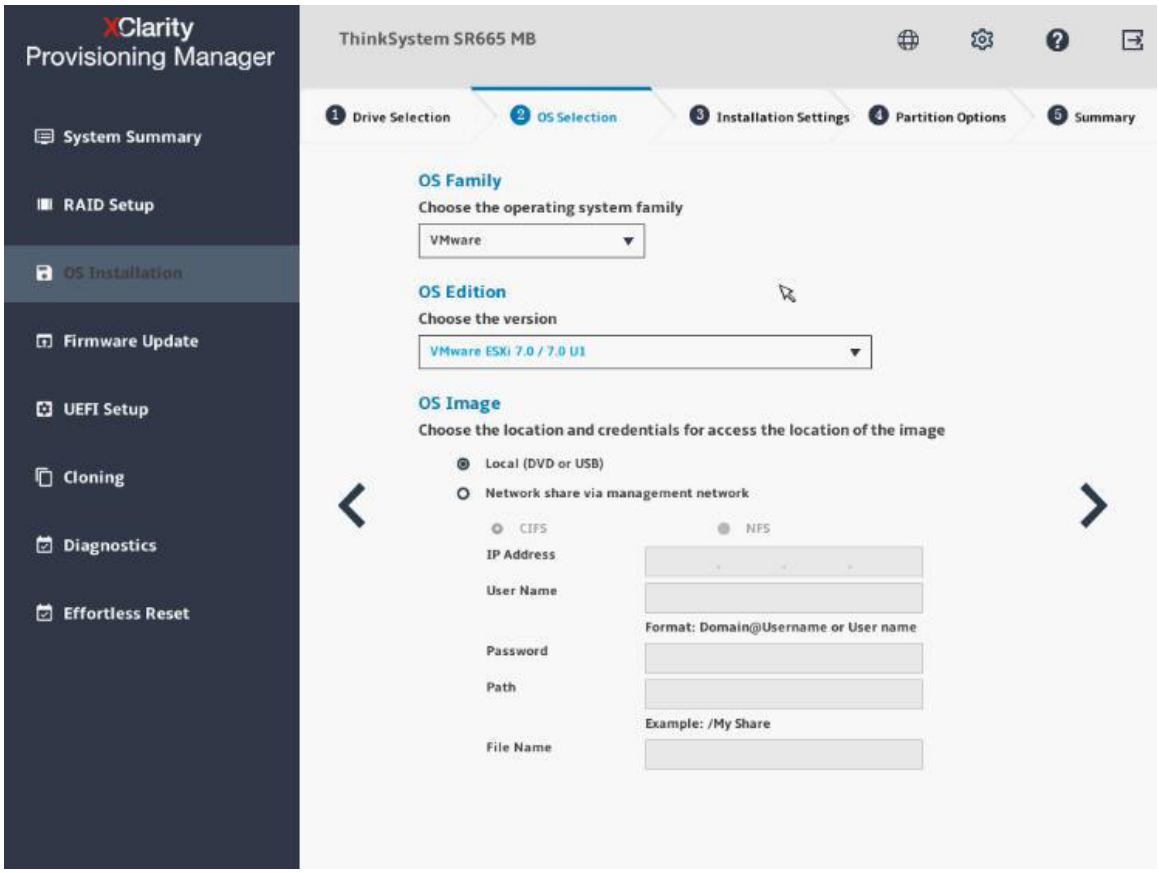


Figure 27. OS Selection step (for VMware)

The IP address is made up of four parts separated by dots. The following table lists the valid value range for each part.

IP Address	Part 1	Part 2	Part 3	Part 4
Valid values	1 – 223	0 – 255	0 – 255	0 – 255

3. **Installation Settings**

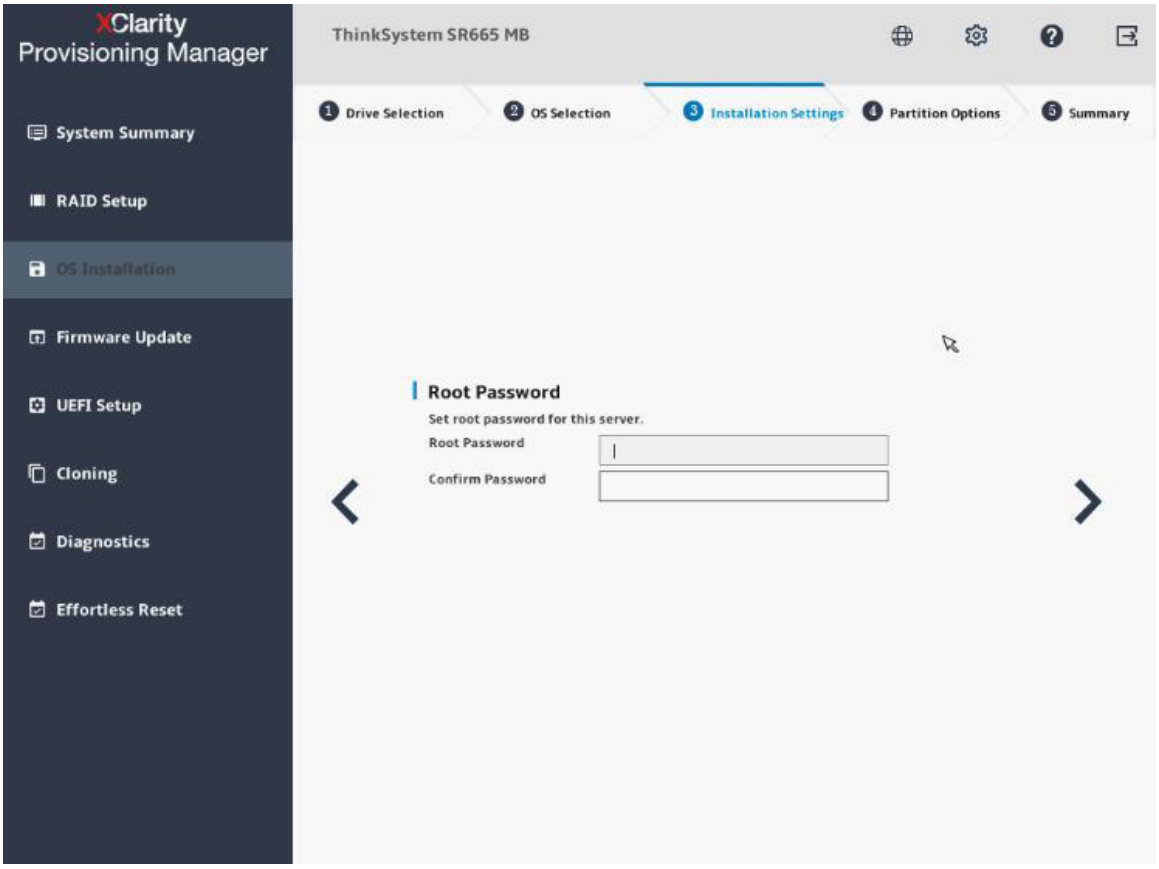


Figure 28. Installation Settings step for VMware)

Root Password: You can change your root password later from the operating system.

4. **Summary**

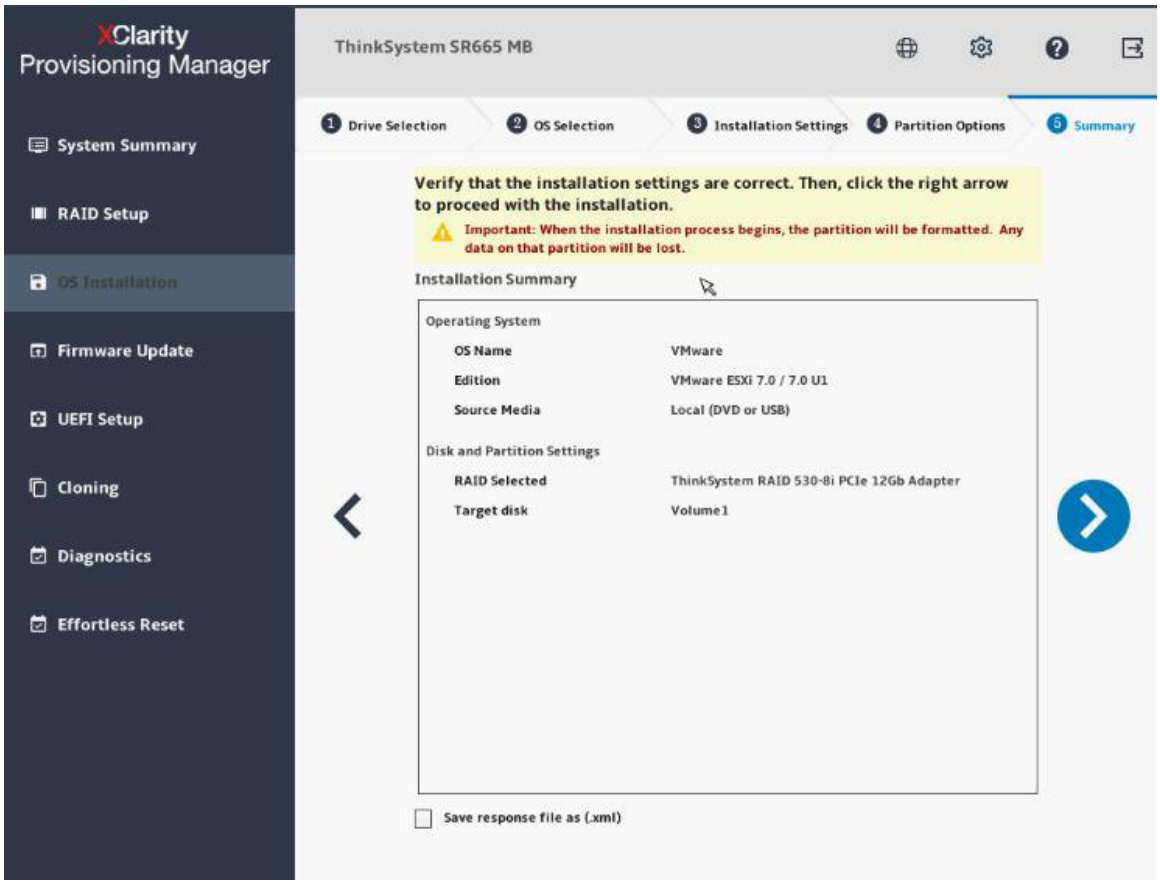


Figure 29. Summary step (for VMware)

If you want to change some settings, click < until you return to the page where you can make the changes.

If you want to export the operating system installation settings to a response file, refer to “Exporting an operating-system-installation response file” on page 40.

Click >. The installation process starts. Wait until the installation is completed.

Exporting an operating-system-installation response file

You can export the operating system installation settings to a response file. Later, you can clone the settings in this response file to other similarly configured Lenovo servers.

To export an operating-system-installation response file, do the following:

1. Attach a USB storage drive to the server or connect your server to a shared network. For instructions on how to connect to a shared network, refer to “Configuring network settings” on page 9.

   Note: The USB storage drive should include an FAT32 partition.
2. Follow the wizard to go through the Drive Selection, OS Selection, Installation Settings, Partition Options, and Summary steps.
3. In the Summary step, select the **Save response file as (.xml)** check box, and click  . The Save Response File window is displayed.
4. Select the location to save the response file and input a file name.
5. Click **Save**. Wait for several minutes until the saving process is completed.

Manual installation

Prerequisites

Before installing an operating system manually,

- Ensure that the boot mode is preset by doing one of the following:
  - Click  on the top right corner of the LXPM V3 main interface and click **Getting Started**. Set the boot mode to be **UEFI Mode**.
  - Go to **UEFI Setup → Boot Manager → Boot Modes → System Boot Mode** and select **UEFI Mode**.
- Ensure that operating system installation files are prepared in one of the following:
  - CD or DVD

    Note: Ensure that the disc is clean and the version and architecture of the operating system are correct.
  - USB storage drive

    To create a USB installation medium, refer to the documentation at: http://cn.download.lenovo.com/ibmdl/pub/pc/pccbbs/thinkservers/how_to_create_usb_os_installation_media.pdf
  - Shared network based on management network

    Note: Ensure that the Ethernet connector for system management is active and can connect to the specified IP address.

    If the shared network is connected, you can prepare the operating system installation files through Lenovo XClarity Controller.

Installing an operating system manually

In the OS Installation interface, select **Manual Install** and click . The following interface is displayed.

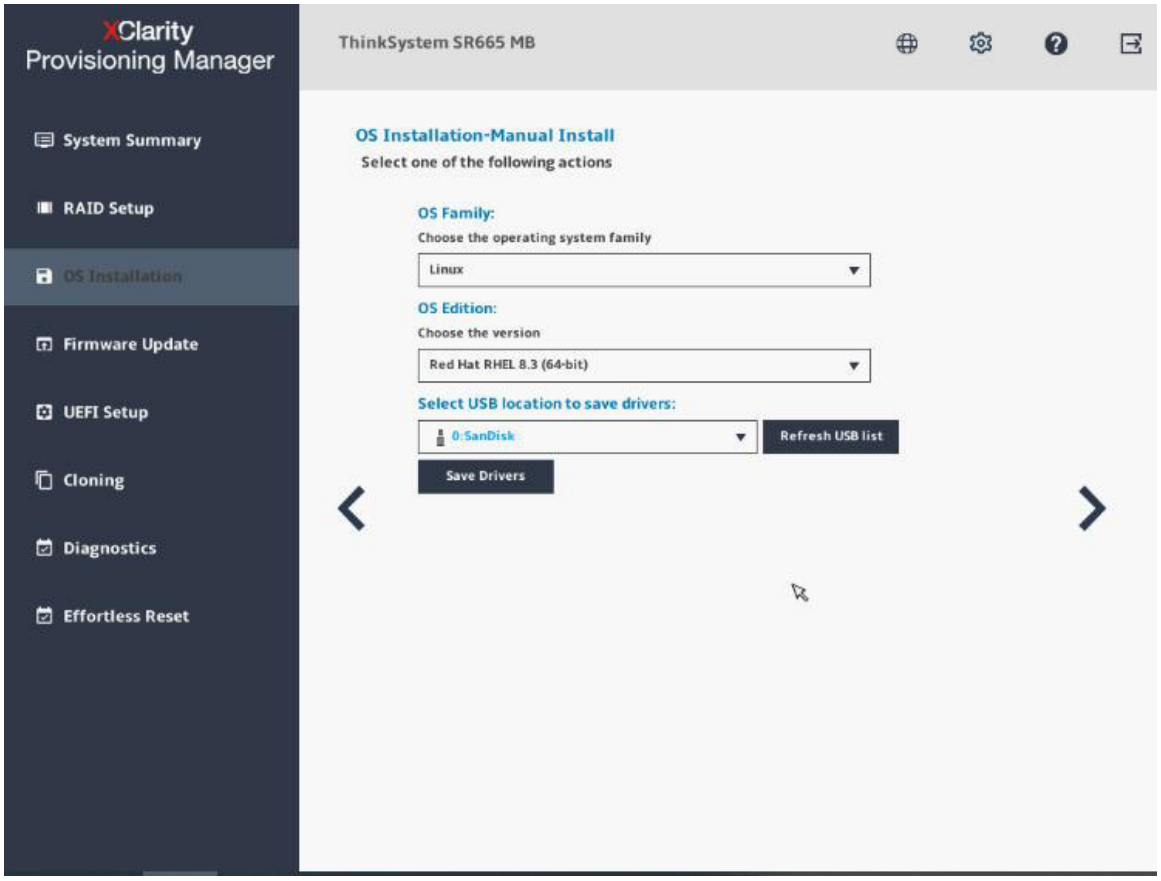


Figure 30. Manual Install interface

Do the following to install an operating system manually:

1. Select the operating system you want to install, select a location to save the drivers, and click .

   Note: If no USB storage drive is detected, the **Save Drivers** button is dimmed.

2. Select **Begin the installation** and click . The server will boot from the operating system medium and the operating system installation process starts.

   Note: You also can select **Reboot system** to restart the server if you want to do other configuration.

3. Install the operating system manually. To get instructions on how to install a specific operating system manually, do the following:
   a. Go to http://datacentersupport.lenovo.com and navigate to the support page for your server.
   b. Click **Documentation**.
   c. Select an operating system and the installation instructions will be displayed.
4. After the operating system installation process is completed, install the drivers saved in step 1 by yourself.

Firmware Update

Click the **Firmware Update** tab in the left pane to enter the Firmware Update interface. You can update the UEFI firmware, Lenovo XClarity Controller, LXPM V3, Windows drivers, and Linux drivers for your server in the Firmware Update interface. To download the update packages, go to: http://datacentersupport.lenovo.com.

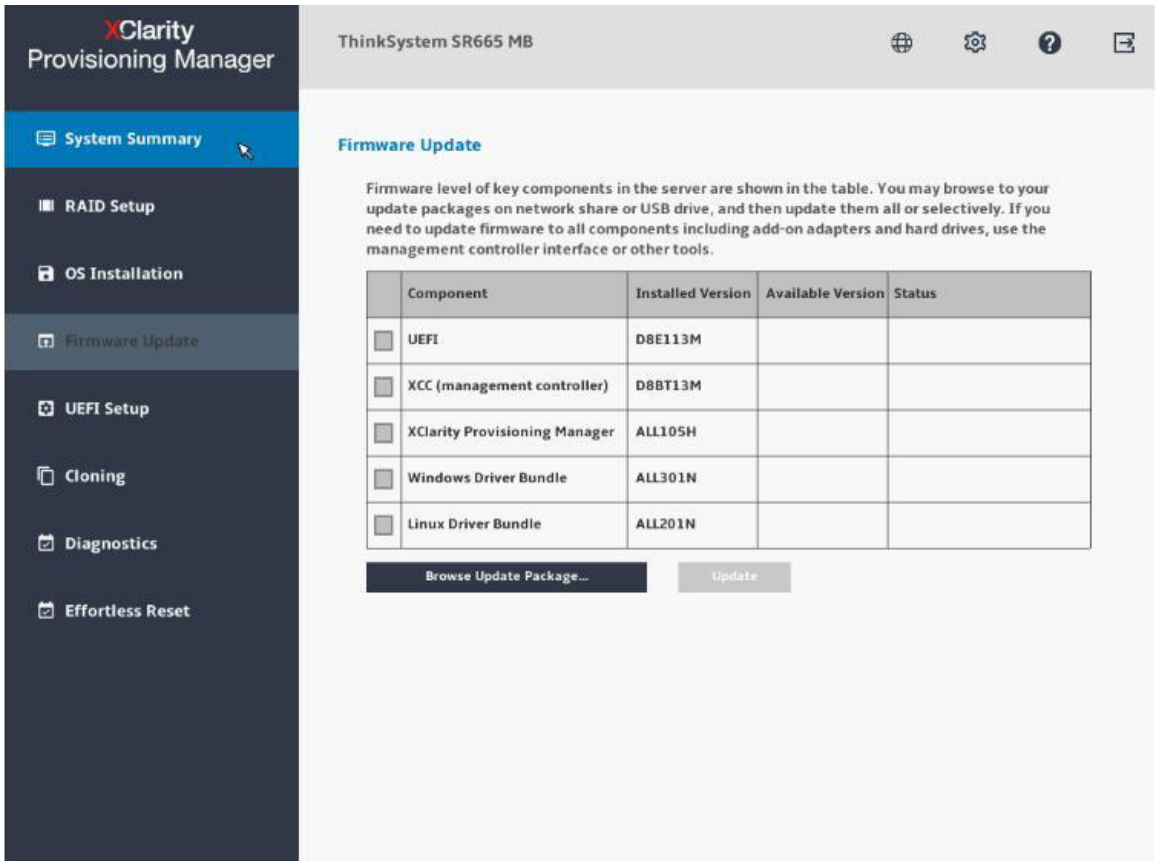


Figure 31. Firmware Update interface

To update firmware, do the following:

1. If the update package is stored on a USB storage drive, insert the USB storage drive into the server. If the update package is stored in a shared network folder, ensure that you have configured the network settings. For instructions on how to configure the network settings, refer to “Configuring network settings” on page 9.
2. Click **Browse Update Package...**. The Select File window is displayed.
3. Select the corresponding XML file in the update package and click **OK**. The check box for the item you want to update will be enabled and the version information will be displayed in the **Available Version** column.

   Notes:

   - If the available version is later than the current version, the check box will be selected automatically.
   - If the selected XML file is a bundled file with multiple items, the check boxes for those items will be enabled, and the version information for those items will be displayed in the **Available Version** column.

- If the selected XML file is not for your server, an error message will be displayed. The check box will not be enabled and the version information will not be displayed.

4. Select the items you want to update.

   Notes:

   - If the available version is earlier than or the same as the current version, a confirmation window will be displayed. Click **Yes** to continue or click **No** to exit.
   - If the XML file for the selected item is not compatible with your server, or does not meet the system configuration requirements, an error message will be displayed, and the check box will not be selected.
   - If the XML file for the selected item is not compatible with the XML files for other selected items, an error message will be displayed, and the check box will not be selected.

5. Click **Update**. The update process takes several minutes. When the **Status** for all the items are shown as **Success**, the update process is completed.

   Notes:

   - If you are updating UEFI firmware or Lenovo XClarity Controller, the server will be restarted automatically.
   - If you are updating LXPM V3, a confirmation window will be displayed. Click **Yes** to restart the server or click **No** to cancel.

UEFI Setup

Click the **UEFI Setup** tab in the left pane to enter the UEFI Setup interface. In the UEFI Setup interface, you can view and change the UEFI settings of your server.

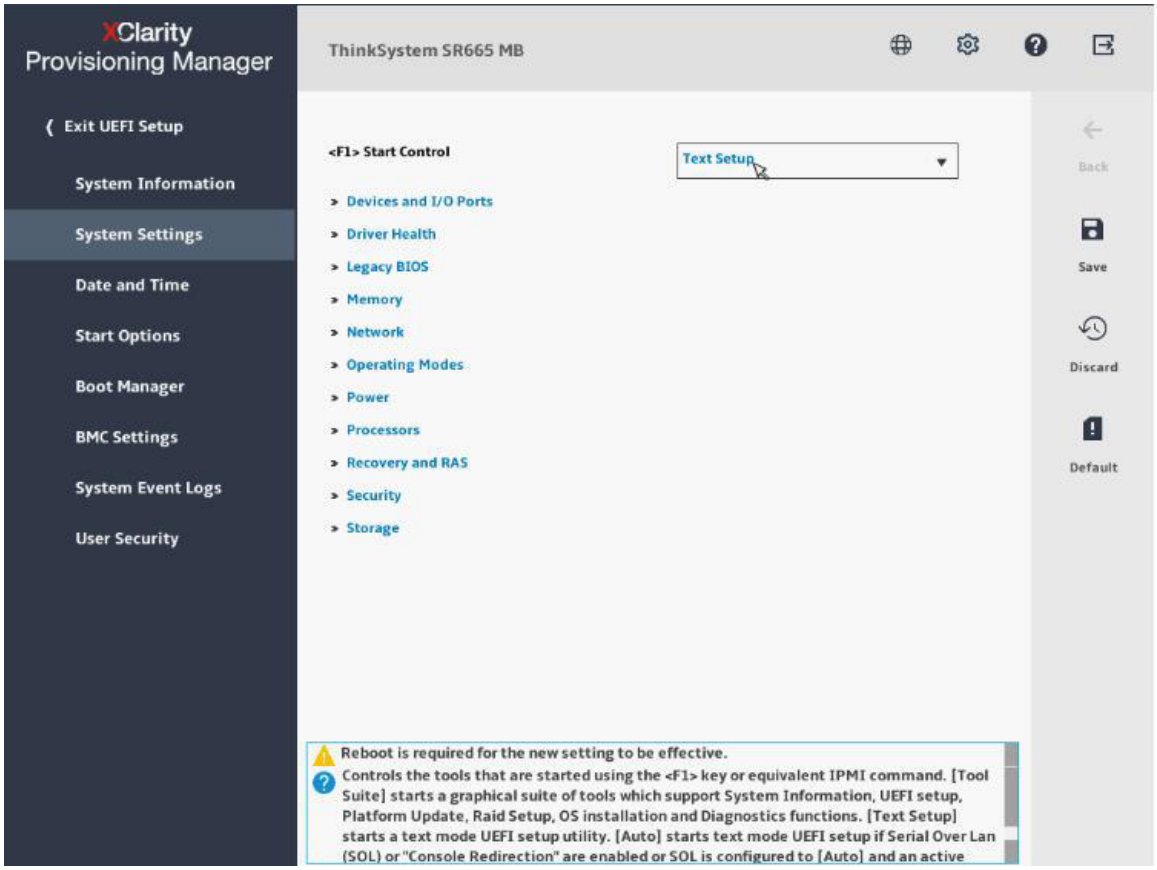


Figure 32. UEFI Setup interface

The UEFI Setup interface consists of the following subinterfaces. Click the tab in the left pane to display the corresponding subinterface in the right pane.

Note: Depending on the UEFI version of your server, some subinterface information might differ slightly from the following.

- **System Information**: View basic information about your server, such as system identification data, processor speed, DIMM information, and firmware version.
- **System Settings**: View and change various server settings.
- **Date and Time**: Set the date and time of the server.
- **Start Options**: Select an option to restart your server from it.
- **Boot Manager**: View and change the server boot options, such as the boot sequence, boot priority for various devices, and boot mode.
- **BMC Settings**: View and set BMC (Lenovo XClarity Controller) configuration parameters.
- **System Event Logs**: View and clear the system event logs.
- **User Security**: Set or modify passwords.

Note: The **Save** button, **Discard** button, and **Default** button on the right side of the interface might not be applicable for some settings, such as BMC settings and RAID adapter settings. If there are options in the setting interfaces for you to save changes, discard changes, or load default settings, you must click these options instead of using the **Save** button, **Discard** button, and **Default** button.

For detailed information, refer to the integrated help system. Click on the top right corner of an interface and click **Help** to view the help information for each interface. For more information about UFEI, refer to UEFI manual for ThinkSystem server.

Intel Optane Persistent Memory (PMEM) management

PMEMs can be managed in the UEFI Setup interface. Go to **UEFI Setup → System Settings → Intel Optane PMEMs** to configure and manage PMEMs.

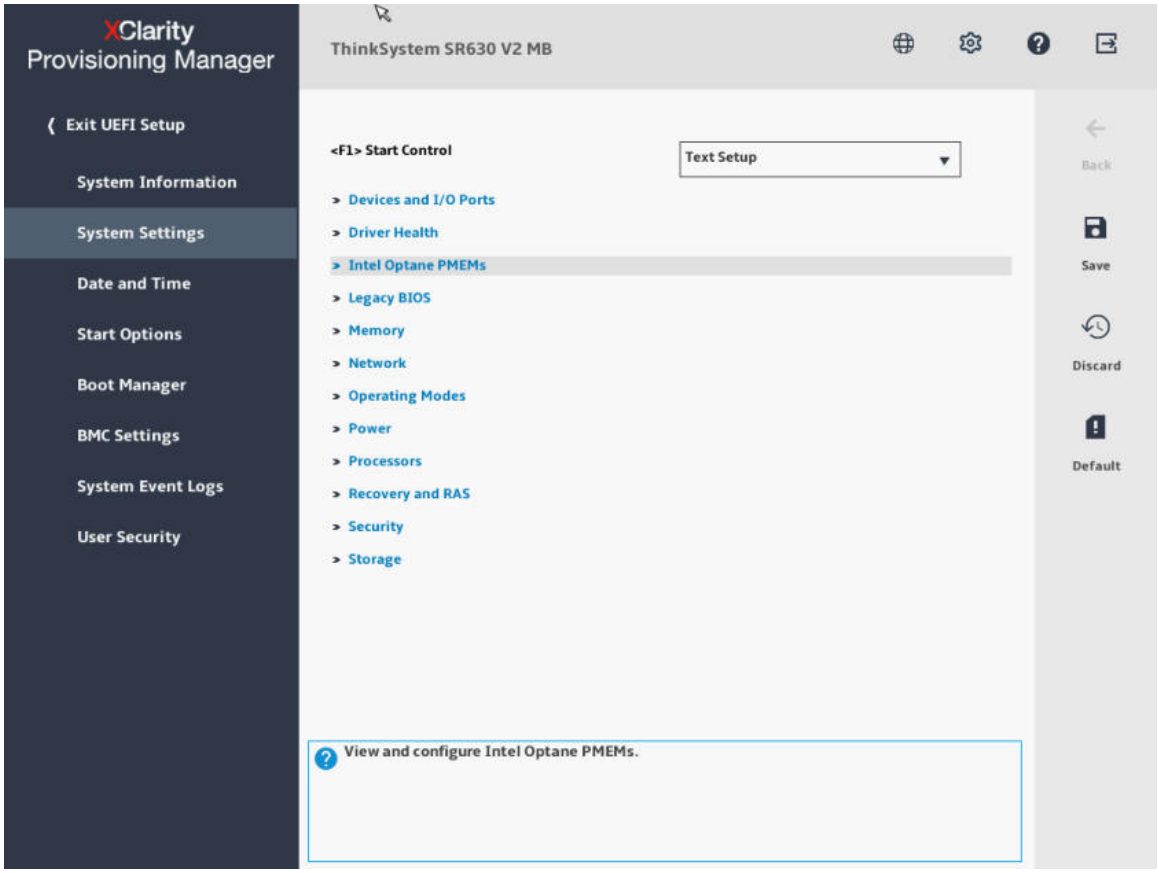


Figure 33. PMEM management

Note: If the text-based interface of Setup Utility opens instead of the Lenovo XClarity Provisioning Manager, go to **System Settings → <F1> Start Control** and select **Tool Suite**. Then, restart the system and press **F1** as soon as the logo screen appears to open Lenovo XClarity Provisioning Manager.

Following are the available management options:

- **PMEM details**

  Select this option to view the following details concerning each of the installed PMEMs:

  – Firmware version
  – Configuration status

  - Raw capacity
  - Memory capacity
  - App Direct capacity
  - Unconfigured capacity
  - Inaccessible capacity
  - Reserved capacity
  - Percentage remaining
  - Security state
  - Master Passphrase Status
- **Goals**
  - **Memory Mode [%]**

    Select this option to define the percentage of PMEM capacity that is invested in system memory, and hence decide the PMEM mode:

    - **0%:** App Direct Mode
    - **100%:** Memory Mode

    Go to **Goals → Memory Mode [%]**, select the memory percentage, 0 or 100%, and reboot the system.

    Notes:

    - Before changing from one mode to another:
      1. Make sure the capacity of installed PMEMs and DRAM DIMMs meets system requirements for the new mode.
      2. Back up all the data and delete all the created namespaces. Go to **Namespaces → View/ Modify/Delete Namespaces** to delete the created namespaces.
      3. Perform secure erase on all the installed PMEMs. Go to **Security → Press to Secure Erase** to perform secure erase.
    - After the system is rebooted and the input goal value is applied, the displayed value in **System Configuration and Boot Management → Intel Optane PMEMs → Goals** will go back to the following default selectable options:

      - **Scope:** [Platform]
      - **Memory Mode [%]:** 0
      - **Persistent Memory Type:** [App Direct]

      These values are selectable options for PMEM settings, and do not represent the current PMEM status.
  - **Persistent Memory Type**

    In App Direct Mode, the PMEMs that are connected to the same processor are by default interleaved (displayed as **App Direct**), while memory banks are used in turns. To set them as not interleaved in the Setup Utility, go to **Intel Optane PMEMs → Goals → Persistent Memory Type**, select **App Direct Not Interleaved** and reboot the system.

    Note: Setting PMEM App Direct capacity to not interleaved will turn the displayed App Direct regions from one region per processor to one region per PMEM.
- **Regions**

  After the memory percentage is set and the system is rebooted, regions for the App Direct capacity will be generated automatically. Select this option to view the App Direct regions.
- **Namespaces**

You can create, delete and view namespaces here. To create a namespace, define the name of namespace, select a Region ID and set the capacity value (GB). Then, it becomes a persistent space. To delete a namespace, select the namespace and delete it.

- **Security**
  - Enable Security

    PMEMs can be secured with passphrases. Two types of passphrase protection scope are available for PMEM:

    - **Platform:** Choose this option to run security operation on all the installed PMEM units at once. Platform passphrase is stored and automatically applied to unlock PMEMs before operating system starts running, but passphrase still has to be disabled manually for secure erase.
    - **Single PMEM:** Choose this option to run security operation on one or more selected PMEM units.

      Notes:

      - Single PMEM passphrases are not stored in the system, and security of the locked units needs to be disabled before the units are available for access or secure erase.
      - Always make sure to keep records of the slot number of locked PMEMs and corresponding passphrases. In the case the passphrases are lost or forgotten, the stored data cannot be backed up or restored, but you can contact Lenovo service for administrative secure erase.
      - After three failed unlocking attempts, the corresponding PMEMs enter “exceeded” state with a system warning message, and the PMEM unit can only be unlocked after the system is rebooted.

      To enable passphrase, go to **Security → Press to Enable Security**.
  - Secure Erase

    Note: If the PMEMs to be secure erased are protected with a passphrase, make sure to disable security and reboot the system before performing secure erase.

    Secure erase cleanses all the data that is stored in the PMEM unit, including encrypted one. This data deletion method is recommended before returning or disposing a malfunctioning unit, or changing PMEM mode. To perform secure erase, go to **Security → Press to Secure Erase**.
- **PMEM Configuration**

  PMEM contains spared internal cells to stand in for the failed ones. When the spared cells are exhausted to 0%, there will be an error message, and it is advised to back up data, collect service log, and contact Lenovo support.

  There will also be a warning message when the percentage reaches 1% and a selectable percentage (10% by default). When this message appears, it is advised to back up data and run PMEM diagnostics (see “Running diagnostics” on page 51). To adjust the selectable percentage that the warning message requires, go to **Intel Optane PMEMs → PMEM Configuration**, and input the percentage.

Cloning

Click the **Cloning** tab in the left pane to enter the Cloning interface. In the Cloning interface, you can clone settings in one server to other similarly configured Lenovo servers. The Cloning interface includes the following two sections:

- **Export**: Used to export UEFI, RAID, and BMC settings for the current server to response files respectively and save the response files to a USB storage drive or a shared network folder.
- **Import**: Used to import UEFI, RAID, BMC, and operating system installation settings from response files.

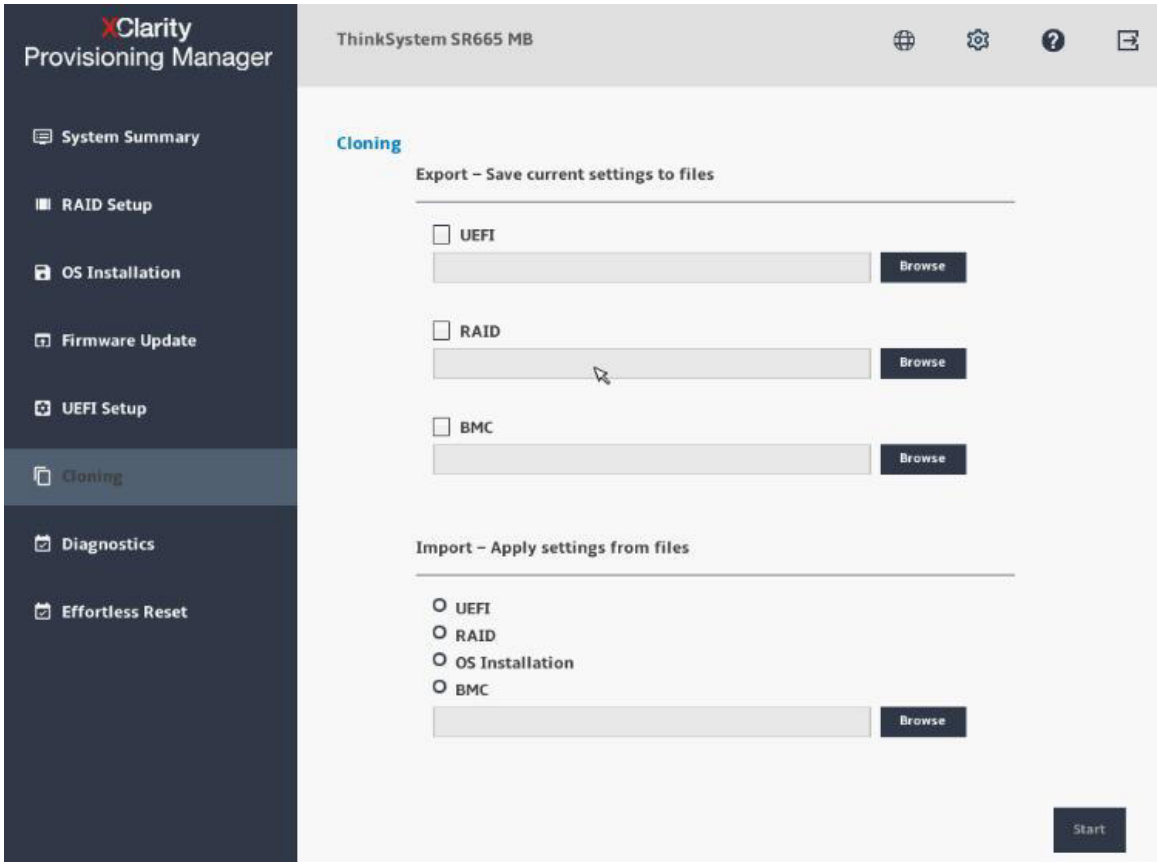


Figure 34. Cloning interface

Exporting response files

To export UEFI, RAID, or BMC settings to response files, do the following:

1. Attach a USB storage drive to the server or connect your server to a shared network. For instructions on how to connect to a shared network, refer to “Configuring network settings” on page 9.

   Note: The USB storage drive should include an FAT32 partition.
2. In the Export section, click the **Browse** button for the item you want to export. The Save Response File window is displayed.
3. Select the location to save the response file and input a file name.
4. Click **Save** to return to the Cloning interface. The check box for the item you want to export will be selected automatically.
5. If necessary, repeat step 2 to step 4 to select other items you want to export.

6. Click  or **Start** and wait for several minutes until the exporting process is completed.

To export operating system installation settings to a response file, refer to “Exporting an operating-system-installation response file” on page 40.

Importing response files

Prerequisites

- Before importing a UEFI response file, ensure that the UEFI version for the target server and the source server is the same.
- Before importing a BMC response file, ensure that the BMC version for the target server and the source server is the same.
- Before importing a RAID response file, ensure that the target server and the source server have same RAID configuration.
- Before importing an operating-system-installation response file, ensure that the target server and the source server have the same RAID adapter installed, and the capacity of the disk drive under the RAID adapter for the target server is greater than the partition size in the response file.

To import UEFI, RAID, BMC, or operating system installation settings saved in response files to your server, do the following:

1. If the response file is stored on a USB storage drive, insert the USB storage drive into the server. If the response file is stored in a shared network folder, ensure that you have configured the network settings. For instructions on how to configure the network settings, refer to “Configuring network settings” on page 9.
2. In the Import section, click the **Browse** button. The Select File window is displayed.
3. Select the corresponding response file. The selected file name is displayed in the **File Name** field.
4. Click **OK** to return to the Cloning interface. The item you want to import will be selected automatically.
5. If you are importing a UEFI, RAID, or BMC response file, click  or **Start**. The importing process starts. Wait for several minutes until the importing process is completed.

   If you are importing an operating-system-installation response file, click  , the Installation Summary page appears. The settings in the operating-system-installation response file are listed in this page. You can edit some settings according to your need. Then, click  or **Start** to start the operating system installation process. Wait until the installation is completed.

Diagnostics

Click the **Diagnostics** tab in the left pane to enter the Diagnostics interface. In the Diagnostics interface, you can run diagnostics and collect service data.

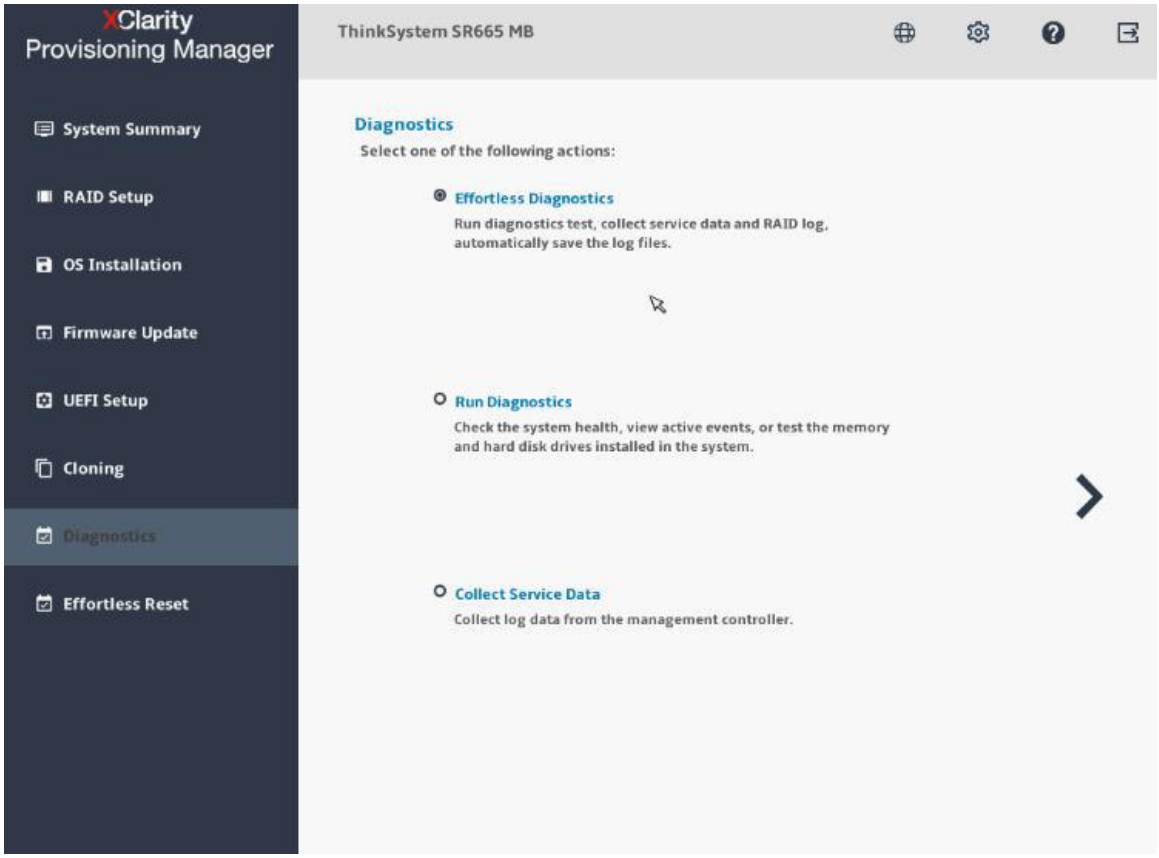


Figure 35. Diagnostics interface

There are three types of operation for your selection:

- **Effortless Diagnostic**: Run system diagnostic and collect all system log in one package.
- **Run Diagnostics**: View health status of server components, check active events, run memory test, disk drive test, and collect RAID logs.
- **Collect Service Data**: Collect service data manually.

Effortless diagnostic

To run system diagnostic and collect all system log in one package, perform effortless diagnostic.

To perform effortless diagnostic, do the following:

1. Attach a USB storage drive to the server or connect your server to a shared network. For instructions on how to connect to a shared network, refer to “Configuring network settings” on page 9.
2. In the Diagnostics interface, select **Effortless Diagnostic** and click ›. The Select device window is displayed.

3. In the Select device window, select a location to save the log and click **OK** to perform effortless diagnostic. The process takes several minutes.
4. When the diagnostics process is completed, the Confirmation window will be displayed. Click **Save Log**, then the log will be saved in the USB storage drive or the shared network. Provide the file to the Lenovo service personnel for problem determination.

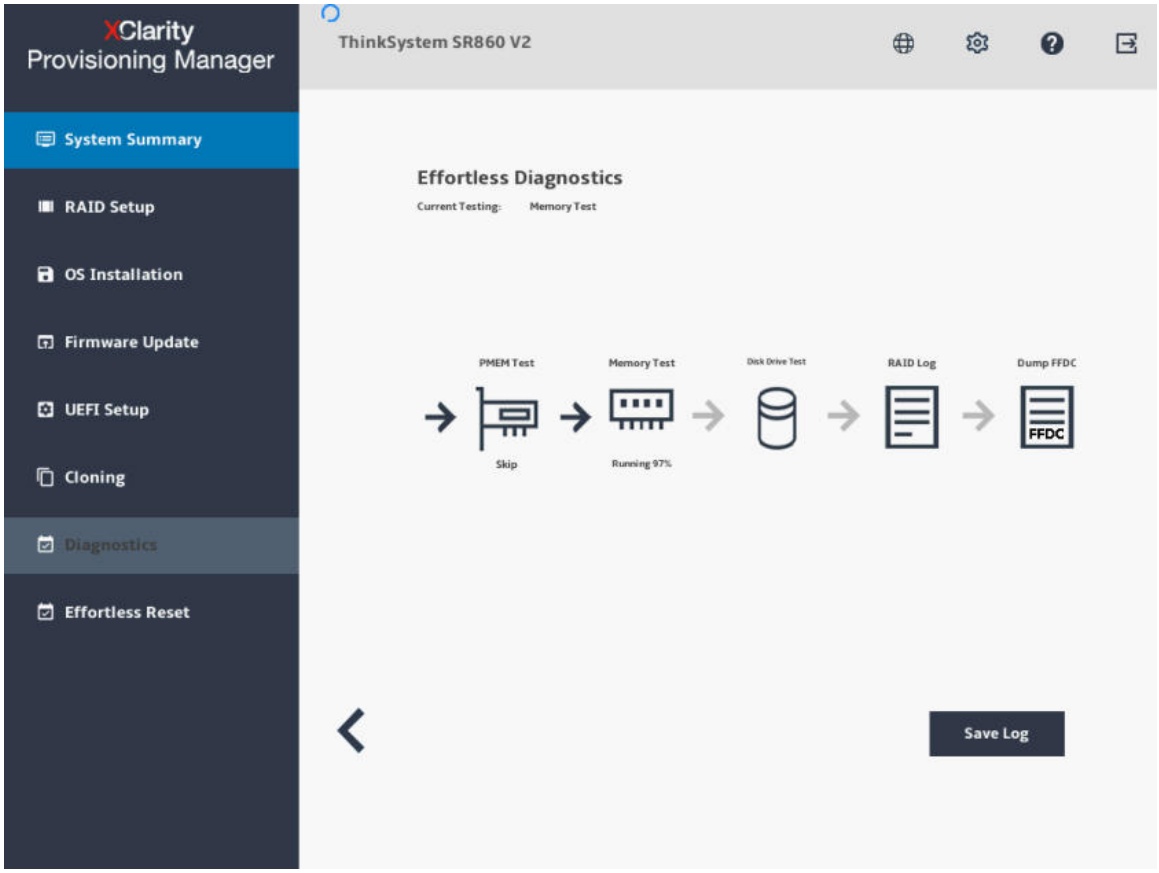


Figure 36. Effortless diagnostic

Running diagnostics

To view health status of server components, check active events, run memory test, disk drive test, and collect RAID logs, perform the “Run Diagnostics” function.

Select **Run Diagnostics** and click . The following four tabs are displayed in the left pane:

- **Dashboard**: View the health status of each server component and check the active events if any one of the components has a problem.
- **Memory Test**: Run the memory test.
- **Disk Drvie Test**: Run the disk drive test.
- **RAID Log**: Collect the logs for the selected RAID adapters.
- **PMEM Test**: Run Intel® Optane™Persistent memory test.

  Note: This item is for servers with Intel processors only.

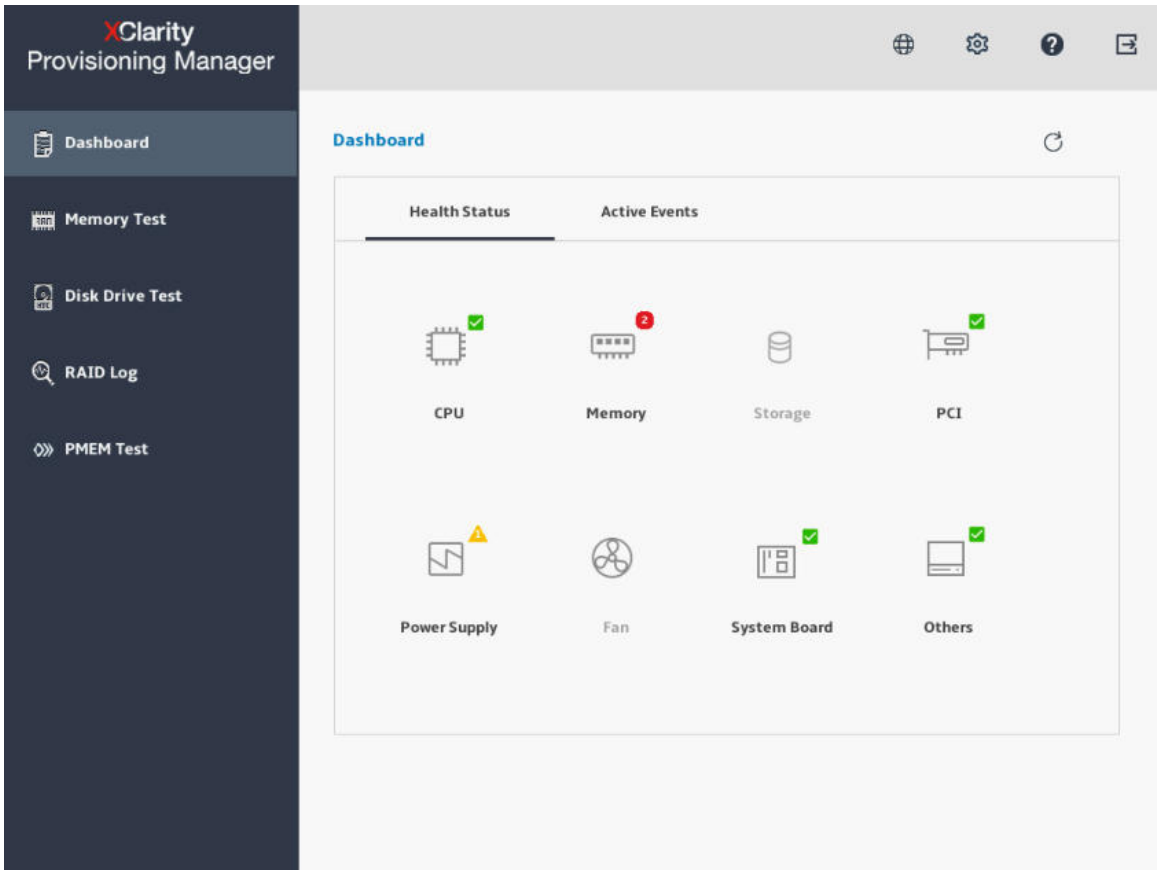


Figure 37. Dashboard interface

To exit this interface and return to the Diagnostics interface, click , and then click **OK** in the Exit window.

Running memory test

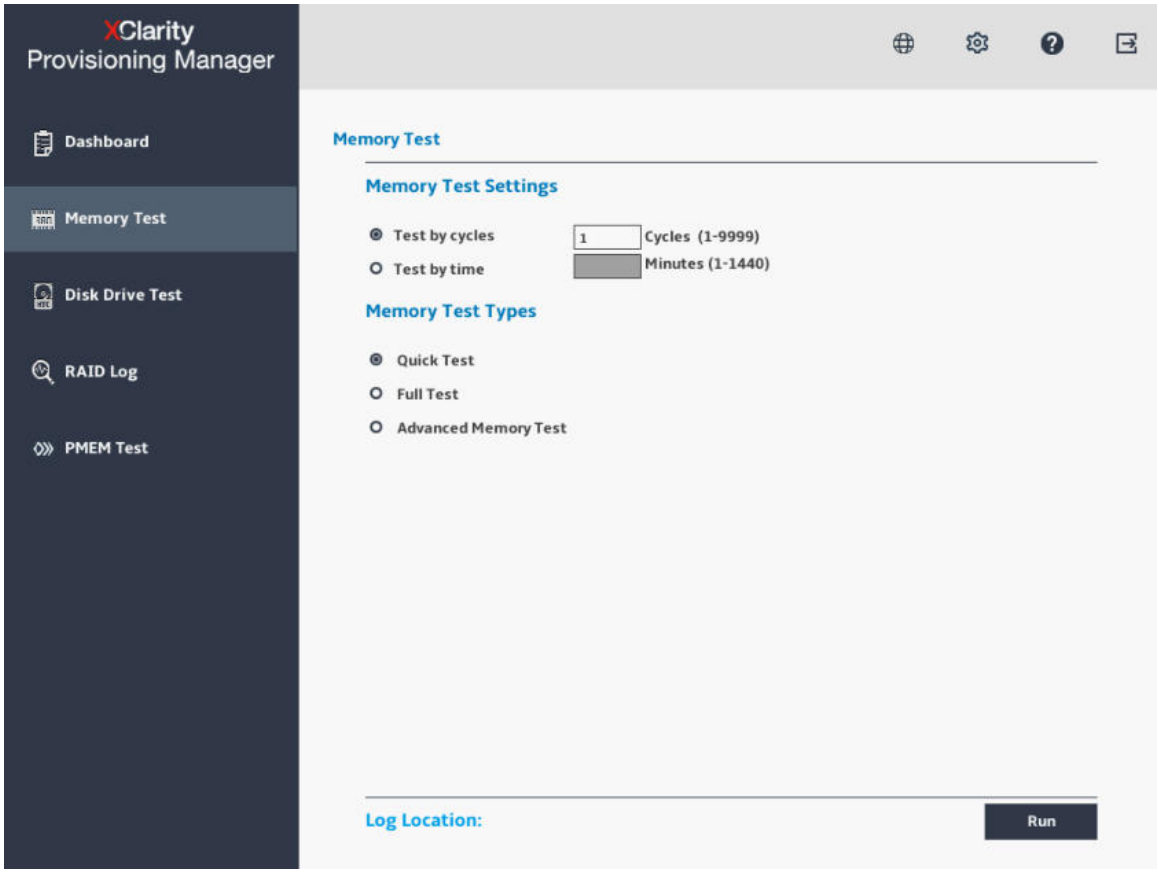


Figure 38. Memory Test interface

To run memory test, do the following:

1. If you want to save the test result, attach a USB storage drive to the server or connect your server to a shared network. For instructions on how to connect to a shared network, refer to “Configuring network settings” on page 9.
2. Click the **Memory Test** tab.

3. Select the test options based on your need, and click **Run** to start testing.

Memory Test Types	Function	Memory Test Settings	Log format	Log save location	Notes
Quick Test	**Quick Test** is selected as the default test type and it only runs the WriteRead test pattern.	Support	`test_mem_%date%.txt`	USB flash drive or website	• The mouse pointer is not active during the test process. • After the testing process is completed, the test result will be displayed to show you if the test is passed or failed. • You can press Esc to stop the test.
Full Test	**Full Test** runs all test patterns and takes a long time to finish.	Support			
Advanced Memory Test	**Advanced Memory Test** runs complicated data test patterns for memory during UEFI POST. The test time depends on the DIMM configuration. The system will be restarted when running the test, and a dialog will be displayed on the Memory Test page after the test. You can save the logs.	Not Support	`test_adv_mem_%date%.txt`	USB flash drive	/

4. Click **Save** after the testing process is completed if you want to save the test result.

   Note: The test result will be saved in a test_mem_%date%.txt file in the USB storage drive or the shared network folder. The file includes more details than the test result displayed on the interface.

Running disk drive test

To run disk drive test, do the following:

1. If you want to save the test result, attach a USB storage drive to the server or connect your server to a shared network. For instructions on how to connect to a shared network, refer to “Configuring network settings” on page 9.
2. Click the **Disk Drive Test** tab.
3. Select the test options according to your needs, and click **Run** to start testing.

   Notes:

   - **Short Self Test** is selected as the test type by default.
   - The mouse pointer is not active during the testing process.
   - If you are running test for NVMe SSDs, no matter you select **Short Self Test** or **Long Self Test**, the test item only includes the Self-Monitoring, Analysis, and Reporting Technology (SMART) flag status.
   - You can press Esc to stop the test.

4. If you want to save the test result after the testing process is completed, click **Save**.

   Notes:

   - The test result will be saved in a test_hdd.txt file in the USB storage drive or the shared network folder. The file includes more details than the test result displayed on the interface.
   - If two M.2 drives are configured as a RAID array, the drives are not supported in the disk drive test. If you want to use disk drive test function to test the M.2 drives, do not configure them as a RAID array.

5. To exit this interface and return to the Diagnostics interface, click , and then click **OK** in the Exit window.

Collecting RAID logs

To collect RAID logs, do the following:

1. If you want to save the logs, attach a USB storage drive to the server or connect your server to a shared network. For instructions on how to connect to a shared network, refer to “Configuring network settings” on page 9.
2. Click the **RAID Log** tab.
3. Select the RAID adapter that you want to collect the logs, and click **Collect RAID Log** to start the collection.

   Notes:

   - The mouse pointer is not active during the collecting process.
   - Only the Broadcom HardsWare RAID Adapter series support the log collection function. M.2/RSTe/NVMe RAID Controller does not support this function because the adapter cannot save the raid log.
4. After the collecting process is completed, the summary information for the RAID adapter will be displayed. You can click **View Recent Log** to see the recent logs of the RAID adapter.
5. If you want to save the detailed logs, click **Save Detailed Log**. The collected logs will be saved in three TXT files in the USB storage drive or the shared network folder. The three TXT files include the following information respectively:

   - Basic information about the RAID adapter
   - Firmware logs for troubleshooting
   - Event logs for the RAID adapter

   Note: You can press Esc to stop the test.
6. To exit this interface and return to the Diagnostics interface, click , and then click **OK** in the Exit window.

Running PMEM test

To run PMEM test, do the following:

1. If you want to save the test result, attach a USB storage drive to the server or connect your server to a shared network. For instructions on how to connect to a shared network, refer to “Configuring network settings” on page 9.
2. Click the **PMEM Test** tab.

   Note: The mouse pointer is not active during the testing process.
3. Select one of the following test options according to your need:

   - **Select All**: Run the following four test options.
   - **Quick diagnostics**: Verify the basic health status for installed PMEMs.
   - **Config diagnostics**: Verify whether the BIOS platform configuration matches the installed hardware or not.
   - **FW diagnostics**: Verify the firmware consistency for installed PMEMs.

     Note: This test cannot verify whether the installed firmware is the optimal version or not.
   - **Security diagnostics**: Verify the consistent security state for installed PMEMs.

     Note: It is recommended that security setting is enabled for all installed PMEMs.

4. If you want to save the test result, click **Save**after the testing process is completed.

   Note: The test result will be saved in a test_PMEM_%date%.txt file in the USB storage drive or the shared network folder. The file includes more details than the test result displayed on the interface.

Collecting service data

To collect service data manually, perform the “Collect Service Data” function.

To collect service data, do the following:

1. Attach a USB storage drive to the server or connect your server to a shared network. For instructions on how to connect to a shared network, refer to “Configuring network settings” on page 9.
2. In the Diagnostics interface, select **Collect Service Data** and click  to collect the service data. The process takes several minutes.
3. When the collecting process is completed, click  . The collected service data will be saved in a ffdc.tzz file.
4. Select a location to save the file and click **Save**. The ffdc.tzz file will be saved to the USB storage drive or the shared network. folder. Provide the file to the Lenovo service personnel for problem determination.

   Note: If the USB storage drive is not available in the list, click the refresh button to display it.

Effortless Reset

In the Effortless Reset interface, you can permanently erase all data on storage devices, clear all system logs, and reset the whole system to factory default, including credentials and networking.

Prerequisites

Before performing effortless reset, disable the security drive.

CAUTION:
Effortless reset will cause data loss, back up your data before performing effortless reset.

To perform effortless reset, do the following:

1. Click the **Effortless Reset** tab in the left pane to enter into the Effortless Reset interface.
2. Input XCC/BMC user name and password, and click **OK**.

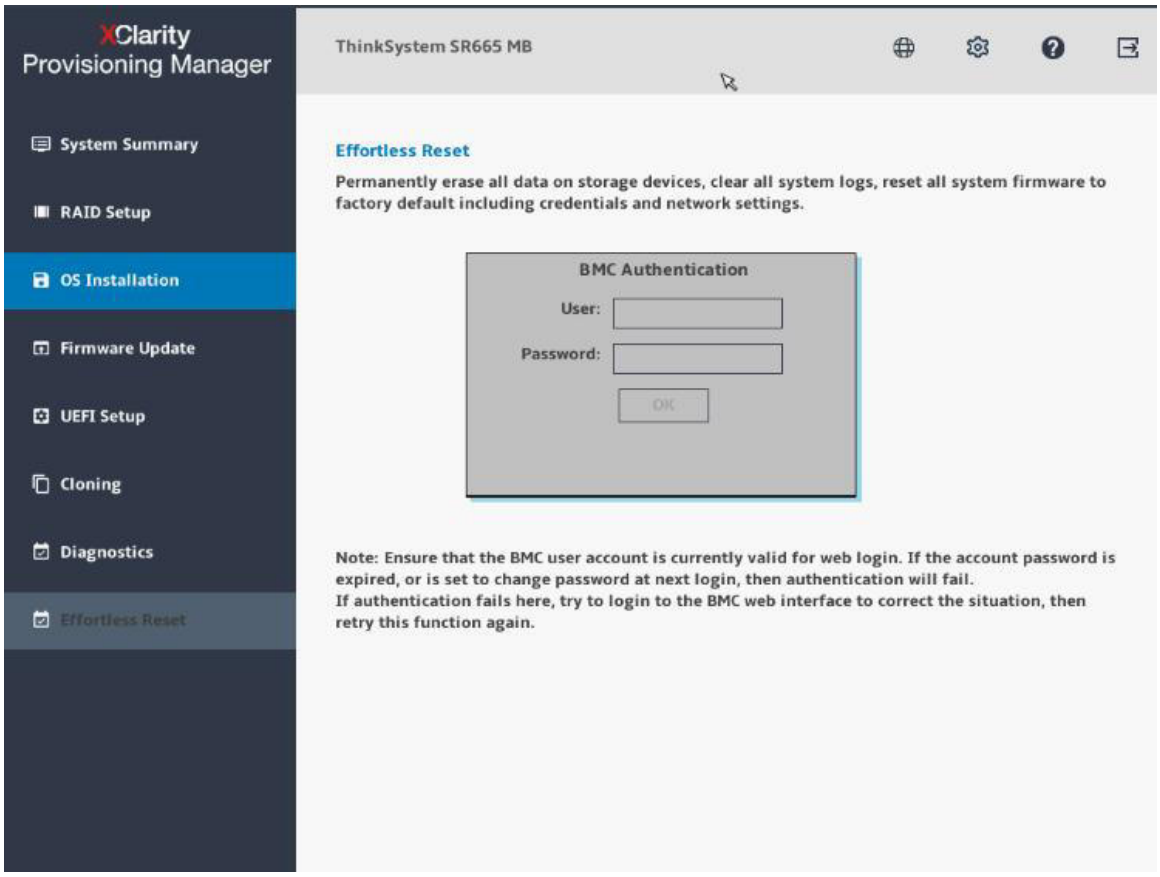


Figure 39. Input user name and password

3. Select one or more of the following based on your actual needs, input **YES** to confirm the reset action, and click **Start**.
   - To erase the data on all RAID volumes and all disk devices (including HDD, SSD, and SED), select **Permanently erase all data on storage devices**.
   - To clear the system event log (SEL), maintenance history (for servers with AMD processors only), and RAID log, select **Clear all system logs**.
   - To reset the credentials and networking of UEFI, BMC, TPM, and CMOS to factory default settings, select **Reset all system to factory default, including credentials and networking**.

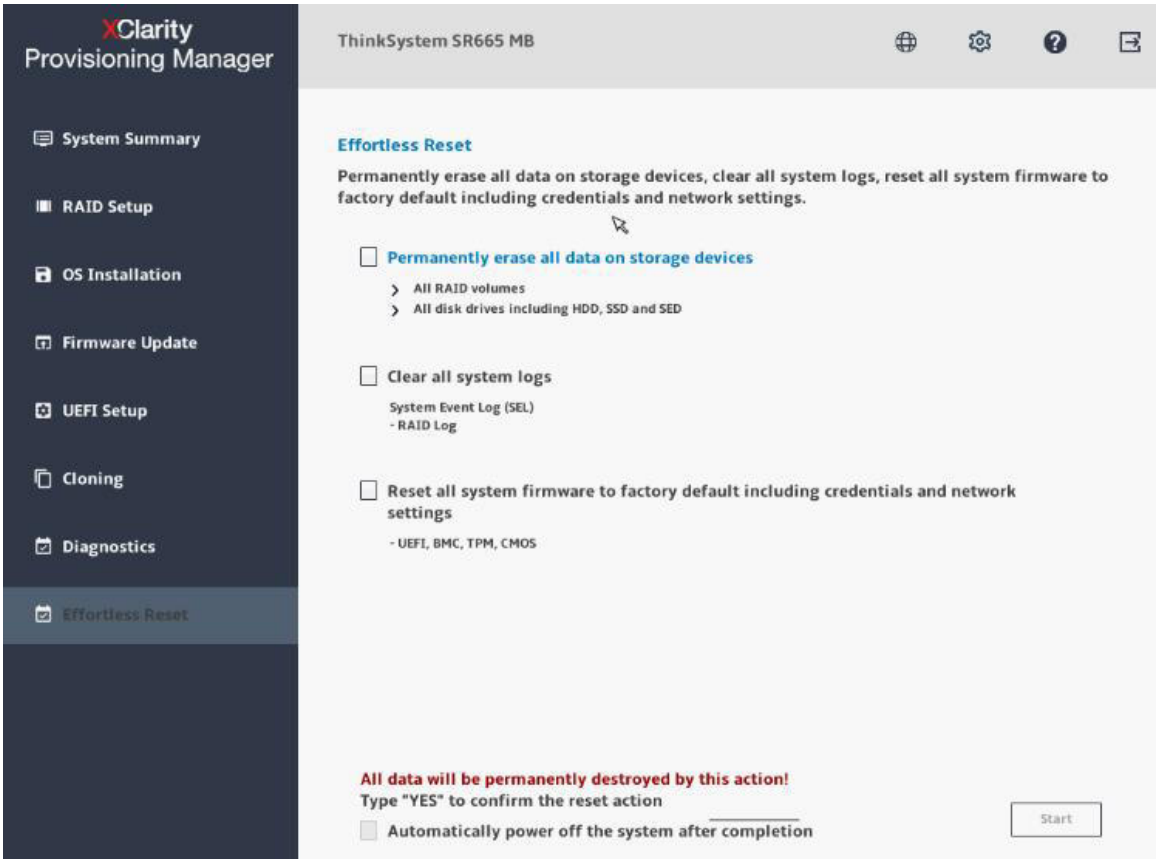


Figure 40. Select item to be deleted

4. When the following page is displayed, wait until the whole progress is completed.

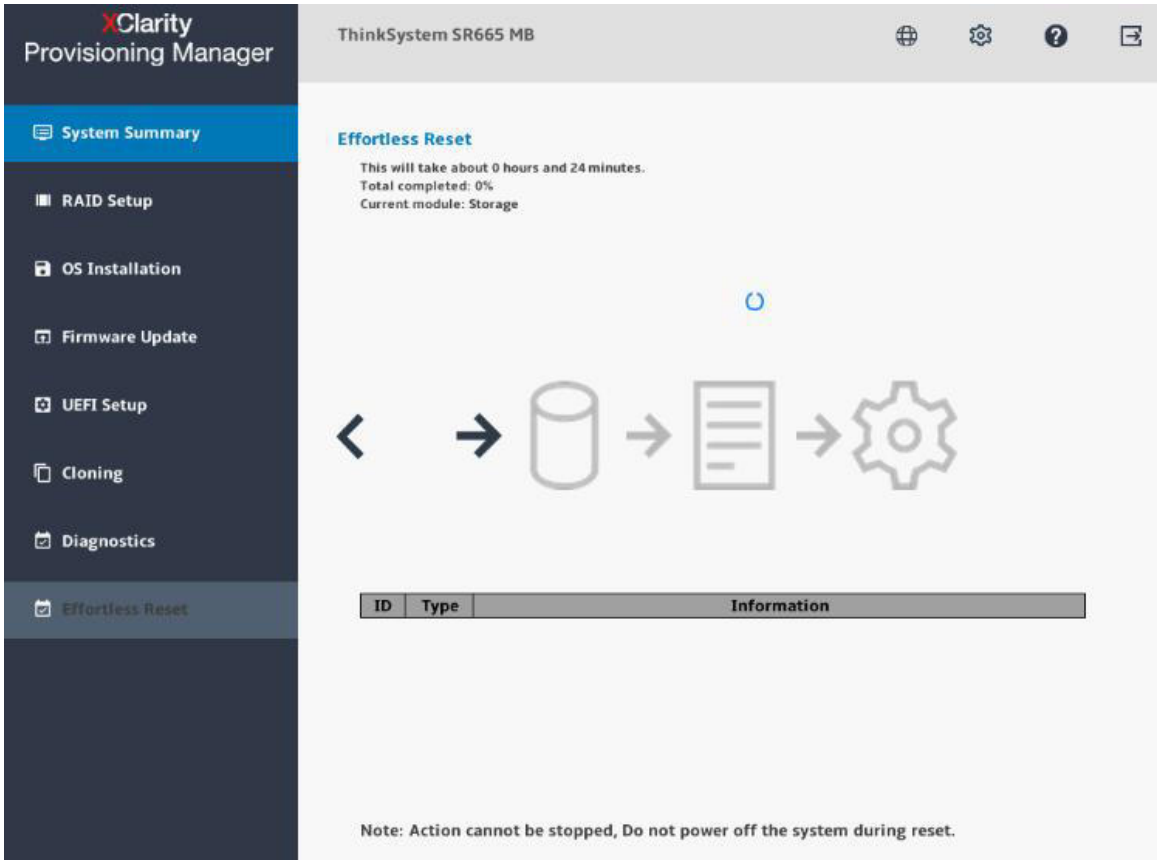


Figure 41. Effortless reset progress

Chapter 3. Troubleshooting

This chapter provides information about basic troubleshooting methods to help you solve problems that might occur while using LXPM V3.

If you cannot diagnose and solve a problem by using the information in this chapter, go to http://datacentersupport.lenovo.com for additional troubleshooting resources. You also can get help and information by telephone through the Customer Support Center. The most up-to-date telephone list for Lenovo Support is always available on the Web site at:
https://datacentersupport.lenovo.com/supportphonelist

The following table lists typical symptoms you might experience and the suggested actions.

Symptom	Action
The process for installing an operating system continuously loops.	Make more space available on the hard disk drive.
LXPM V3 cannot start the operating system medium.	Do one of the following: • Ensure that the disc has no problem. • Ensure that your server can connect to the shared network correctly. • Ensure that the USB installation medium is created correctly. Refer to: http://cn.download.lenovo.com/ibmdl/pub/pc/ pccbbs/thinkservers/how_to_create_usb_os_ installation_media.pdf
No drive is found in **OS Installation → Guided Install → Drive Selection**.	Ensure that you have configured a RAID adapter for the server in the RAID Setup interface. For instructions on how to configure a RAID adapter, refer to “RAID Setup” on page 12.

© Copyright Lenovo 2020, 2021

Appendix A. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2020, 2021

Trademarks

LENOVO, FLEX SYSTEM, SYSTEM X, and NEXTSCALE SYSTEM are trademarks of Lenovo. Intel, Optane, and Xeon are trademarks of Intel Corporation in the United States, other countries, or both. Microsoft and Windows are trademarks of the Microsoft group of companies. Linux is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners. © 2020 Lenovo.

Lenovo

ThinkSystem SR530
Maintenance Manual



Machine Types: 7X07 and 7X08

Note

Before using this information and the product it supports, be sure to read and understand the safety information and the safety instructions, which are available at:
http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html

In addition, be sure that you are familiar with the terms and conditions of the Lenovo warranty for your server, which can be found at:
http://datacentersupport.lenovo.com/warrantylookup

Tenth Edition (May 2020)

© Copyright Lenovo 2017, 2020.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Safety iii
Safety inspection checklist iv

Chapter 1. Introduction 1
Specifications 2
Firmware updates 7
Configuring the LAN over USB interface manually 10
Installing the LAN over USB Windows device driver 10
Tech Tips 11
Security advisories 11
Power on the server 11
Power off the server 11

Chapter 2. Server components 13
Front view 13
Operator information panel 15
Rear view 17
Rear view LEDs 21
System board components 23
System board switches and jumpers 25
System board LEDs 27
Internal cable routing 28
VGA connector 29
Front I/O assembly 31
RAID super capacitor module 32
Backplanes 33
Parts list 36
Power cords 39

Chapter 3. Hardware replacement procedures 41
Installation Guidelines 41
System reliability guidelines 42
Working inside the server with the power on . . 43
Handling static-sensitive devices 43
Rack latches replacement 44
Remove the rack latches 44
Install the rack latches 46
Security bezel replacement 48
Remove the security bezel 48
Install the security bezel 50
Top cover replacement 52
Remove the top cover 52
Install the top cover 54
Air baffle replacement 55
Remove the air baffle 55
Install the air baffle 57
RAID super capacitor module replacement 58
Remove a RAID super capacitor module . . . 58
Install a RAID super capacitor module 60
System fan replacement 62
Remove a system fan 62
Install a system fan 64
Front I/O assembly replacement 65
Remove the front I/O assembly 65
Install the front I/O assembly 66
Hot-swap drive backplane replacement 67
Remove the backplane for four 3.5-inch hot-swap drives 67
Install the backplane for four 3.5-inch hot-swap drives 68
Remove the backplane for eight 2.5-inch hot-swap drives 69
Install the backplane for eight 2.5-inch hot-swap drives 70
Simple-swap drive backplate assembly replacement 71
Remove the simple-swap drive backplate assembly 71
Install the simple-swap drive backplate assembly 72
Hot-swap drive replacement 73
Remove a hot-swap drive 73
Install a hot-swap drive 74
Simple-swap drive replacement 76
Remove a simple-swap drive 76
Install a simple-swap drive 78
Memory module replacement 79
Remove a memory module 79
Memory module installation rules 80
Install a memory module 85
CMOS battery replacement 87
Remove the CMOS battery 87
Install the CMOS battery 89
TCM/TPM adapter replacement (for Chinese Mainland only) 90
Remove the TCM/TPM adapter (for Chinese Mainland only) 90
Install the TCM/TPM adapter (for Chinese Mainland only) 91
Hot-swap power supply replacement 93
Remove a hot-swap power supply 93
Install a hot-swap power supply 99

© Copyright Lenovo 2017, 2020

PCIe adapter replacement 105
Remove a PCIe adapter 105
Install a PCIe adapter 106
Riser card replacement 107
Remove a riser card 107
Install a riser card 109
M.2 backplane and M.2 drive replacement 111
Remove the M.2 backplane and M.2 drive . . . 111
Adjust the retainer on the M.2 backplane . . . 113
Install the M.2 backplane and M.2 drive 114
Serial port module replacement 117
Remove the serial port module 117
Install the serial port module 119
LOM adapter replacement 121
Remove the LOM adapter 121
Install the LOM adapter 122
Processor and heat sink replacement 123
Remove a processor and heat sink 123
Install a processor and heat sink 126
System board replacement 131
Remove the system board 131
Install the system board 134
Update the Universal Unique Identifier (UUID) 135
Update the DMI/SMBIOS data 137
Enable TPM/TCM 139
Enable UEFI Secure Boot 142
Complete the parts replacement 143

Chapter 4. Problem determination 145

Event logs 145
General problem determination procedures 147
Resolving suspected power problems 147
Resolving suspected Ethernet controller problems 148
Troubleshooting by symptom 148
Power on and power off problems 149
Memory problems 150
Hard disk drive problems 151
Monitor and video problems 153
Keyboard, mouse, or USB-device problems 154
Optional-device problems 155
Serial-device problems 157
Intermittent problems 157
Power problems 158
Network problems 158
Observable problems 159
Software problems 161

Appendix A. Getting help and technical assistance 163

Before you call 163
Collecting service data 164
Contacting Support 165

Appendix B. Notices 167

Trademarks 168
Important notes 168
Particulate contamination 168
Telecommunication regulatory statement 169
Electronic emission notices 169
Taiwan BSMI RoHS declaration 170
Taiwan import and export contact information . . . 170

Index 171

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information （安全信息）。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

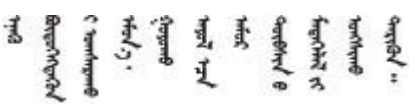
A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.



Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

© Copyright Lenovo 2017, 2020

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

ཐོན་རྫས་འདི་བདེ་སྤྱོད་མ་བྱས་གོང་། ·སྐྱོན་ཐྱི་ཡིད་གཟབ་ བྱ་འདྲ་མིན་ཡོད་པའི་འོད་སྣེར་བལྟ་དགོས།

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun.

.مەزكۇر مەھسۇلاتنى ئورنىتىشتىن بۇرۇن بىخەتەرلىك ئۇچۇرلىرىنى ئوقۇپ چىقىڭ

Youq mwngz yungh canjbinj neix gaxgonq, itdingh aeu doeg aen canjbinj soengq cungj vahgangj ancien siusik.

Safety inspection checklist

Use the information in this section to identify potentially unsafe conditions with your server. As each machine was designed and built, required safety items were installed to protect users and service technicians from injury.

CAUTION:
This equipment must be installed or serviced by trained personnel, as defined by the NEC, IEC 62368-1 & IEC 60950-1, the standard for Safety of Electronic Equipment within the Field of Audio/Video, Information Technology and Communication Technology. Lenovo assumes you are qualified in the servicing of equipment and trained in recognizing hazards energy levels in products. Access to the equipment is by the use of a tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

Important: Electrical grounding of the server is required for operator safety and correct system function. Proper grounding of the electrical outlet can be verified by a certified electrician.

Use the following checklist to verify that there are no potentially unsafe conditions:

1. Make sure that the power is off and the power cord is disconnected.
2. Check the power cord.
   - Make sure that the third-wire ground connector is in good condition. Use a meter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and the frame ground.
   - Make sure that the power cord is the correct type.

     To view the power cords that are available for the server:

     a. Go to:

        http://dcsc.lenovo.com/#/

     b. In the Customize a Model pane:

        1) Click **Select Options/Parts for a Model**.
        2) Enter the machine type and model for your server.

c. Click the Power tab to see all line cords.

- Make sure that the insulation is not frayed or worn.

3. Check for any obvious non-Lenovo alterations. Use good judgment as to the safety of any non-Lenovo alterations.
4. Check inside the server for any obvious unsafe conditions, such as metal filings, contamination, water or other liquid, or signs of fire or smoke damage.
5. Check for worn, frayed, or pinched cables.
6. Make sure that the power-supply cover fasteners (screws or rivets) have not been removed or tampered with.

© Copyright Lenovo 2017, 2020

Chapter 1. Introduction

The ThinkSystem™ SR530 is a general-purpose dual-socket 1U rack server that is great for various IT workloads, include web hosting, entry cloud, and virtualization. It is ideal for small and medium-size business (SMB) customers to run many kinds of applications by offering the latest technology to support multi-core processors, faster memory speed, flexible input/output (I/O) options and tiered system management.

The server comes with a limited warranty. For details about the warranty, see:
https://support.lenovo.com/us/en/solutions/ht503310

For details about your specific warranty, see:
http://datacentersupport.lenovo.com/warrantylookup

Identifying your server

When you contact Lenovo for help, the machine type and serial number information helps support technicians to identify your server and provide faster service.

The machine type and serial number are on the ID label on the right rack latch in the front of the server.

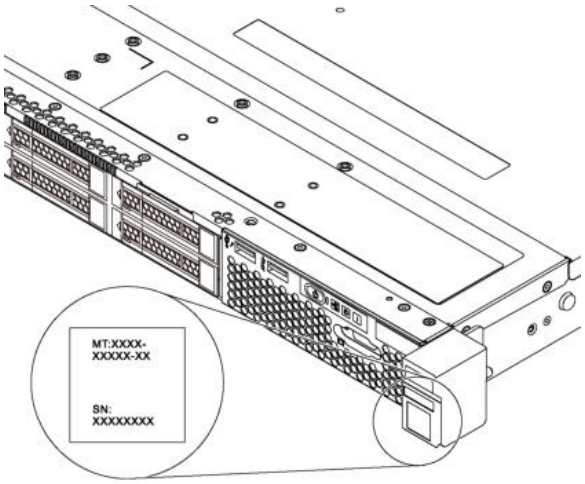


Figure 1. Location of the ID label

© Copyright Lenovo 2017, 2020

XClarity Controller network access label

The XClarity® Controller network access label is attached on the top side of the pull-out information tab. After you get the server, peel the XClarity Controller network access label away and store it in a safe place.

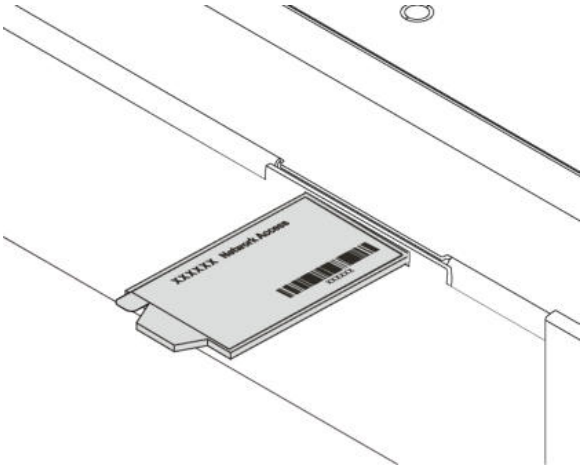


Figure 2. Location of the XClarity Controller network access label

Quick response code

The system service label, which is on the top cover, provides a quick response (QR) code for mobile access to service information. Scan the QR code with a mobile device and a QR code reader application to get quick access to the Lenovo Service web site for this server. The Lenovo Service Information Web site provides additional information for parts installation and replacement videos, and error codes for server support.

The following illustration shows the QR code: https://support.lenovo.com/p/servers/sr530



Figure 3. QR code

Specifications

The following information is a summary of the features and specifications of the server. Depending on the model, some features might not be available, or some specifications might not apply.

Table 1. Server specifications

Specification	Description
Dimension	• Form factor: 1U • Height: 43.0 mm (1.7 inches) • Width: – With rack latches: 482.0 mm (19.0 inches) – Without rack latches: 434.4 mm (17.1 inches) • Depth: 778.3 mm (30.7 inches) **Note:** The depth is measured with rack latches and power supply installed, but without security bezel installed.
Weight	Up to 16.0 kg (35.3 lb), depending on your configuration
Processor (depending on the model)	• Up to two Intel® Xeon® Scalable Processors – Designed for Land Grid Array (LGA) 3647 socket – Scalable up to 20 cores For a list of supported processors, see: http://www.lenovo.com/us/en/serverproven/
Memory	For 1st Generation Intel Xeon Scalable Processor (SP Gen 1) : • Minimum: 8 GB • Maximum: – 384 GB using registered DIMMs (RDIMMs) – 768 GB using load-reduced DIMMs (LRDIMMs) • Type (depending on the model): – TruDDR4 2666, single-rank or dual-rank, 8 GB/16 GB/32 GB RDIMMs – TruDDR4 2666, quad-rank, 64 GB LRDIMMs • Slots: 12 slots For 2nd Generation Intel Xeon Scalable Processor (SP Gen 2): • Minimum: 8 GB • Maximum: 768 GB • Type (depending on the model): – TruDDR4 2666, single-rank or dual-rank, 16 GB/32 GB RDIMMs – TruDDR4 2933, single-rank or dual-rank, 8 GB/16 GB/32 GB/64 GB RDIMMs • Slots: 12 slots **Note:** Operating speed and total memory capacity depend on the processor model and UEFI settings. For a list of supported memory, see: http://www.lenovo.com/us/en/serverproven/

Table 1. Server specifications (continued)

Specification	Description
Internal drives	Drives supported by your server vary by model. • Up to four 3.5-inch hot-swap SAS/SATA drives • Up to four 3.5-inch simple-swap SATA drives • Up to eight 2.5-inch hot-swap SAS/SATA drives • Up to two M.2 drives
PCIe slots	Depending on the server model, your server supports up to three PCIe slots. For more information about the PCIe slots, see “Rear view” on page 17.
Input/Output (I/O) features	• Front panel: – One VGA connector* – One XClarity Controller USB connector – One USB 3.0 connector • Rear panel: – One VGA connector – Two USB 3.0 connectors – Two Ethernet connectors (RJ-45) – One XClarity Controller network connector – Two Ethernet connectors on the LOM adapter* – One serial port* * Available on some models
RAID adapters (depending on the model)	• A RAID 530-8i SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 10, and 50 • A RAID 730-8i 1G Cache SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 10, and 50 • A RAID 730-8i 2G Flash SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 6, 10, 50, and 60 • A RAID 930-8i or 930-16i SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 6, 10, 50, and 60 • A RAID 930-8e SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 6, 10, 50, and 60 **Notes:** • RAID 730-8i 1G Cache SAS/SATA adapter is not available for North America. • RAID 530-8i SAS/SATA adapter cannot be mixed with RAID 730-8i 1G Cache SAS/SATA adapter. • RAID 730-8i 2G Flash SAS/SATA adapter cannot be mixed with RAID 730-8i 1G Cache SAS/SATA adapter or RAID 930- 8i SAS/SATA adapter. • A RAID super capacitor module must be installed if the RAID 930-8i or 930-16i SAS/SATA adapter, RAID 930-8e SAS/SATA adapter, or RAID 730-8i 2G Flash SAS/SATA adapter is installed.

Table 1. Server specifications (continued)

Specification	Description
System fans	• One processor: four system fans • Two processors: six system fans **Note:** If your server is installed with one processor, four system fans (fan 1 to fan 4) are adequate to provide proper cooling. However, you must keep the locations for fan 5 and fan 6 occupied by fan fillers to ensure proper airflow.
Power supplies	Up to two hot-swap power supplies for redundancy support. • 550-watt ac 80 PLUS Platinum • 750-watt ac 80 PLUS Platinum • 750-watt ac 80 PLUS Titanium
Acoustical noise emissions	• Sound power levels, idle – 4.5 bels, minimum – 4.6 bels, typical – 5.2 bels, maximum • Sound power levels, operating – 5.0 bels, minimum – 5.1 bels, typical – 5.5 bels, maximum **Notes:** • These sound power levels are measured in controlled acoustical environments according to procedures specified by ISO 7779 and are reported in accordance with ISO 9296. • The declared acoustic noise levels are based on specified configurations, which may change slightly depending on configuration/conditions.
Electrical input	• Sine-wave input (50–60 Hz) required • Input voltage low range – Minimum: 100 V ac – Maximum: 127 V ac • Input voltage high range: – Minimum: 200 V ac – Maximum: 240 V ac **Note:** For server models with 750-watt ac 80 PLUS Titanium power supplies, the 100–127 V ac input voltage is not supported. **CAUTION:** • **240 V dc input (input range: 180-300 V dc) is supported in Chinese Mainland ONLY. Power supply with 240 V dc input cannot support hot plugging power cord function. Before removing the power supply with dc input, please turn off server or disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the power cord.** • **In order for the ThinkSystem products to operate error free in both a DC or AC electrical environment, a TN-S earthing system which complies to 60364-1 IEC 2005 standard has to be present or installed.**

Table 1. Server specifications (continued)

Specification	Description
Minimal configuration for debugging	• One processor in processor socket 1 • One DIMM in slot 3 • One power supply • One HDD or M.2 (If OS installation is needed for debugging) • Four system fans (fan 1 to fan 4)
Environment	The server is supported in the following environment: • Air temperature: – Operating: – ASHRAE class A2: 10–35°C (50–95°F); when the altitude exceeds 900 m (2953 ft), the maximum ambient temperature value decreases by 1°C (1.8°F) with every 300 m (984 ft) of altitude increase. – ASHRAE class A3: 5–40°C (41–104°F); when the altitude exceeds 900 m (2953 ft), the maximum ambient temperature value decreases by 1°C (1.8°F) with every 175 m (574 ft) of altitude increase. – ASHRAE class A4: 5–45°C (41–113°F); when the altitude exceeds 900 m (2953 ft), the maximum ambient temperature value decreases by 1°C (1.8°F) with every 125 m (410 ft) of altitude increase. – Server off: 5–45°C (41–113°F) – Shipping or storage: -40–60°C (-40–140°F) • Maximum altitude: 3050 m (10 000 ft) • Relative humidity (non-condensing): – Operating: – ASHRAE class A2: 8%–80%; maximum dew point: 21°C (70°F) – ASHRAE class A3: 8%–85%; maximum dew point: 24°C (75°F) – ASHRAE class A4: 8%–90%; maximum dew point: 24°C (75°F) – Shipping or storage: 8%–90% • Particulate contamination **Attention:** Airborne particulates and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the server. For information about the limits for particulates and gases, see “Particulate contamination” on page 168. **Notes:** Your server complies with ASHRAE class A2 specifications. The server performance might be impacted when the operating temperature is outside the ASHRAE A2 specifications. Depending on the hardware configuration, some server models comply with ASHRAE class A3 and class A4 specifications. To comply with ASHRAE class A3 and class A4 specifications, the server models must meet the following hardware configuration requirements at the same time: • Two power supplies must be installed. • No system fan fails.

Important information about EU ecodesign requirements

To meet the EU ecodesign requirements for energy-related products (ErP) Lot 9, your server must meet the following requirements:

- Minimum memory: 16 GB
- For server configured with one processor, these processors are not supported: Intel Xeon 3104, 3106, 3204, 4108, 4109T, 4110, 4112, 5122, 5222, 8156, and 8256.

Firmware updates

Several options are available to update the firmware for the server.

You can use the tools listed here to update the most current firmware for your server and the devices that are installed in the server.

Note: Lenovo typically releases firmware in bundles called UpdateXpress System Packs (UXSPs). To ensure that all of the firmware updates are compatible, you should update all firmware at the same time. If you are updating firmware for both the Lenovo XClarity Controller and UEFI, update the firmware for Lenovo XClarity Controller first.

Best practices related to updating firmware is available at the following location:

http://lenovopress.com/LP0656

Important terminology

- **In-band update**. The installation or update is performed using a tool or application within an operating system that is executing on the server's core CPU.
- **Out-of-band update**. The installation or update is performed by the Lenovo XClarity Controller collecting the update and then directing the update to the target subsystem or device. Out-of-band updates have no dependency on an operating system executing on the core CPU. However, most out-of-band operations do require the server to be in the S0 (Working) power state.
- **On-Target update.** The installation or update is initiated from an Operating System executing on the server's operating system.
- **Off-Target update.** The installation or update is initiated from a computing device interacting directly with the server's Lenovo XClarity Controller.
- **UpdateXpress System Packs (UXSPs)**. UXSPs are bundled updates designed and tested to provide the interdependent level of functionality, performance, and compatibility. UXSPs are server machine-type specific and are built (with firmware and device driver updates) to support specific Windows Server, Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) operating system distributions. Machine-type-specific firmware-only UXSPs are also available.

See the following table to determine the best Lenovo tool to use for installing and setting up the firmware:

Note: The server UEFI settings for option ROM must be set to **Auto** or **UEFI** to update firmware using Lenovo XClarity Administrator or Lenovo XClarity Essentials. For more information, see the following Tech Tip:

https://datacentersupport.lenovo.com/us/en/solutions/ht506118

Tool	In-band update	Out-of-band update	On-target update	Off-target update	Graphical user interface	Command-line interface	Supports UXSPs
Lenovo XClarity Provisioning Manager Limited to core system firmware only.	√			√	√		√
Lenovo XClarity Controller Supports core system firmware and most advanced I/O option firmware updates		√		√	√	√	
Lenovo XClarity Essentials OneCLI Supports all core system firmware, I/O firmware, and installed operating system driver updates	√	√				√	√
Lenovo XClarity Essentials UpdateXpress Supports all core system firmware, I/O firmware, and installed operating system driver updates	√	√			√		√
Lenovo XClarity Essentials Bootable Media Creator Supports core system firmware and I/O firmware updates. You can update the Microsoft Windows operating system, but device drivers are not included on the bootable image	√				√	√	√
Lenovo XClarity Administrator Supports core system firmware and I/O firmware updates	√	√		√	√		

The latest firmware can be found at the following site:

http://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr530/7X07/downloads

- **Lenovo XClarity Provisioning Manager**

  From Lenovo XClarity Provisioning Manager, you can update the Lenovo XClarity Controller firmware, the UEFI firmware, and the Lenovo XClarity Provisioning Manager software.

Note: By default, the Lenovo XClarity Provisioning Manager Graphical User Interface is displayed when you press F1. If you have changed that default to be the text-based system setup, you can bring up the Graphical User Interface from the text-based system setup interface.

Additional information about using Lenovo XClarity Provisioning Manager to update firmware is available at:

http://sysmgt.lenovofiles.com/help/topic/LXPM/platform_update.html

- **Lenovo XClarity Controller**

  If you need to install a specific update, you can use the Lenovo XClarity Controller interface for a specific server.

  Notes:

  – To perform an in-band update through Windows or Linux, the operating system driver must be installed and the Ethernet-over-USB (sometimes called LAN over USB) interface must be enabled.

    Additional information about configuring Ethernet over USB is available at:

    http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_configuringUSB.html

  – If you update firmware through the Lenovo XClarity Controller, make sure that you have downloaded and installed the latest device drivers for the operating system that is running on the server.

  Specific details about updating firmware using Lenovo XClarity Controller are available at:

  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_manageserverfirmware.html

- **Lenovo XClarity Essentials OneCLI**

  Lenovo XClarity Essentials OneCLI is a collection of command line applications that can be used to manage Lenovo servers.Its update application can be used to update firmware and device drivers for your servers. The update can be performed within the host operating system of the server (in-band) or remotely through the BMC of the server (out-of-band).

  Specific details about updating firmware using Lenovo XClarity Essentials OneCLI is available at:

  http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_c_update.html

- **Lenovo XClarity Essentials UpdateXpress**

  Lenovo XClarity Essentials UpdateXpress provides most of OneCLI update functions through a graphical user interface (GUI). It can be used to acquire and deploy UpdateXpress System Pack (UXSP) update packages and individual updates. UpdateXpress System Packs contain firmware and device driver updates for Microsoft Windows and for Linux.

  You can obtain Lenovo XClarity Essentials UpdateXpress from the following location:

  https://datacentersupport.lenovo.com/solutions/lnvo-xpress

- **Lenovo XClarity Essentials Bootable Media Creator**

  You can use Lenovo XClarity Essentials Bootable Media Creator to create bootable media that is suitable for applying firmware updates, running preboot diagnostics, and deploying Microsoft Windows operating systems.

  You can obtain Lenovo XClarity Essentials BoMC from the following location:

  https://datacentersupport.lenovo.com/solutions/lnvo-bomc

- **Lenovo XClarity Administrator**

If you are managing multiple servers using the Lenovo XClarity Administrator, you can update firmware for all managed servers through that interface. Firmware management is simplified by assigning firmware-compliance policies to managed endpoints. When you create and assign a compliance policy to managed endpoints, Lenovo XClarity Administrator monitors changes to the inventory for those endpoints and flags any endpoints that are out of compliance.

Specific details about updating firmware using Lenovo XClarity Administrator are available at:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/update_fw.html

Configuring the LAN over USB interface manually

To perform a firmware update through the operating system using Lenovo XClarity Essentials OneCLI, the Lenovo XClarity Controller must be configured to use the LAN over USB interface. The firmware update package attempts to perform the setup automatically, if needed. If the automatic setup fails or if you prefer to set up the LAN over USB manually, use one of the following procedures.

Additional information about using the Lenovo XClarity Controller to enable LAN over USB is available at:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_configuringUSB.html

Installing the LAN over USB Windows device driver

When you install a Windows operating system, there might be an unknown RNDIS device in the Device Manager. Lenovo provides a Windows INF file that identifies this device.

Complete the following steps to install `ibm_rndis_server_os.inf`:

Note: You only have to perform these steps if the compute node is running a Windows operating system and the `ibm_rndis_server_os.inf` file has not been previously installed. The file only has to be installed once. It is required by Windows operating systems to detect and use the LAN over USB functionality.

Step 1. Click **Administrative Tools → Computer Management → Device Manager** and find the RNDIS Device. Click **Properties → Driver → Reinstall driver**. Point the server to the `\Windows\inf` directory where it can find the `ibm_rndis_server_os.inf` file and install the device.

Step 2. Click **Administrative Tools → Device Manager**. Right-click **Network adapters** and select **Scan for hardware changes**. A small pop-up confirms that the Ethernet device is found and installed. The New Hardware Wizard starts automatically.

Step 3. When you are prompted `Can Windows connect to Windows Update to search for software?`, select **No, not this time**. Click **Next** to continue.

Step 4. When you are prompted `What do you want the wizard to do?`, select **Install from a list or specific location (Advanced)**. Click **Next** to continue.

Step 5. When you are prompted `Please choose your search and installation options`, select **Don't search. I will choose the driver to install**. Click **Next** to continue.

Step 6. When you are prompted `Select a hardware type, and then click Next`, select **Network adapters**. Click **Next** to continue.

Step 7. When you are prompted with the statement `Completing the Found New Hardware Wizard`, click **Finish**. A new local area connection appears. If the message `This connection has limited or no connectivity` is displayed, ignore this message.

Step 8. Return to the Device Manager. **Lenovo USB Remote NDIS Network Device** appears under **Network Adapters**.

Step 9. Use the Lenovo XClarity Controller interface to view or set the IP address for the LAN adapter.

Additional information about using the Lenovo XClarity Controller to configure LAN over USB is available at:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_configuringUSB.html

Tech Tips

Lenovo continually updates the support Web site with the latest tips and techniques that you can use to solve issues that you might have with your server. These Tech Tips (also called retain tips or service bulletins) provide procedures to work around issues related to the operation of your server.

To find the Tech Tips available for your server:

1. Go to http://datacentersupport.lenovo.com and navigate to the support page for your server.
2. Click **Documentation** from the navigation pane.

   Follow the on-screen instructions to choose the category for the problem that you are having.

Security advisories

Lenovo is committed to developing products and services that adhere to the highest security standards in order to protect our customers and their data. When potential vulnerabilities are reported, it is the responsibility of the Lenovo Product Security Incident Response Team (PSIRT) to investigate and provide information to our customers so they may put mitigation plans in place as we work toward providing solutions.

The list of current advisories is available at the following location:
https://datacentersupport.lenovo.com/product_security/home

Power on the server

After the server performs a short self-test (power status LED flashes quickly) when connected to input power, it enters a standby state (power status LED flashes once per second).

The server can be turned on (power status LED on) in any of the following ways:

- You can press the power button.
- The server can restart automatically after a power interruption.
- The server can respond to remote power-on requests sent to the Lenovo XClarity Controller.

For information about powering off the server, see “Power off the server” on page 11.

Power off the server

The server remains in a standby state when it is connected to a power source, allowing the Lenovo XClarity Controller to respond to remote power-on requests. To remove all power from the server (power status LED off), you must disconnect all power cables.

To place the server in a standby state (power status LED flashes once per second):

Note: The Lenovo XClarity Controller can place the server in a standby state as an automatic response to a critical system failure.

- Start an orderly shutdown using the operating system (if supported by your operating system).
- Press the power button to start an orderly shutdown (if supported by your operating system).

- Press and hold the power button for more than 4 seconds to force a shutdown.

When in a standby state, the server can respond to remote power-on requests sent to the Lenovo XClarity Controller. For information about powering on the server, see “Power on the server” on page 11.

Chapter 2. Server components

Use the information in this section to learn about each of the components associated with your server.

Front view

The front view of the server varies by the model.

- Front view of server models with 3.5-inch drive bays
- Front view of server models with 2.5-inch drive bays

The following illustrations show the front views of server models with hot-swap drives. Depending on the model, your server might look slightly different the illustrations.

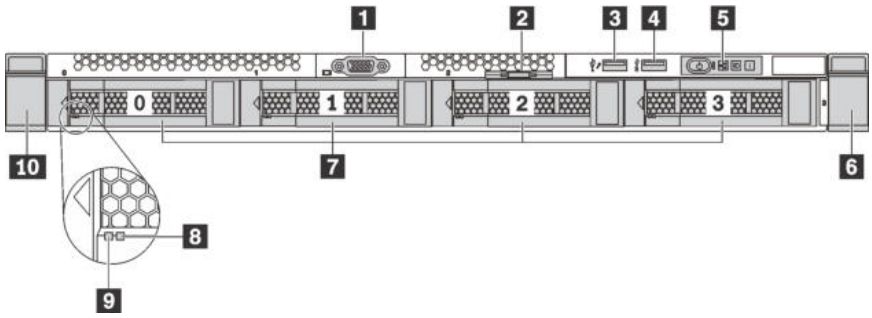


Figure 4. Front view of server models with 3.5-inch drive bays

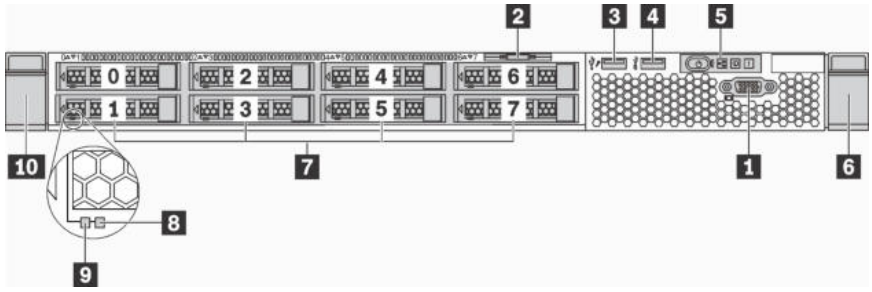


Figure 5. Front view of server models with 2.5-inch drive bays

Table 2. Components on the front of the server

Callout	Callout
1 VGA connector (available on some model)	2 Pull-out information tab
3 XClarity Controller USB connector	4 USB 3.0 connector
5 Operator information panel	6 Rack latch (right)
7 Drive bays	8 Drive status LED (yellow)
9 Drive activity LED (green)	10 Rack latch (left)

1 VGA connector (available on some models)

© Copyright Lenovo 2017, 2020

Used to attach a high-performance monitor, a direct-drive monitor, or other devices that use a VGA connector.

2 Pull-out information tab

The Lenovo XClarity Controller network access label is attached on the pull-out information tab.

3 XClarity Controller USB connector

Depending on the setting, this connector supports USB 2.0 function, XClarity Controller management function, or both.

- If the connector is set for USB 2.0 function, you can attach a device that requires a USB 2.0 connection, such as a keyboard, a mouse, or a USB storage device.
- If the connector is set for XClarity Controller management function, you can attach a mobile device installed with the application to run XClarity Controller event logs.
- If the connector is set to have both functions, you can press the ID button for three seconds to switch between the two functions.

4 USB 3.0 connector

Attach a USB-compatible device, such as a USB keyboard, USB mouse, or USB storage device.

5 Operator information panel

For information about the controls and status LEDs on the operator information panel, see “Operator information panel” on page 15.

6 10 Rack latches

If your server is installed in a rack, you can use the rack latches to help you slide the server out of the rack. You also can use the latches and screws to secure the server in the rack so that the server cannot slide out, especially in vibration-prone areas. For more information, refer to the *Rack Installation Guide* that comes with your rail kit.

7 Drive bays

The number of the installed drives in your server varies by model. When you install drives, follow the order of the drive bay numbers.

The EMI integrity and cooling of the server are protected by having all drive bays occupied. The vacant drive bays must be occupied by drive fillers.

8 Drive status LED

9 Drive activity LED

Each hot-swap drive has two LEDs.

Drive LED	Status	Description
8 Drive status LED (right)	Solid yellow	The drive has an error.
	Blinking yellow (blinking slowly, about one flash per second)	The drive is being rebuilt.
	Blinking yellow (blinking rapidly, about four flashes per second)	The RAID controller is locating the drive.
9 Drive activity LED (left)	Solid green	The drive is powered but not active.
	Blinking green	The drive is active.

Operator information panel

The operator information panel of the server provides controls and LEDs.

The following illustration shows the operator information panel of the server.

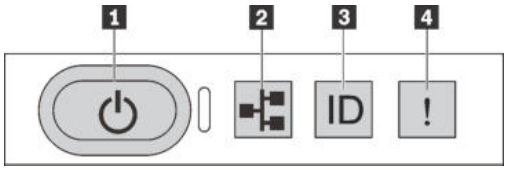


Figure 6. Operator information panel

Table 3. Components on the operator information panel

Callout	Callout
1 Power button with power status	2 Network activity
3 System ID button with ID	4 System error

1 Power button with power status

You can press the power button to power on the server when you finish setting up the server. You also can hold the power button for several seconds to power off the server if you cannot shut down the server from the operating system. The power status helps you to determine the current power status.

Status	Color	Description
Solid on	Green	The server is on and running.
Slow blinking (about one flash per second)	Green	The server is off and is ready to be powered on (standby state).
Fast blinking (about four flashes per second)	Green	The server is off, but the XClarity Controller is initializing, and the server is not ready to be powered on.
Off	None	There is no ac power applied to the server.

2 Network activity LED

Compatibility of the NIC adapter and the network activity LED.

NIC adapter	Network activity LED
LOM adapter	Support
ML2 NIC adapter	Support
PCIe NIC adapter	Not support

The network activity LED on the operator information panel helps you identify the network connectivity and activity.

Status	Color	Description
On	Green	The server is connected to a network.
Blinking	Green	The network is connected and active.
Off	None	The server is disconnected from the network.

3 System ID button with ID LED

Use this system ID button and the blue system ID LED to visually locate the server. A system ID LED is also located on the rear of the server. Each time you press the system ID button, the state of both the system ID LEDs changes. The LEDs can be changed to on, blinking, or off. You can also use the Lenovo XClarity Controller or a remote management program to change the state of the system ID LEDs to assist in visually locating the server among other servers.

If the XClarity Controller USB connector is set to have both the USB 2.0 function and XClarity Controller management function, you can press the ID button for three seconds to switch between the two functions.

4 System error LED

Status	Color	Description	Action
On	Yellow	An error has been detected on the server. Causes might include but not limited to the following errors: • The temperature of the server reached the non-critical temperature threshold. • The voltage of the server reached the non-critical voltage threshold. • A fan has been detected to be running at low speed. • A fan has been removed. • The power supply has a critical error. • The power supply is not connected to the power.	Check the event log to determine the exact cause of the error. For information about troubleshooting, see “Troubleshooting by symptom” on page 148 .
Off	None	The server is off or the server is on and is working correctly.	None.

Rear view

The rear of the server provides access to several components, including the power supplies, PCIe adapters, serial port, and Ethernet connectors.

- “Rear view of server models with three PCIe slots” on page 17
- “Rear view of server models with two PCIe slots” on page 19

Rear view of server models with three PCIe slots

The following illustration shows the rear view of server models with three PCIe slots. Depending on the model, your server might look slightly different from the illustrations in this topic.

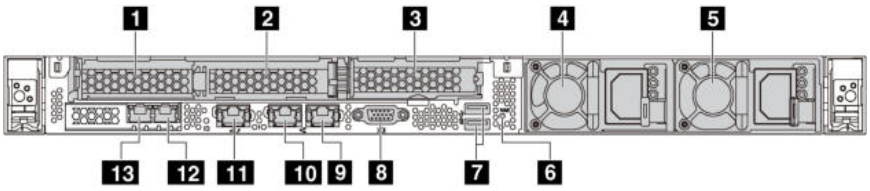


Figure 7. Rear view of server models with three PCIe slots

Table 4. Connectors on the rear of the server

Callout	Callout
1 PCIe slot 1 on riser 1 assembly	2 PCIe slot 2 on riser 1 assembly
3 PCIe slot 3 on riser 2 assembly	4 Power supply 1
5 Power supply 2 (available on some models)	6 NMI button
7 USB 3.0 connectors	8 VGA connector
9 Ethernet connector 2 (RJ-45)	10 Ethernet connector 1 (RJ-45)
11 XClarity Controller network connector	12 Ethernet connector 2 on the LOM adapter (available on some models)
13 Ethernet connector 1 on the LOM adapter (available on some models)	

1 2 PCIe slots on riser 1 assembly

Your server supports two types of riser cards for riser 1 assembly.

- Type 1
  - Slot 1: PCIe x16 (x8, x4, x1), low-profile
  - Slot 2: PCIe x16 (x16, x8, x4, x1), low-profile
- Type 2
  - Slot 1: PCIe x16 (x8, x4, x1), low-profile
  - Slot 2: ML2 x8 (x8, x4, x1), low-profile

3 PCIe slot on riser 2 assembly

Your server supports two types of riser cards for riser 2 assembly.

- Type 1: PCIe x16 (x8, x4, x1), low-profile

- Type 2: PCIe x16 (x16, x8, x4, x1), low-profile

  Note: Type 2 is supported only when two processors are installed.

4 Power supply 1

5 Power supply 2 (available on some models)

The hot-swap redundant power supplies help you avoid significant interruption to the operation of the system when a power supply fails. You can purchase a power supply option from Lenovo and install the power supply to provide power redundancy without turning off the server.

On each power supply, there are three status LEDs near the power cord connector. For information about the LEDs, see “Rear view LEDs” on page 21.

6 NMI button

Press this button to force a nonmaskable interrupt (NMI) to the processor. By this way, you can blue screen the server and take a memory dump. You might have to use a pen or the end of a straightened paper clip to press the button.

7 USB 3.0 connectors (2)

Attach a USB-compatible device, such as a USB keyboard, USB mouse, or USB storage device.

8 VGA connector

Used to attach a high-performance monitor, a direct-drive monitor, or other devices that use a VGA connector.

9 Ethernet connector 2

10 Ethernet connector 1

Used to attach an Ethernet cable for a LAN. Each Ethernet connector has two status LEDs to help you identify the Ethernet connectivity and activity. For information about the LEDs, see “Rear view LEDs” on page 21.

Ethernet connector 1 can be set as XClarity Controller network connector. To set Ethernet connector 1 as XClarity Controller network connector, start Setup utility, go to **BMC Settings → Network Settings → Network Interface Port** and select **Shared**. Then, go to **Shared NIC on** and select **Onboard Port 1**.

11 XClarity Controller network connector

Used to attach an Ethernet cable to manage the system using XClarity Controller.

12 Ethernet connector 2 on the LOM adapter

13 Ethernet connector 1 on the LOM adapter

The LOM adapter provides two extra Ethernet connectors for network connections.

Ethernet connector 1 on the LOM adapter can be set as XClarity Controller network connector. To set the Ethernet connector as XClarity Controller network connector, start Setup utility, go to **BMC Settings → Network Settings → Network Interface Port** and select **Shared**. Then, go to **Shared NIC on** and select **PHY Card**.

Rear view of server models with two PCIe slots

The following illustrations show the rear view of the server models with two PCIe slots. Depending on the model, your server might look slightly different from the illustrations in this topic.

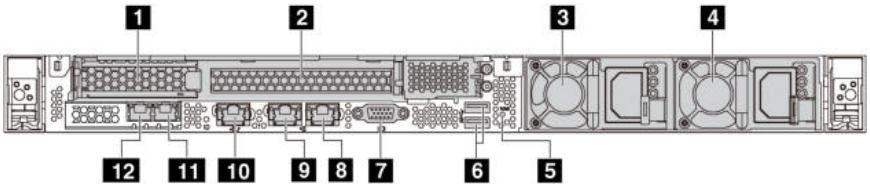


Figure 8. Rear view of server models with two PCIe slots

Table 5. Connectors on the rear of the server

Callout	Callout
1 PCIe slot 1 on riser 1 assembly	2 PCIe slot 2 on riser 1 assembly
3 Power supply 1	4 Power supply 2 (available on some models)
5 NMI button	6 USB 3.0 connectors
7 VGA connector	8 Ethernet connector 2 (RJ-45)
9 Ethernet connector 1 (RJ-45)	10 XClarity Controller network connector
11 Ethernet connector 2 on the LOM adapter (available on some models)	12 Ethernet connector 1 on the LOM adapter (available on some models)

1 2 PCIe slots on riser 1 assembly

Your server supports two types of riser cards for riser 1 assembly.

- Type 1
  - Slot 1: PCIe x16 (x8, x4, x1), low-profile
  - Slot 2: PCIe x16 (x16, x8, x4, x1), full-height, half-length
- Type 2
  - Slot 1: PCIe x16 (x8, x4, x1), low-profile
  - Slot 2: ML2 x8 (x8, x4, x1), low-profile adapter with full-height bracket

3 Power supply 1

4 Power supply 2 (available on some models)

The hot-swap redundant power supplies help you avoid significant interruption to the operation of the system when a power supply fails. You can purchase a power supply option from Lenovo and install the power supply to provide power redundancy without turning off the server.

On each power supply, there are three status LEDs near the power cord connector. For information about the LEDs, see “Rear view LEDs” on page 21.

5 NMI button

Press this button to force a nonmaskable interrupt (NMI) to the processor. By this way, you can blue screen the server and take a memory dump. You might have to use a pen or the end of a straightened paper clip to press the button.

6 USB 3.0 connectors (2)

Attach a USB-compatible device, such as a USB keyboard, USB mouse, or USB storage device.

7 VGA connector

Used to attach a high-performance monitor, a direct-drive monitor, or other devices that use a VGA connector.

8 Ethernet connector 2

9 Ethernet connector 1

Used to attach an Ethernet cable for a LAN. Each Ethernet connector has two status LEDs to help you identify the Ethernet connectivity and activity. For information about the LEDs, see “Rear view LEDs” on page 21.

Ethernet connector 1 can be set as XClarity Controller Network connector. To set Ethernet connector 1 as XClarity Controller Network connector, start Setup utility, go to **BMC Settings → Network Settings → Network Interface Port** and select **Shared**. Then, go to **Shared NIC on** and select **Onboard Port 1**.

10 XClarity Controller network connector

Used to attach an Ethernet cable to manage the system using XClarity Controller.

11 Ethernet connector 2 on the LOM adapter

12 Ethernet connector 1 on the LOM adapter

The LOM adapter provides two extra Ethernet connectors for network connections.

Ethernet connector 1 on the LOM adapter can be set as XClarity Controller Network connector. To set the Ethernet connector as XClarity Controller Network connector, start Setup utility, go to **BMC Settings → Network Settings → Network Interface Port** and select **Shared**. Then, go to **Shared NIC on** and select **PHY Card**.

Rear view LEDs

The rear of the server provides system ID LED, system error LED, network LEDs, and power supply LEDs.

The following illustration shows the LEDs on the rear view of server models with three PCIe slots. The LEDs on the rear view of server models with two PCIe slots are the same.

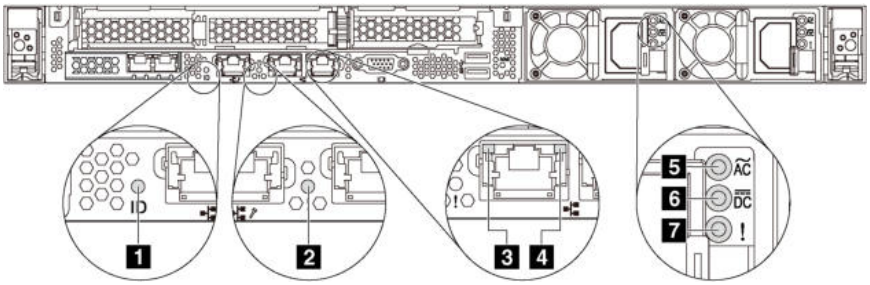


Figure 9. Rear view LEDs

Table 6. LEDs on the rear view of the server

Callout	Callout
1 System ID LED	2 System error LED
3 Ethernet link LED	4 Ethernet activity LED
5 Power input LED	6 Power output LED
7 Power supply error LED	

1 System ID LED

The blue system ID LED helps you to visually locate the server. A system ID LED is also located on the front of the server. Each time you press the system ID button, the state of both the system ID LEDs changes. The LEDs can be changed to on, blinking, or off. You can also use the Lenovo XClarity Controller or a remote management program to change the state of the system ID LEDs to assist in visually locating the server among other servers.

2 System error LED

The system error LED helps you to determine if there are any system errors. For details, see “System error LED” on page 16.

3 Ethernet link LED

4 Ethernet activity LED

Each Ethernet connector has two status LEDs.

Ethernet status LED	Color	Status	Description
3 Ethernet link LED	Green	On	Network link is established.
	None	Off	Network link is disconnected.
4 Ethernet activity LED	Green	Blinking	Network link is connected and active.
	None	Off	The server is disconnected from a LAN.

5 6 7 Power supply LEDs

Each hot-swap power supply has three status LEDs.

LED	Description
5 Power input LED	• Green: The power supply is connected to the ac power source. • Off: The power supply is disconnected from the ac power source.
6 Power output LED	• Green: The server is on and the power supply is working normally. • Blinking green: The power supply is in the zero-output mode (standby). When the server power load is low, one of the installed power supplies enters into the standby state while the other one delivers the entire load. When the power load increases, the standby power supply will switch to active state to provide sufficient power to the system. To disable zero-output mode, start the Setup utility, go to **System Settings → Power → Zero Output** and select **Disable**. If you disable the zero-out mode, both power supplies will be in the active state. • Off: The server is powered off, or the power supply is not working properly. If the server is powered on but the LED is off, replace the power supply.
7 Power supply error LED	• Yellow: The power supply has failed. To resolve the issue, replace the power supply. • Off: The power supply is working normally

System board components

The illustration in this section shows the component locations on the system board.

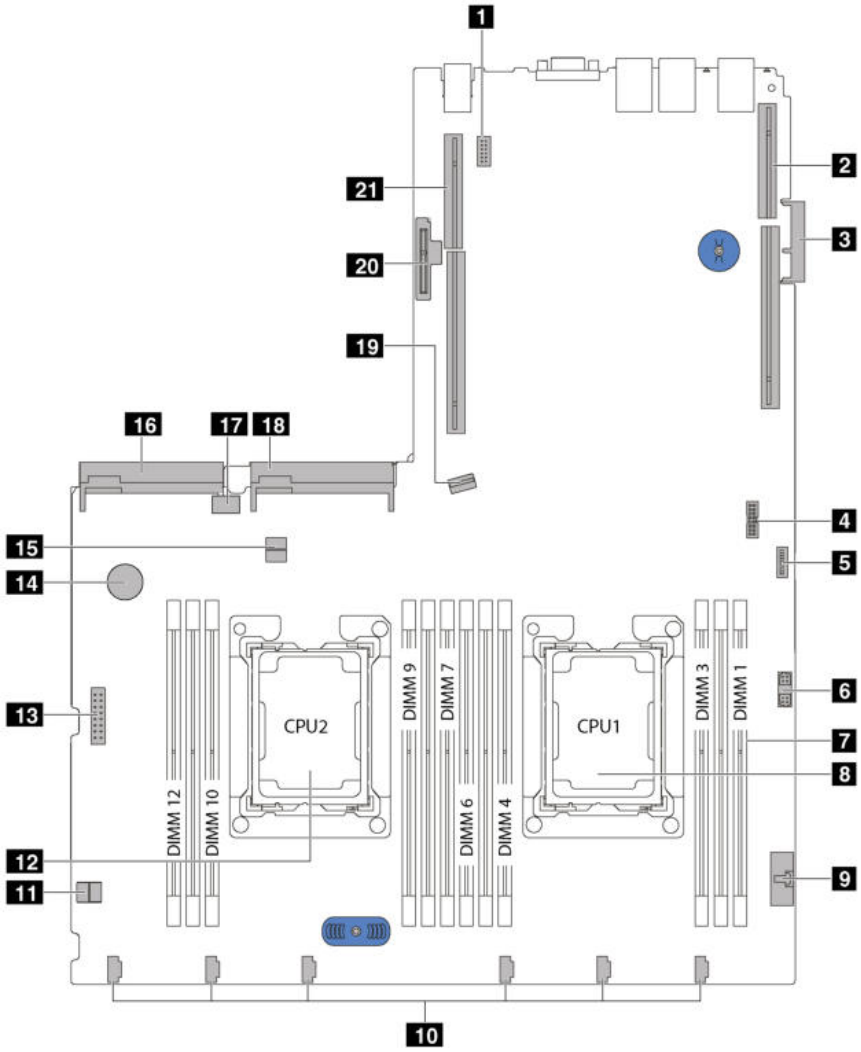


Figure 10. System board components

Callout	Callout
1 Serial-port-module connector	2 Riser 1 slot
3 LOM adapter connector	4 TCM[1]/TPM[2] connector (for Chinese Mainland only)
5 Front USB connector	6 Front VGA connector
7 DIMM slots	8 Processor 1 socket
9 Operator-information-panel connector	10 System fan connectors
11 Cable retainer	12 Processor 2 socket
13 Backplane power connector	14 CMOS battery
15 Cable retainer	16 Power supply 2 connector

Callout	Callout
17 Internal USB connector	18 Power supply 1 connector
19 SATA 0-3 connector	20 M.2 module slot
21 Riser 2 slot	

Notes:

- [1] Trusted Cryptography Module
- [2] Trusted Platform Module

System board switches and jumpers

The following illustration shows the location of the switches and jumpers on the server.

Note: If there is a clear protective sticker on the top of the switch blocks, you must remove and discard it to access the switches.

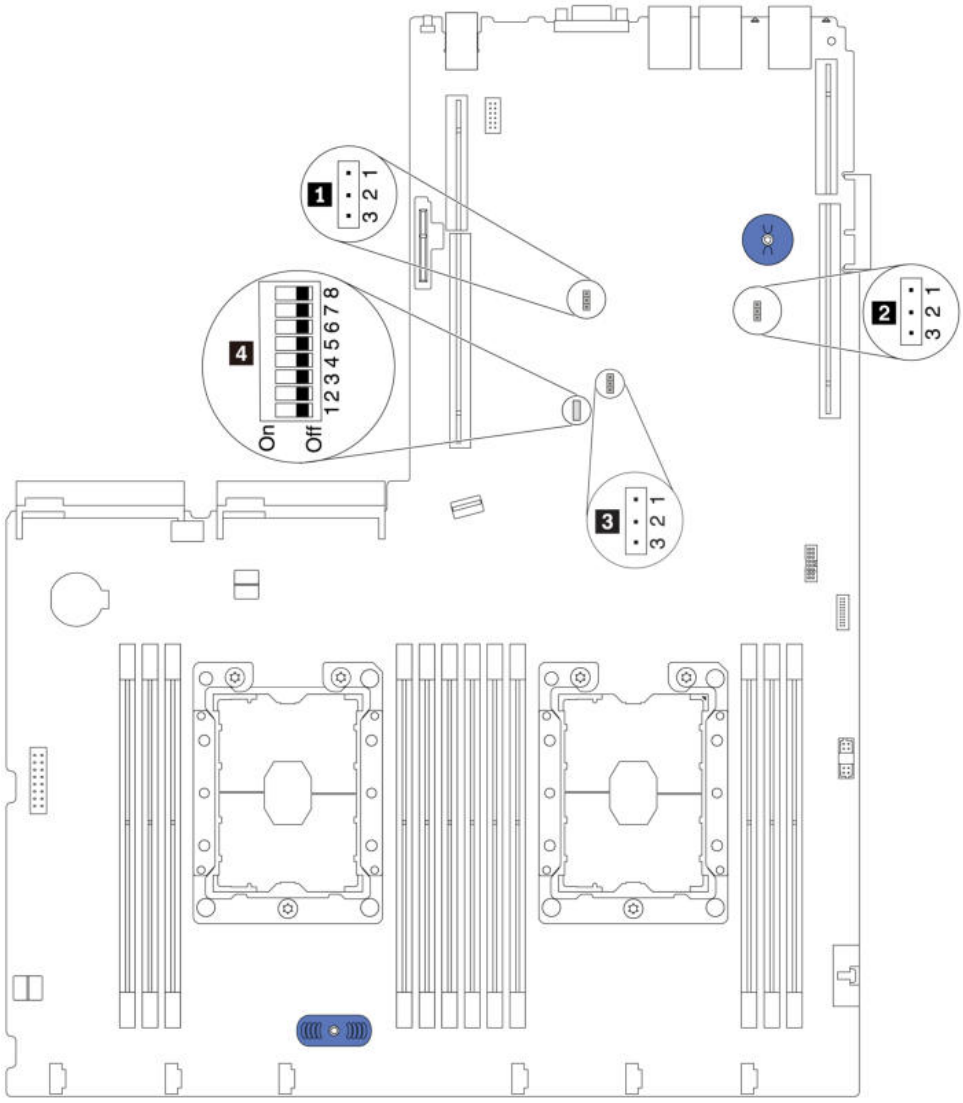


Figure 11. System-board switches and jumpers

Table 7. Jumpers and switches on the system board

Jumper/Switch name	Jumper/Switch number	Jumper/Switch setting
1 TPM/TCM physical presence jumper	JP6	• Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: TPM/TCM physical presence is asserted.
2 Clear CMOS jumper	JP3	• Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: Clear the real-time clock (RTC) registry.
3 ME firmware security override	JP8	• Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: Enable Flash security override. **Note:** For debug only.
4 SW6 switch block	SW6 (including switches 1, 2, 3, 4, 5, 6, 7, and 8)	All the switches are in the **Off** position by default. • Switches 1, 6, and 8: Reserved. • Switch 2: Override power-on password switch. Changing position of this switch overrides the power-on password. Changing position of this switch does not affect the administrator password.
4 Power permission	SW6 (switch 7)	The default position is Off. Changing this switch to the On position enables Power On.
4 Force XCC reset	SW6 (switch 4)	The default position is Off. Changing this switch to the On position resets the Lenovo XClarity Controller.
4 Force XCC update	SW6 (switch 3)	The default position is Off. Changing this switch to the On position forces the Lenovo XClarity Controller to update to the latest version.

Important:

- Before you move the switches and jumpers, turn off the server. Then, disconnect all power cords and external cables. Do not open your server or attempt any repair before reading and understanding the following information:
  - http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html
  - “Handling static-sensitive devices” on page 43
- Any system-board switch or jumper block that is not shown in the illustrations in this document are reserved.

System board LEDs

The following illustrations show the light-emitting diodes (LEDs) on the system board.

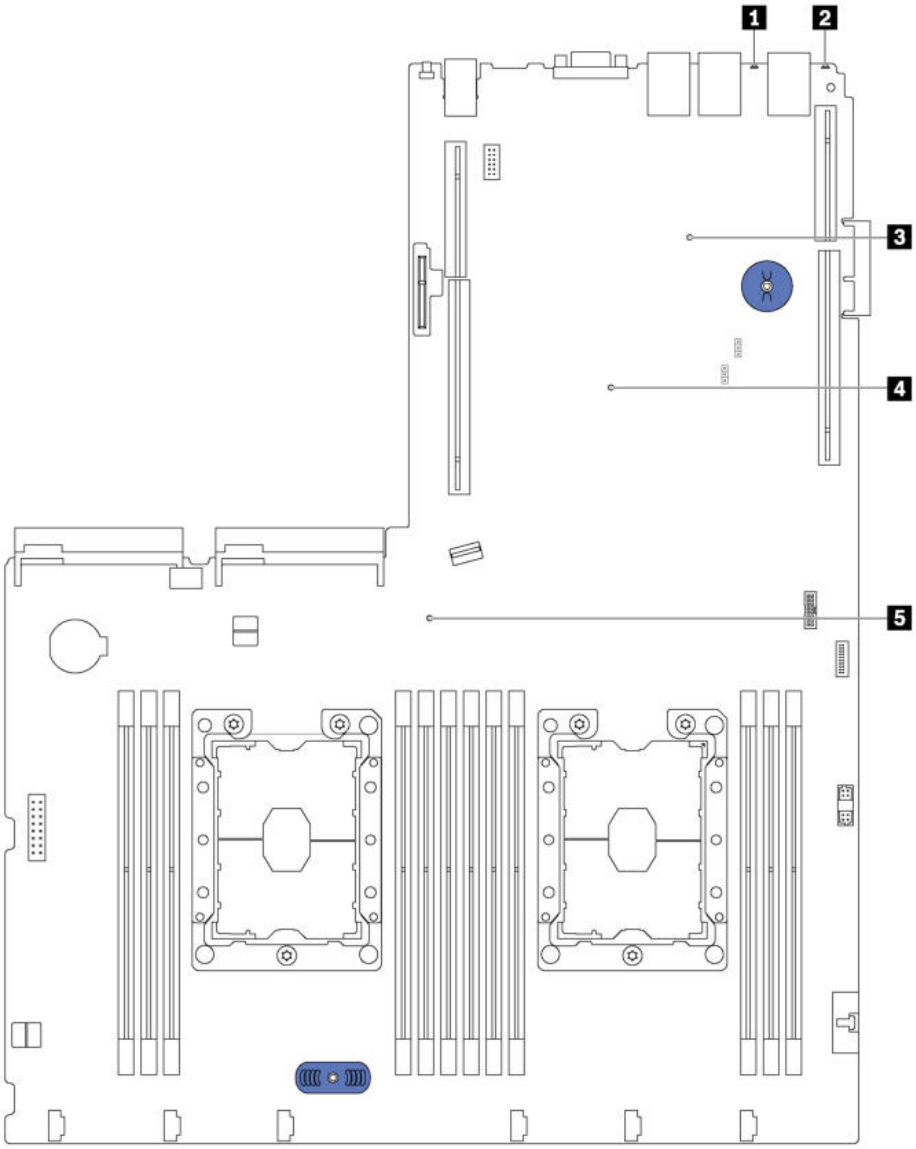


Figure 12. System board LEDs

Table 8. LEDs on the system board

Callout	Callout
1 System error LED	2 System ID LED
3 XClarity Controller heartbeat LED	4 Field-Programmable Gate Array (FPGA) error LED
5 System power LED	

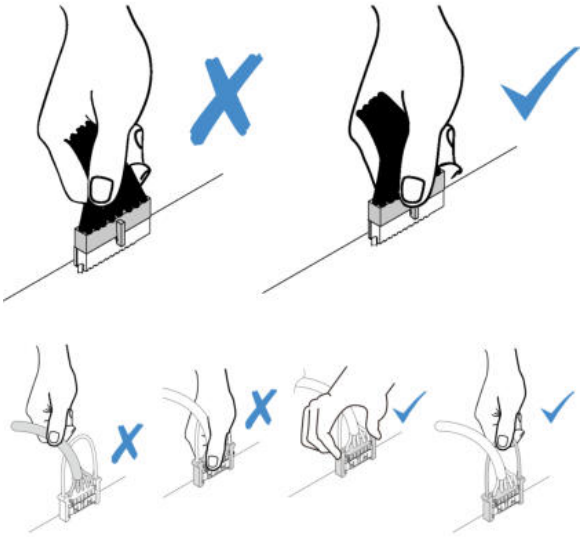
Internal cable routing

Some of the components in the server have internal cables and cable connectors.

To connect cables, observe the following guidelines:

- Power off the server before you connect or disconnect any internal cables.
- See the documentation that comes with any external devices for additional cabling instructions. It might be easier for you to route cables before you connect the devices to the server.
- Cable identifiers of some cables are printed on the cables that come with the server and optional devices. Use these identifiers to connect the cables to the correct connectors.
- Ensure that the relevant cables pass through the cable clips.

Note: Disengage all latches, release tabs, or locks on cable connectors when you disconnect cables from the system board. Failing to release them before removing the cables will damage the cable sockets on the system board, which are fragile. Any damage to the cable sockets might require replacing the system board.



VGA connector

Use this section to understand the cable routing for the video graphic adapter (VGA) connector.

Note: The VGA connector is available on some models.

Server models with 3.5-inch drive bays

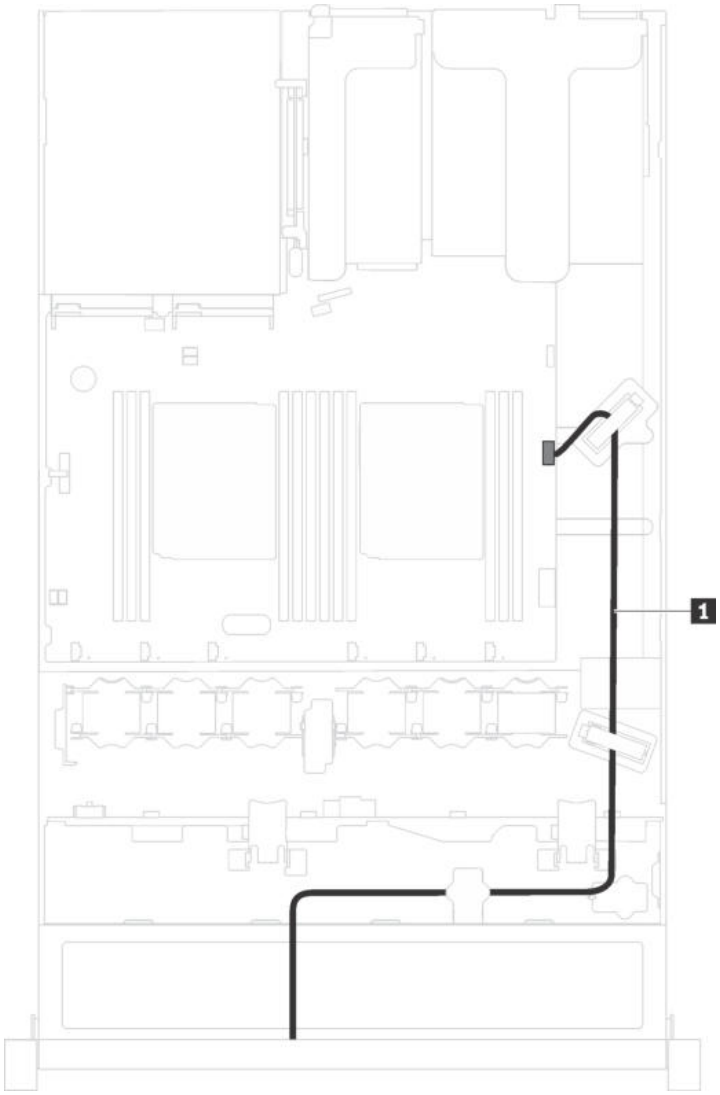


Figure 13. VGA connector cable routing

From	To
1 VGA cable	Front VGA connector on the system board

Server models with 2.5-inch drive bays

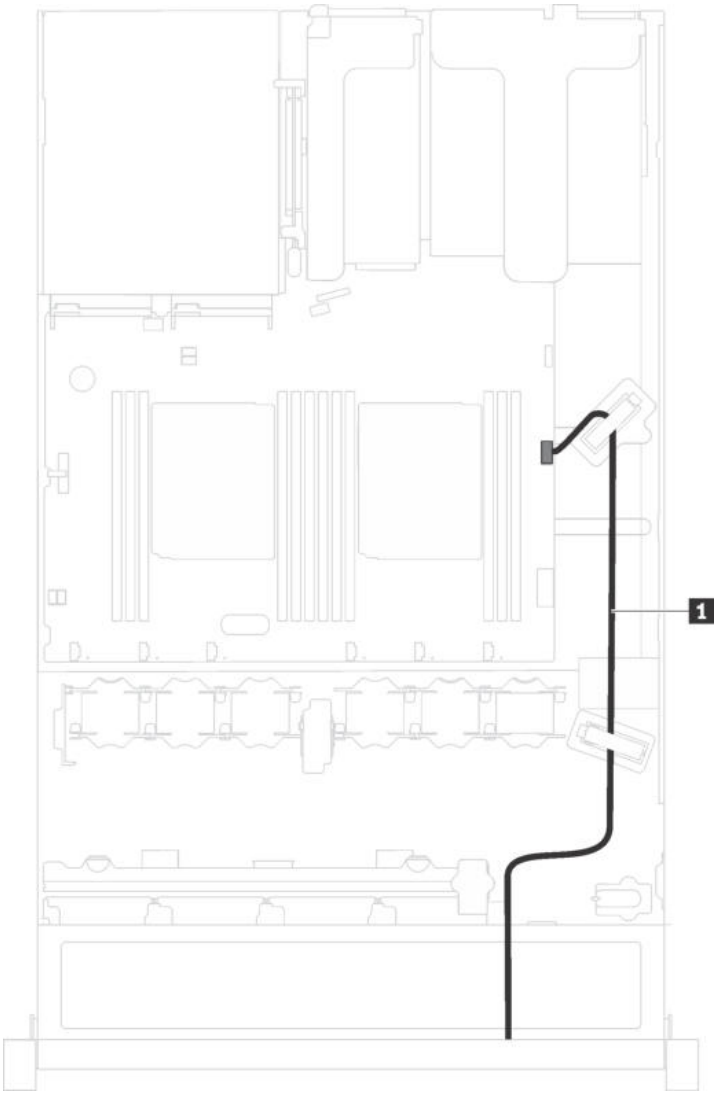


Figure 14. VGA connector cable routing

From	To
1 VGA cable	Front VGA connector on the system board

Front I/O assembly

Use this section to understand the cable routing for the front I/O assembly.

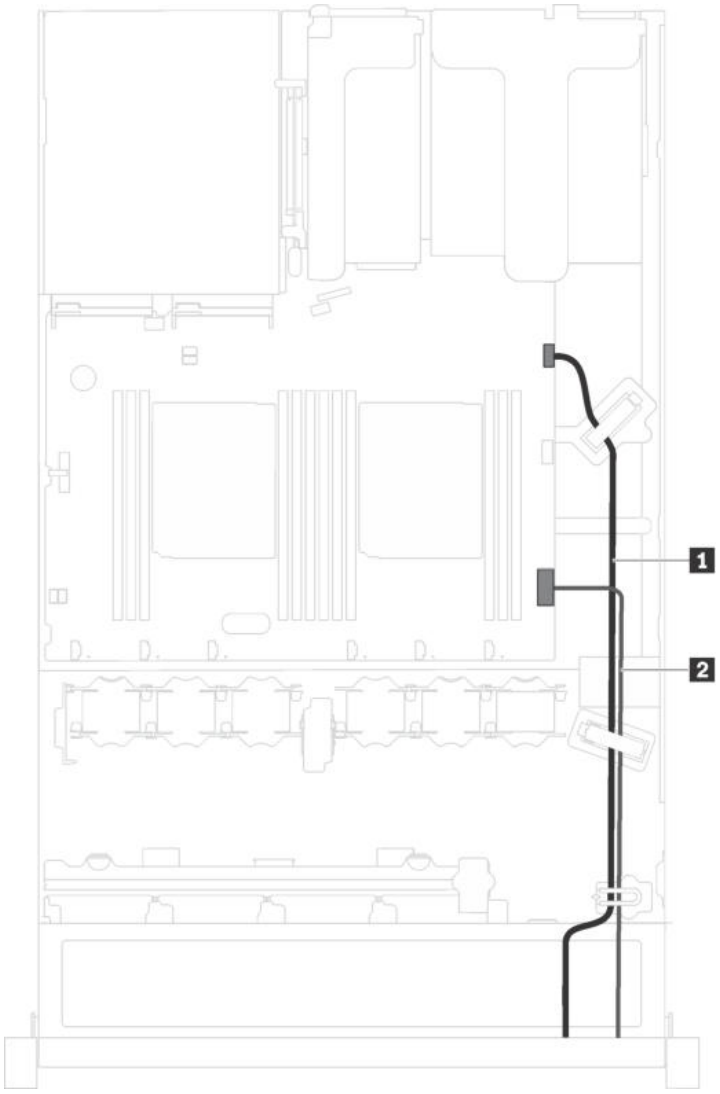


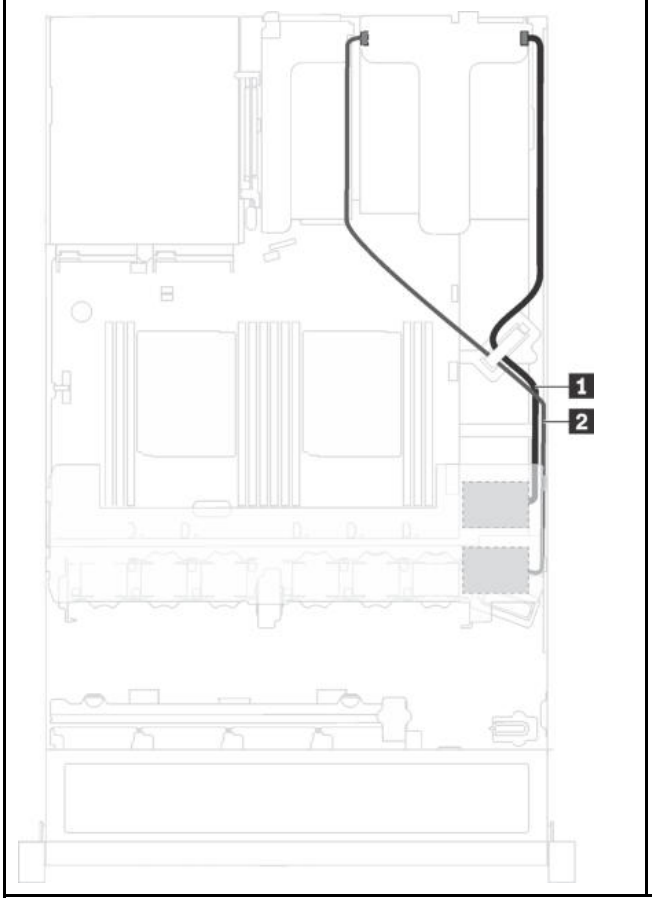
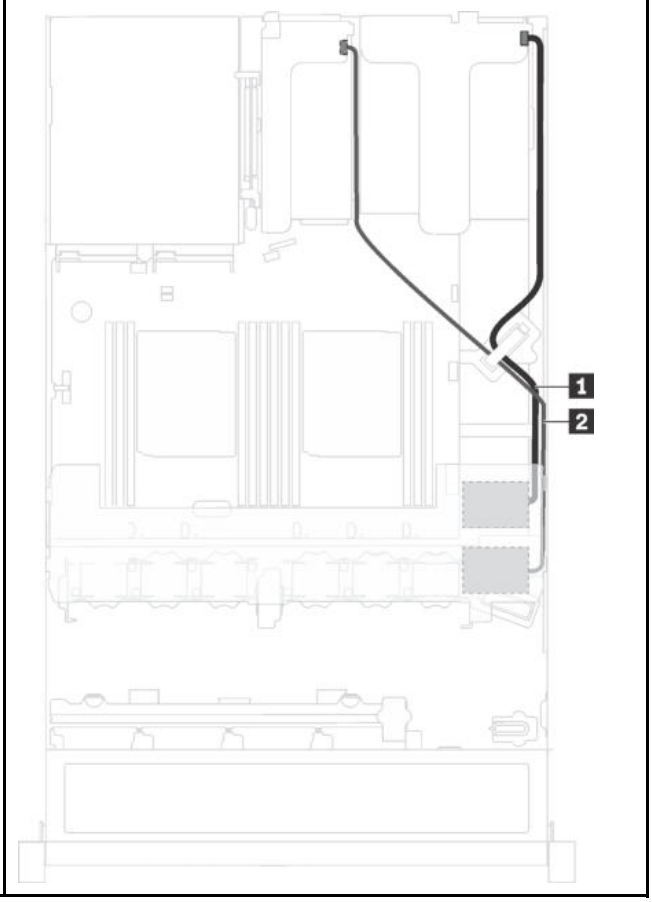
Figure 15. Cable routing for the front I/O assembly

From	To
1 Front USB cable	Front USB connector on the system board
2 Operator-information-panel cable	Operator-information-panel connector on the system board

RAID super capacitor module

Use this section to understand the cable routing for RAID super capacitor modules.

Your server supports up to two RAID super capacitor modules.

Scenario 1: the second RAID adapter in PCIe slot 2	Scenario 2: the second RAID adapter in PCIe slot 3
	

1 Cable routing for RAID super capacitor module 1

2 Cable routing for RAID super capacitor module 2

An extension cable is provided for each RAID super capacitor module for connection.

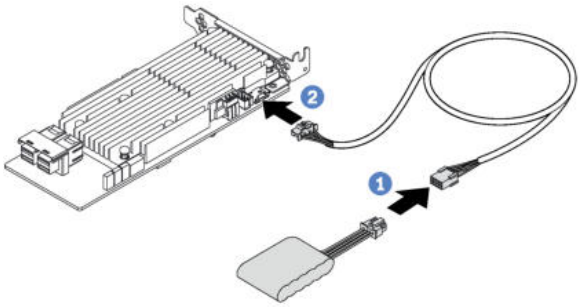


Figure 16. Connecting the RAID super capacitor module to the RAID adapter

Backplanes

Use this section to understand the cable routing for the backplanes.

Server model with eight 2.5-inch hot-swap drives

Use this section to understand the internal cable routing for the server model with eight 2.5-inch hot-swap drives.

The following illustration shows the cable routing for the server model with eight 2.5-inch hot-swap drives.

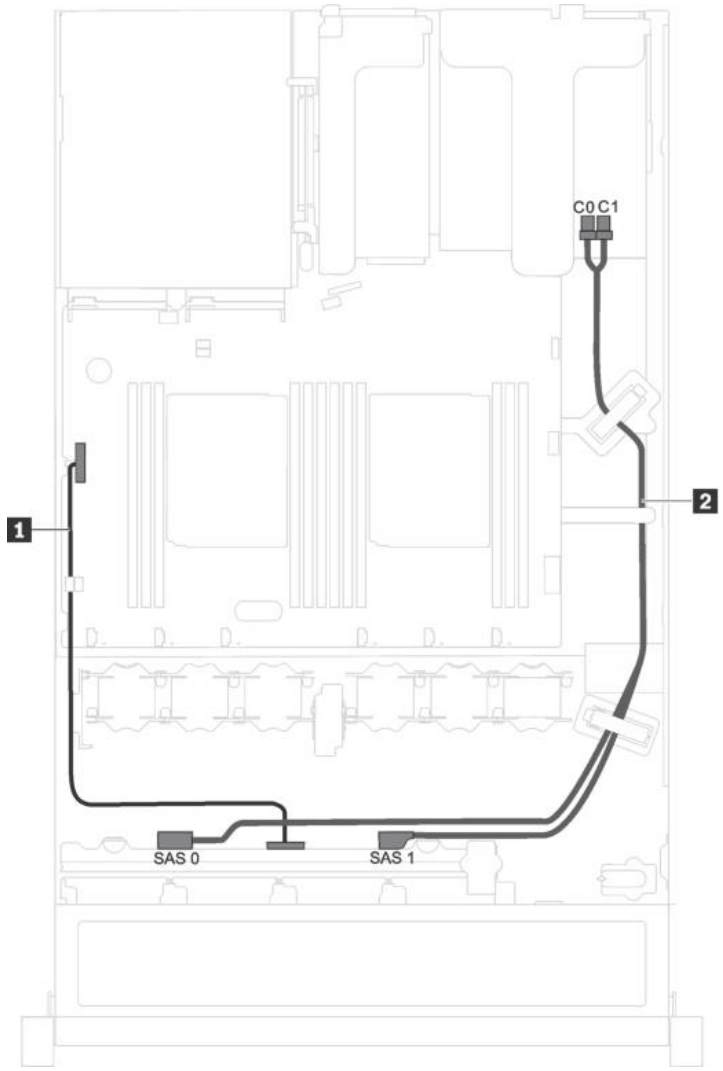


Figure 17. Cable routing for the server model with eight 2.5-inch hot-swap drives

Cable	From	To
1 Power cable	Power connector on the backplane	Backplane power connector on the system board
2 SAS signal cable	SAS 0 and SAS 1 connectors on the backplane	C0 and C1 connectors on the HBA/RAID adapter

Server model with four 3.5-inch hot-swap drives

Use this section to understand the internal cable routing for the server model with four 3.5-inch hot-swap drives.

The following illustration shows the cable routing for the server model with four 3.5-inch hot-swap drives.

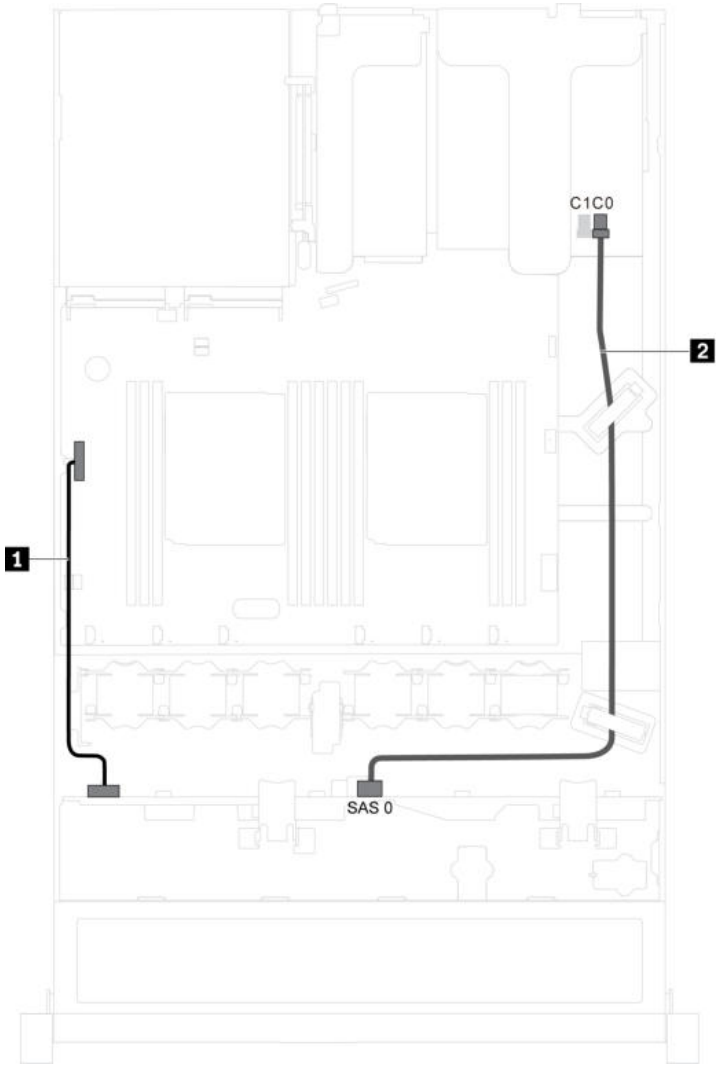


Figure 18. Cable routing for the server model with four 3.5-inch hot-swap drives

Cable	From	To
1 Power cable	Power connector on the backplane	Backplane power connector on the system board
2 SAS signal cable	SAS 0 connector on the backplane	C0 connector on the HBA/RAID adapter

Server model with four 3.5-inch simple-swap drives

Use this section to understand the internal cable routing for the server model with four 3.5-inch simple-swap drives.

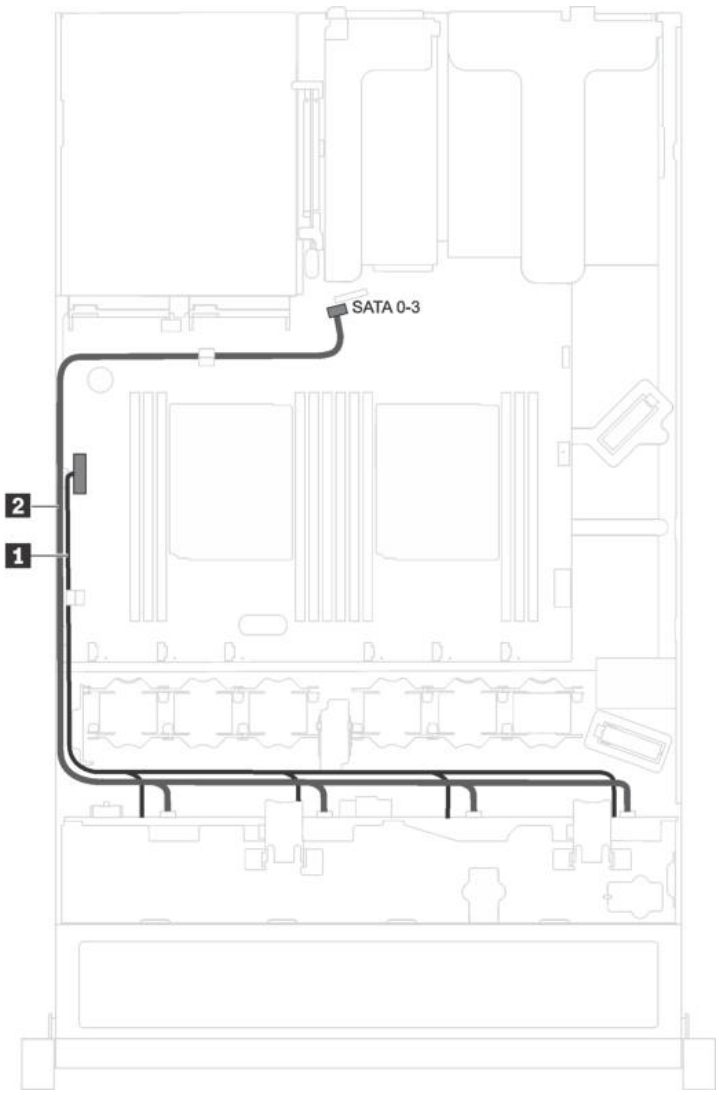


Figure 19. Cable routing for the server model with four 3.5-inch simple-swap drives

The simple-swap drive backplate assembly comes with a power cable and a SATA signal cable.

From	To
1 Power cable of the backplate assembly	Backplane power connector on the system board
2 SATA signal cable of the backplate assembly	SATA 0-3 connector on the system board

Parts list

Use the parts list to identify each of the components that are available for your server.

For more information about ordering the parts shown in Figure 20 “Server components” on page 36, go to:

http://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr530/7x07/parts

Note: Depending on the model, your server might look slightly different from the following illustration. Some of the components might not be available on your server.

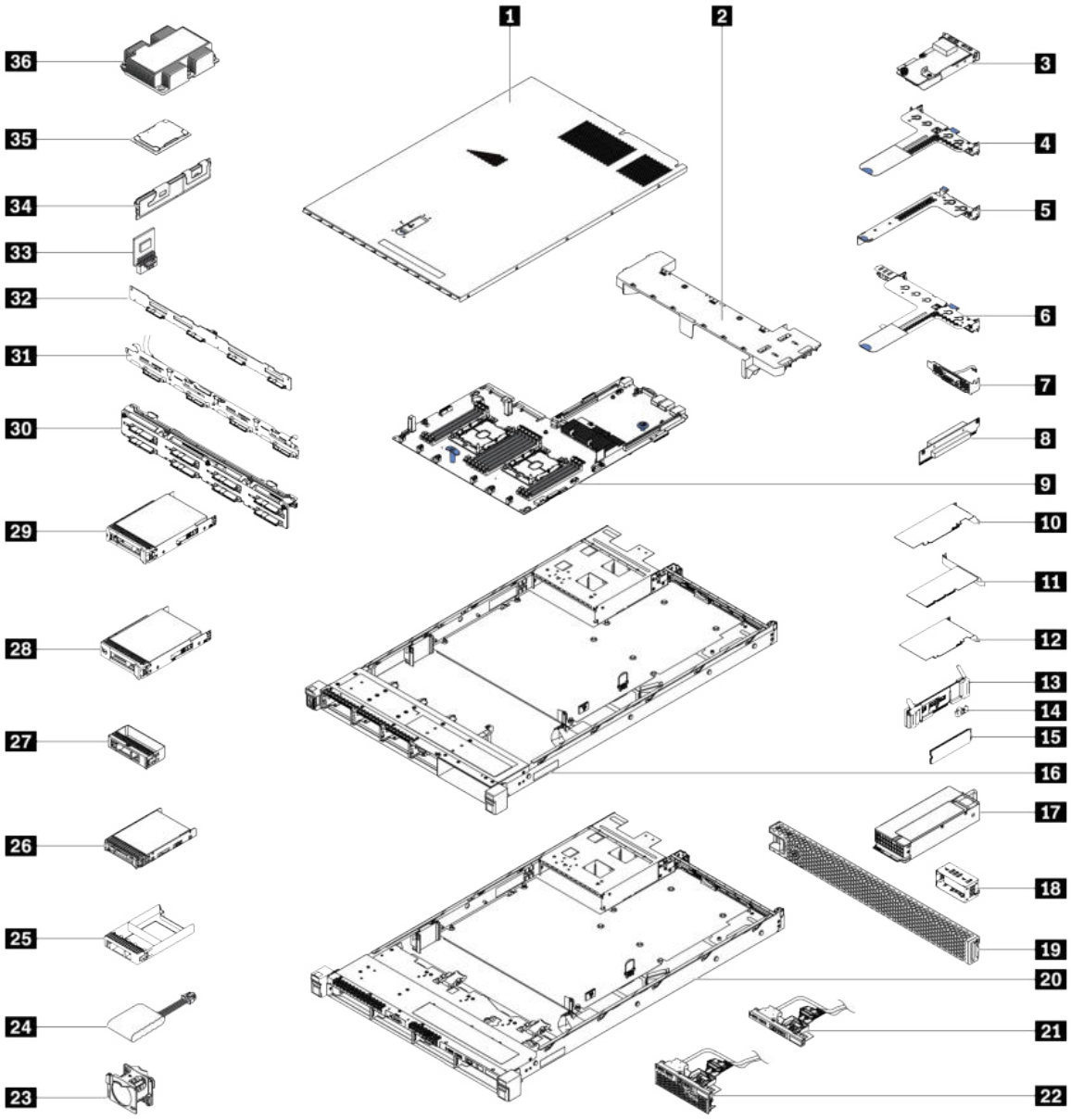


Figure 20. Server components

The parts listed in the following table are identified as one of the following:

- **Tier 1 customer replaceable unit (CRU):** Replacement of Tier 1 CRUs is your responsibility. If Lenovo installs a Tier 1 CRU at your request with no service agreement, you will be charged for the installation.
- **Tier 2 customer replaceable unit:** You may install a Tier 2 CRU yourself or request Lenovo to install it, at no additional charge, under the type of warranty service that is designated for your server.
- **Field replaceable unit (FRU):** FRUs must be installed only by trained service technicians.
- **Consumable and Structural parts:** Purchase and replacement of consumable and structural parts (components, such as a cover or bezel) is your responsibility. If Lenovo acquires or installs a structural component at your request, you will be charged for the service.

Table 9. Parts listing

Index	Description	Tier 1 CRU	Tier 2 CRU	FRU	Consumable and Structural parts
For more information about ordering the parts shown in Figure 20 “Server components” on page 36, go to: http://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr530/7x07/parts					
1	Top cover	√			
2	Air baffle				√
3	LOM adapter	√			
4	Riser 1 bracket (two low profile)	√			
5	Riser 2 bracket (one low profile)	√			
6	Riser 1 bracket (one low-profile and one full-height half-length)	√			
7	Serial port module	√			
8	Riser card	√			
9	System board			√	
10	Low-profile PCIe adapter	√			
11	ML2 adapter	√			
12	Full-height half-length PCIe adapter	√			
13	M.2 backplane	√			
14	M.2 retainer	√			
15	M.2 drive	√			
16	Chassis with eight 2.5-inch drive bays			√	
17	Power supply	√			
18	Power supply filler				√
19	Security bezel	√			
20	Chassis with four 3.5-inch drive bays			√	
21	Front I/O assembly for server models with 3.5-inch drive bays	√			
22	Front I/O assembly for server models with 2.5-inch drive bays	√			

Table 9. Parts listing (continued)

Index	Description	Tier 1 CRU	Tier 2 CRU	FRU	Consumable and Structural parts
23	System fan	√			
24	RAID super capacitor module	√			
25	2.5-inch drive filler				√
26	2.5-inch hot-swap drive	√			
27	3.5-inch drive filler				√
28	3.5-inch simple-swap drive	√			
29	3.5-inch hot-swap drive	√			
30	Backplane for eight hot-swap 2.5-inch drives	√			
31	Simple-swap drive backplate assembly	√			
32	Backplane for four hot-swap 3.5-inch drives	√			
33	TCM/TPM adapter (for Chinese Mainland only)			√	
34	DIMM	√			
35	Processor			√	
36	Processor heat sink			√	

Power cords

Several power cords are available, depending on the country and region where the server is installed.

To view the power cords that are available for the server:

1. Go to:

   http://dcsc.lenovo.com/#/
2. Click **Preconfigured Model** or **Configure to order**.
3. Enter the machine type and model for your server to display the configurator page.
4. Click **Power → Power Cables** to see all line cords.

Notes:

- For your safety, a power cord with a grounded attachment plug is provided to use with this product. To avoid electrical shock, always use the power cord and plug with a properly grounded outlet.
- Power cords for this product that are used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).
- For units intended to be operated at 115 volts: Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a parallel blade, grounding-type attachment plug rated 15 amperes, 125 volts.
- For units intended to be operated at 230 volts (U.S. use): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes, 250 volts.
- For units intended to be operated at 230 volts (outside the U.S.): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.
- Power cords for a specific country or region are usually available only in that country or region.

Chapter 3. Hardware replacement procedures

This section provides installation and removal procedures for all serviceable system components. Each component replacement procedure references any tasks that need to be performed to gain access to the component being replaced.

For more information about ordering parts, go to:

http://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr530/7x07/parts

Note: If you replace a part, such as an adapter, that contains firmware, you might also need to update the firmware for that part. For more information about updating firmware, see “Firmware updates” on page 7.

Installation Guidelines

Before installing components in your server, read the installation guidelines.

Before installing optional devices, read the following notices carefully:

Attention: Prevent exposure to static electricity, which might lead to system halt and loss of data, by keeping static-sensitive components in their static-protective packages until installation, and handling these devices with an electrostatic-discharge wrist strap or other grounding system.

- Read the safety information and guidelines to ensure that you work safely.
  - http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html
  - “Handling static-sensitive devices” on page 43
  - “Working inside the server with the power on” on page 43
- Make sure the components you are installing are supported by the server. For a list of supported optional components for the server, see http://www.lenovo.com/us/en/serverproven/.
- When you install a new server, download and apply the latest firmware. This will help ensure that any known issues are addressed, and that your server is ready to work with optimal performance. Go to ThinkSystem SR530 Drivers and Software to download firmware updates for your server.

  Important: Some cluster solutions require specific code levels or coordinated code updates. If the component is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.
- It is good practice to make sure that the server is working correctly before you install an optional component.
- Keep the working area clean, and place removed components on a flat and smooth surface that does not shake or tilt.
- Do not attempt to lift an object that might be too heavy for you. If you have to lift a heavy object, read the following precautions carefully:
  - Make sure that you can stand steadily without slipping.
  - Distribute the weight of the object equally between your feet.
  - Use a slow lifting force. Never move suddenly or twist when you lift a heavy object.
  - To avoid straining the muscles in your back, lift by standing or by pushing up with your leg muscles.
- Make sure that you have an adequate number of properly grounded electrical outlets for the server, monitor, and other devices.

© Copyright Lenovo 2017, 2020

- Back up all important data before you make changes related to the disk drives.
- Have a small flat-blade screwdriver, a small Phillips screwdriver, and a T8 torx screwdriver available.
- To view the error LEDs on the system board and internal components, leave the power on.
- You do not have to turn off the server to remove or install hot-swap power supplies, hot-swap fans, or hot-plug USB devices. However, you must turn off the server before you perform any steps that involve removing or installing adapter cables, and you must disconnect the power source from the server before you perform any steps that involve removing or installing a riser card.
- Blue on a component indicates touch points, where you can grip to remove a component from or install it in the server, open or close a latch, and so on.
- Orange on a component or an orange label on or near a component indicates that the component can be hot-swapped if the server and operating system support hot-swap capability, which means that you can remove or install the component while the server is still running. (Orange can also indicate touch points on hot-swap components.) See the instructions for removing or installing a specific hot-swap component for any additional procedures that you might have to perform before you remove or install the component.
- The Red strip on the drives, adjacent to the release latch, indicates that the drive can be hot-swapped if the server and operating system support hot-swap capability. This means that you can remove or install the drive while the server is still running.

  Note: See the system specific instructions for removing or installing a hot-swap drive for any additional procedures that you might need to perform before you remove or install the drive.
- After finishing working on the server, make sure you reinstall all safety shields, guards, labels, and ground wires.

System reliability guidelines

Review the system reliability guidelines to ensure proper system cooling and reliability.

Make sure the following requirements are met:

- When the server comes with redundant power, a power supply must be installed in each power-supply bay.
- Adequate space around the server must be spared to allow server cooling system to work properly. Leave approximately 50 mm (2.0 in.) of open space around the front and rear of the server. Do not place any object in front of the fans.
- For proper cooling and airflow, refit the server cover before you turn the power on. Do not operate the server for more than 30 minutes with the server cover removed, for it might damage server components.
- Cabling instructions that come with optional components must be followed.
- A failed fan must be replaced within 48 hours since malfunction.
- A removed hot-swap fan must be replaced within 30 seconds after removal.
- A removed hot-swap drive must be replaced within two minutes after removal.
- A removed hot-swap power supply must be replaced within two minutes after removal.
- Every air baffle that comes with the server must be installed when the server starts (some servers might come with more than one air baffle). Operating the server with a missing air baffle might damage the processor.
- All processor sockets must contain either a socket cover or a processor with heat sink.
- When more than one processor is installed, fan population rules for each server must be strictly followed.

Working inside the server with the power on

You might need to keep the power on with the server cover removed to look at system information on the display panel or to replace hot-swap components. Review these guidelines before doing so.

Attention: The server might stop and loss of data might occur when internal server components are exposed to static electricity. To avoid this potential problem, always use an electrostatic-discharge wrist strap or other grounding systems when working inside the server with the power on.

- Avoid loose-fitting clothing, particularly around your forearms. Button or roll up long sleeves before working inside the server.
- Prevent your necktie, scarf, badge rope, or long hair from dangling into the server.
- Remove jewelry, such as bracelets, necklaces, rings, cuff links, and wrist watches.
- Remove items from your shirt pocket, such as pens and pencils, in case they fall into the server as you lean over it.
- Avoid dropping any metallic objects, such as paper clips, hairpins, and screws, into the server.

Handling static-sensitive devices

Review these guidelines before you handle static-sensitive devices to reduce the possibility of damage from electrostatic discharge.

Attention: Prevent exposure to static electricity, which might lead to system halt and loss of data, by keeping static-sensitive components in their static-protective packages until installation, and handling these devices with an electrostatic-discharge wrist strap or other grounding system.

- Limit your movement to prevent building up static electricity around you.
- Take additional care when handling devices during cold weather, for heating would reduce indoor humidity and increase static electricity.
- Always use an electrostatic-discharge wrist strap or other grounding system, particularly when working inside the server with the power on.
- While the device is still in its static-protective package, touch it to an unpainted metal surface on the outside of the server for at least two seconds. This drains static electricity from the package and from your body.
- Remove the device from the package and install it directly into the server without putting it down. If it is necessary to put the device down, put it back into the static-protective package. Never place the device on the server or on any metal surface.
- When handling a device, carefully hold it by the edges or the frame.
- Do not touch solder joints, pins, or exposed circuitry.
- Keep the device from others' reach to prevent possible damages.

Rack latches replacement

Use this information to remove and install the rack latches.

Remove the rack latches

Use this information to remove the rack latches.



"**Read** the installation Guidelines" on page 41

Before removing the rack latches:

1. If you have installed the security bezel, remove it. See "Remove the security bezel" on page 48.
2. Use a flat-blade screwdriver to remove the ID label plate on the right rack latch and place it in a safe place.

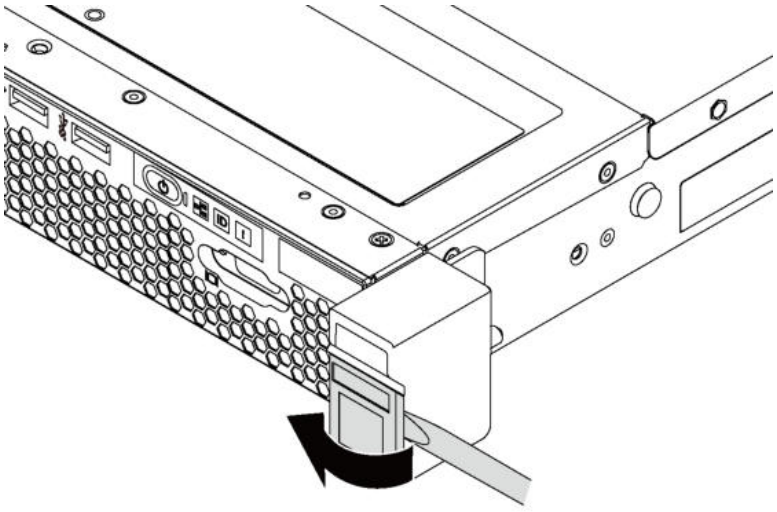


Figure 21. ID label plate removal

To remove the rack latches, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. On each side of the server, remove the two screws that secure the rack latch.

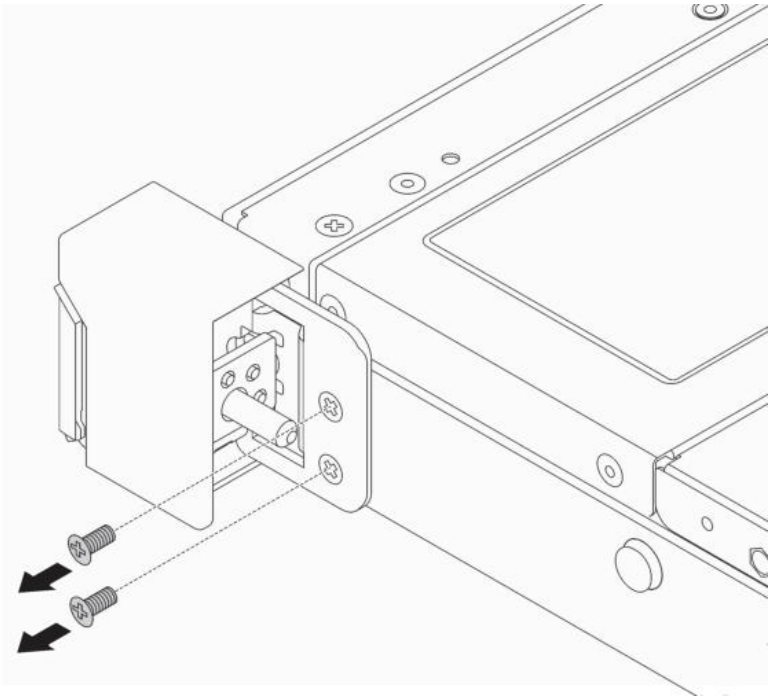


Figure 22. Rack latch screws removal

Step 2. On each side of the server, remove the rack latch from the chassis as shown.

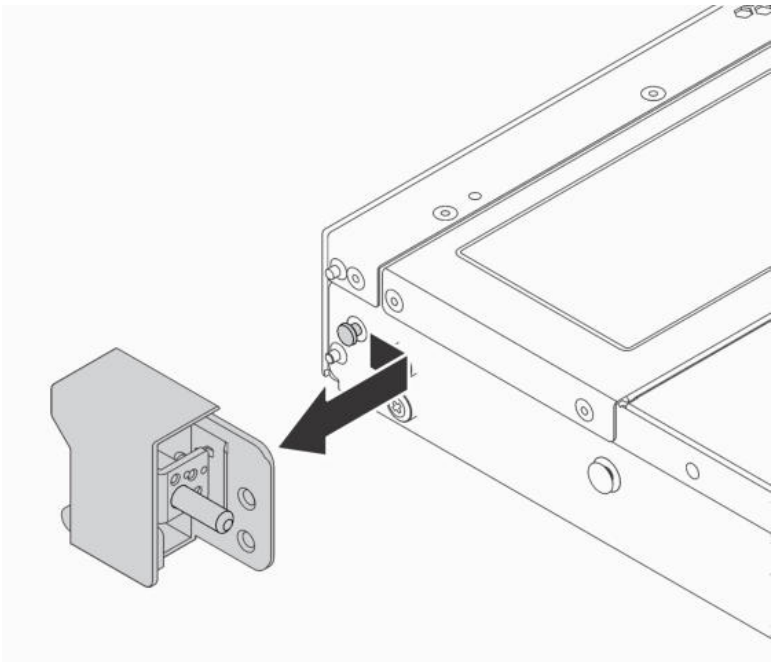


Figure 23. Rack latch removal

If you are instructed to return the old rack latches, follow all packaging instructions and use any packaging materials that are provided.

Install the rack latches

Use this information to install the rack latches.

"**Read** the installation Guidelines" on page 41

To install the rack latches, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. On each side of the server, align the rack latch with the pin on the chassis; then, press the rack latch onto the chassis and slightly slide it forward as shown.

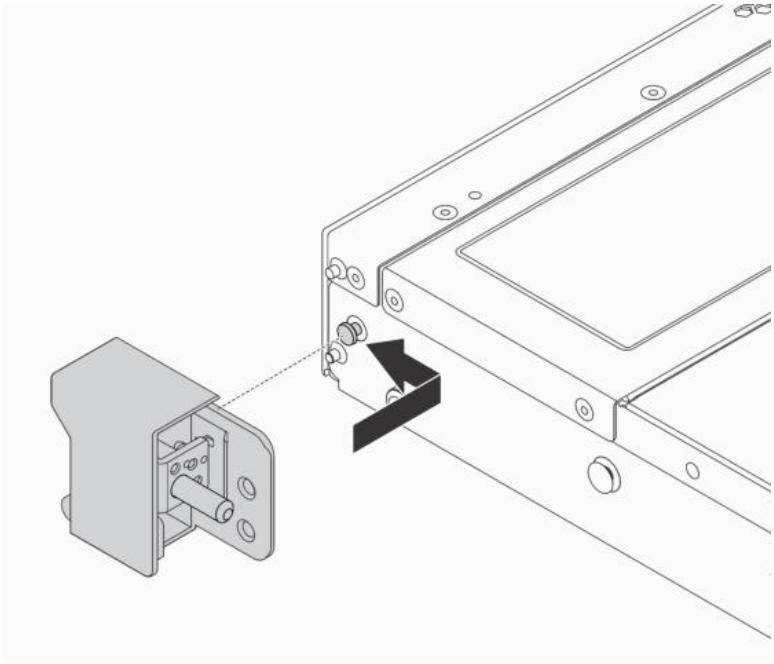


Figure 24. Rack latch installation

Step 2. Install the two screws to secure the rack latch on each side of the server.

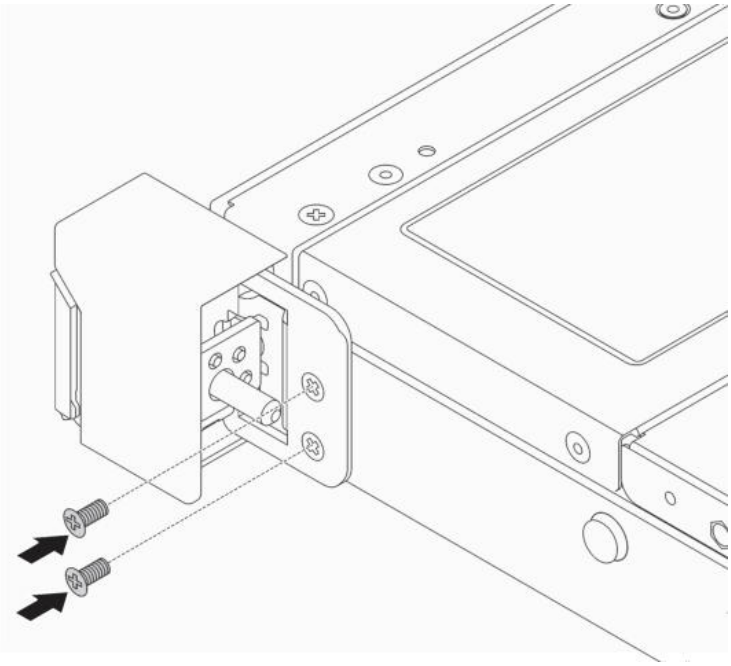


Figure 25. Rack latch screws installation

After installing the rack latches:

1. Install the ID label plate to the right rack latch as shown.

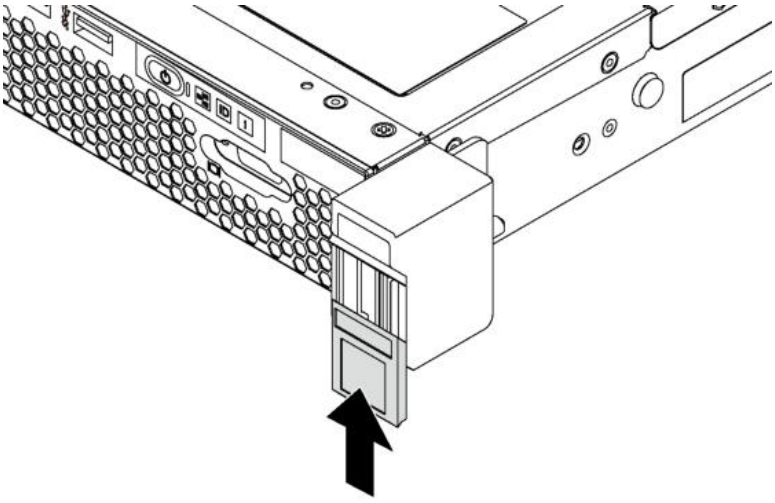


Figure 26. ID label plate installation

2. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Security bezel replacement

Use this information to remove and install the security bezel.

Remove the security bezel

Use this information to remove the security bezel.



"**Read** the installation Guidelines" on page 41

To remove the security bezel, complete the following steps:

Step 1. Use the key to unlock the security bezel.

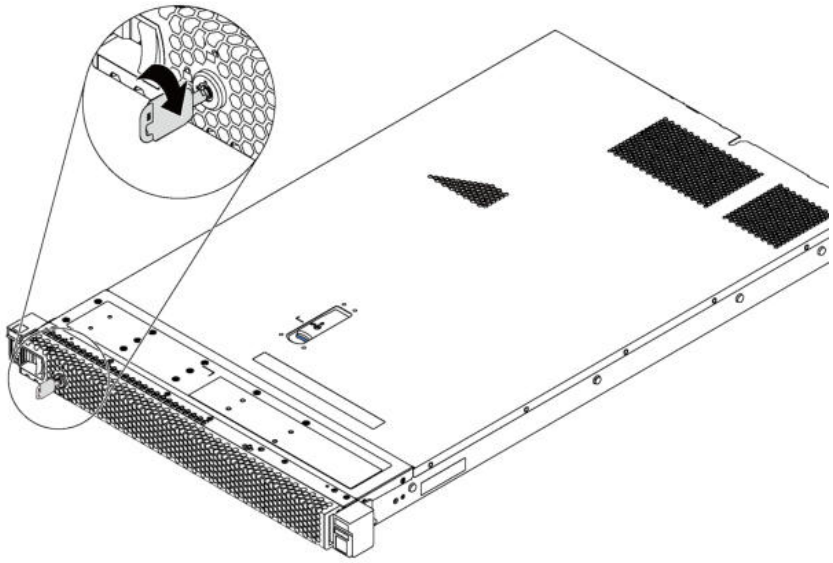


Figure 27. Security bezel unlock

Step 2. Press the blue release latch 1 and pivot the security bezel outward to remove it from the chassis.

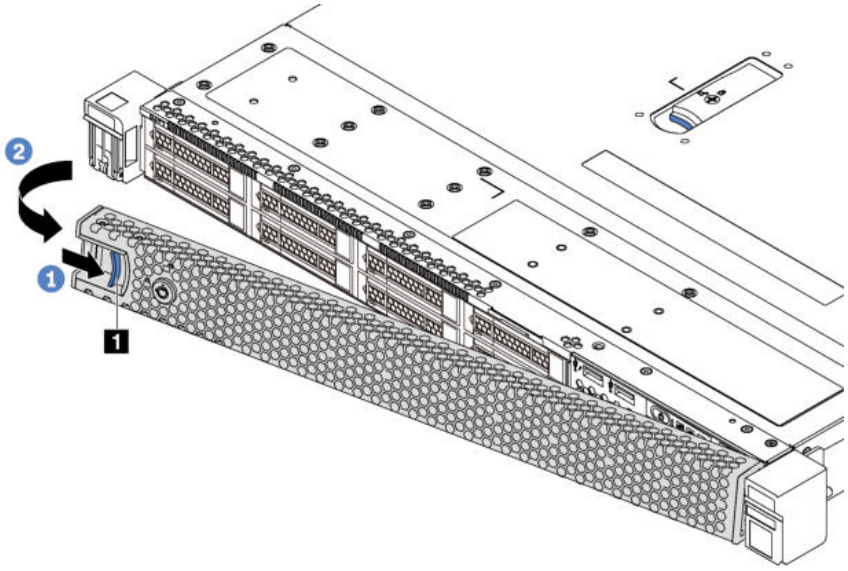


Figure 28. Security bezel removal

Attention: Before you ship the rack with the server installed, reinstall and lock the security bezel into place.

Install the security bezel

Use this information to install the security bezel.



"**Read** the installation Guidelines" on page 41

Attention: Before you ship the rack with the server installed, install and lock the security bezel into place.

Before installing the security bezel, if you have removed the rack latches, reinstall them. See "Install the rack latches" on page 46.

To install the security bezel, complete the following steps:

Step 1. If the key is held inside the security bezel, remove it out of the security bezel.

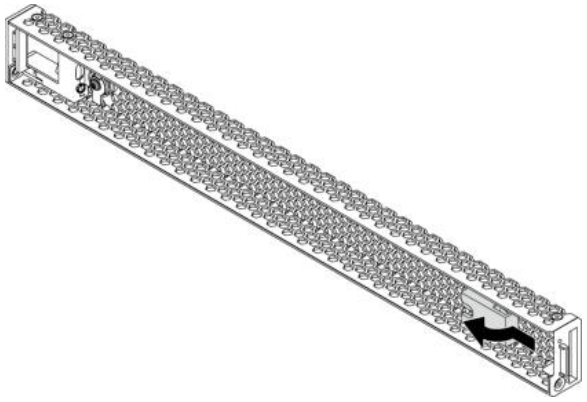


Figure 29. Key removal

Step 2. Insert the tab on the security bezel into the slot on the right side of the chassis. Then, press the blue release latch 1 and pivot the security bezel inward until it clicks into place.

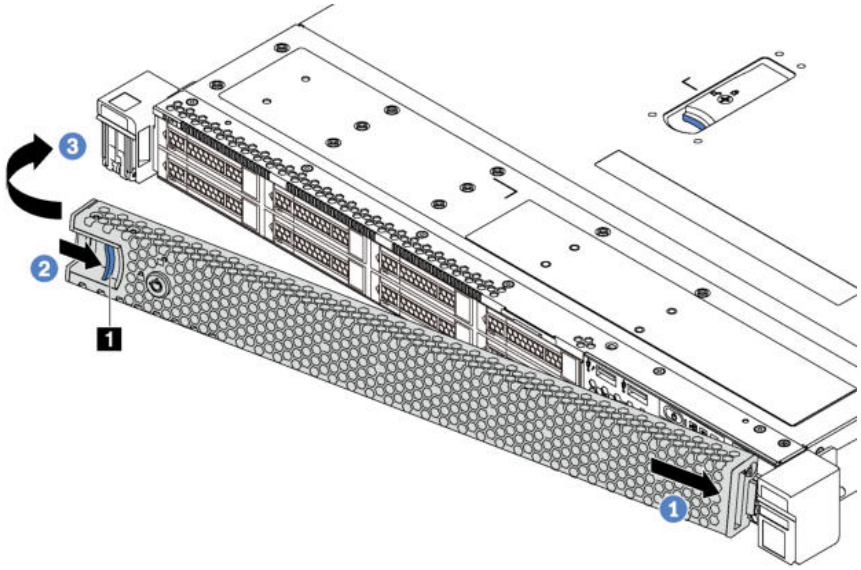


Figure 30. Security bezel installation

Step 3. Use the key to lock the security bezel.

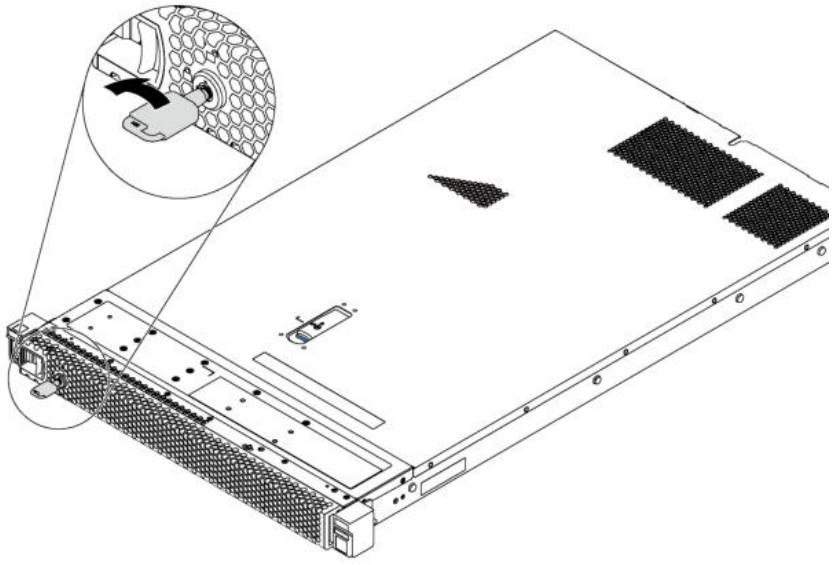


Figure 31. Security bezel lockup

Top cover replacement

Use this information to remove and install the top cover.

S033



CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

S014



CAUTION:
Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the label is attached.

Remove the top cover

Use this information to remove the top cover.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

To remove the top cover, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

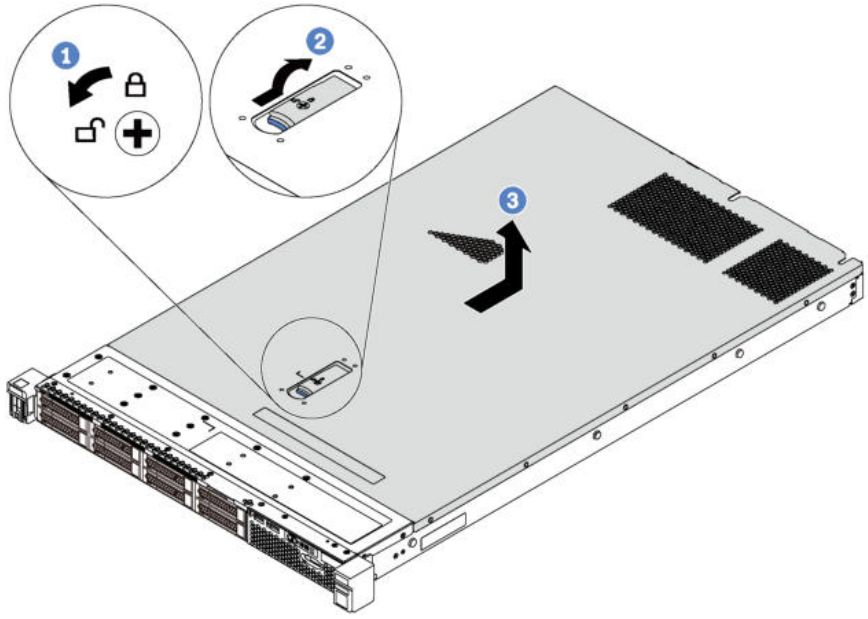


Figure 32. Top cover removal

Step 1. Use a screwdriver to turn the cover lock to the open position.

Step 2. Press the blue button on the cover latch and open the cover latch.

Step 3. Slide the cover to the rear until it is disengaged from the chassis. Then, lift the cover off the chassis and place it on a flat clean surface.

Attention:

- Handle the top cover carefully. Dropping the top cover with the cover latch open might damage the cover latch.
- For proper cooling and airflow, install the top cover before you power on the server.

Install the top cover

Use this information to install the top cover.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the top cover:

1. Ensure that all cables, adapters, and other components are installed and seated correctly and that you have not left loose tools or parts inside the server.
2. Ensure that all internal cables are correctly routed. See “Internal cable routing” on page 28.
3. If you are installing a new top cover, attach the service label to the new top cover first if necessary.

   Note: A new top cover comes without a service label attached. If you need a service label, order it together with the new top cover. The service label is free of charge.

To install the top cover, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

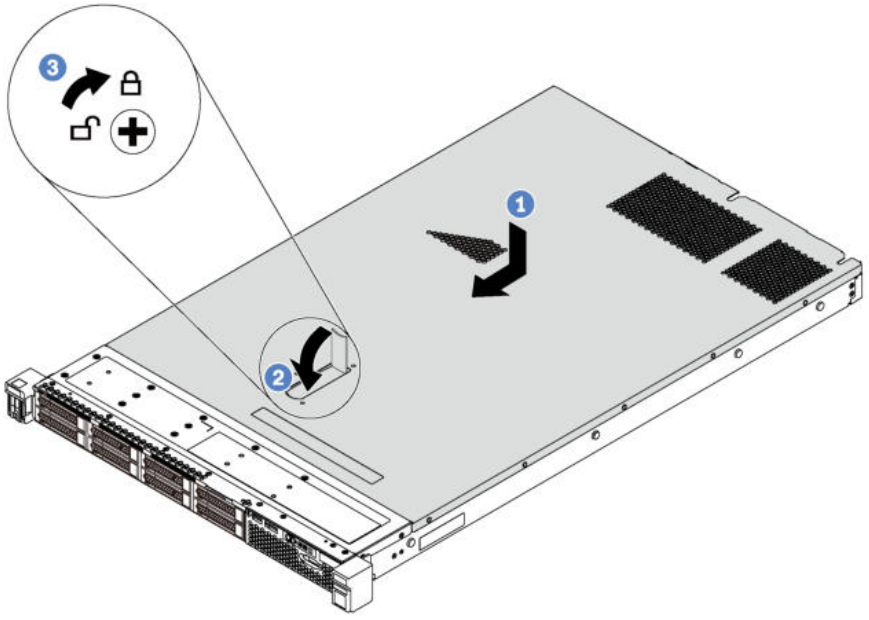


Figure 33. Top cover installation

Note: Before you slide the top cover forward, ensure that all the tabs on the top cover engage the chassis correctly. If the tabs do not engage the chassis correctly, it will be very difficult to remove the top cover later.

Step 1. Ensure that the cover latch is in the open position. Lower the cover onto the chassis until all tabs on both sides of the cover engage with the guides on both sides of the chassis.

Step 2. Pivot the cover latch and slide the cover forward until the cover snaps into position. Ensure that the cover latch is completely closed.

Step 3. Use a screwdriver to turn the cover lock to the closed position.

After installing the top cover, complete the parts replacement. See “Complete the parts replacement” on page 143.

Air baffle replacement

Use this information to remove and install the air baffle

S033



CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

S017



CAUTION:
Hazardous moving fan blades nearby. Keep fingers and other body parts away.

Remove the air baffle

Use this information to remove the air baffle.



“**Read** the installation Guidelines” on page 41



“**Power off** the server for this task” on page 11

To remove the air baffle, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

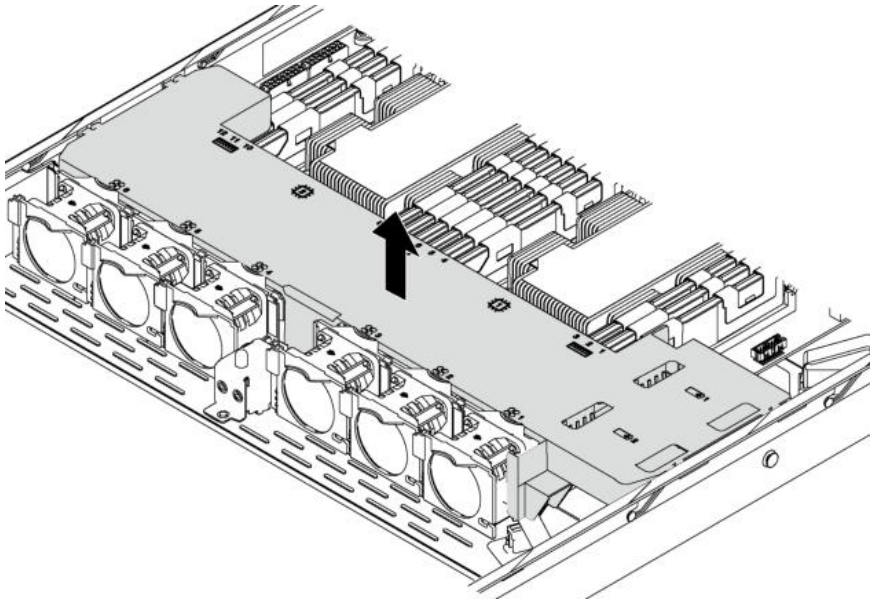


Figure 34. Air baffle removal

Step 1. Remove the top cover. See “Remove the top cover” on page 52.

Step 2. If the server has a RAID super capacitor module installed underneath the air baffle, disconnect its cable from the extension cable.

Step 3. Grasp the air baffle and carefully lift it out of the server.

Attention: For proper cooling and airflow, install the air baffle before you power on the server. Operating the server without an air baffle might damage server components.

Install the air baffle

Use this information to install the air baffle.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11

Before installing the air baffle:

1. Ensure that the retaining clips on each end of the DIMM connectors are closed.
2. If you want to install a RAID super capacitor module, install it onto the air baffle first. See "Install a RAID super capacitor module" on page 60.

To install the air baffle, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

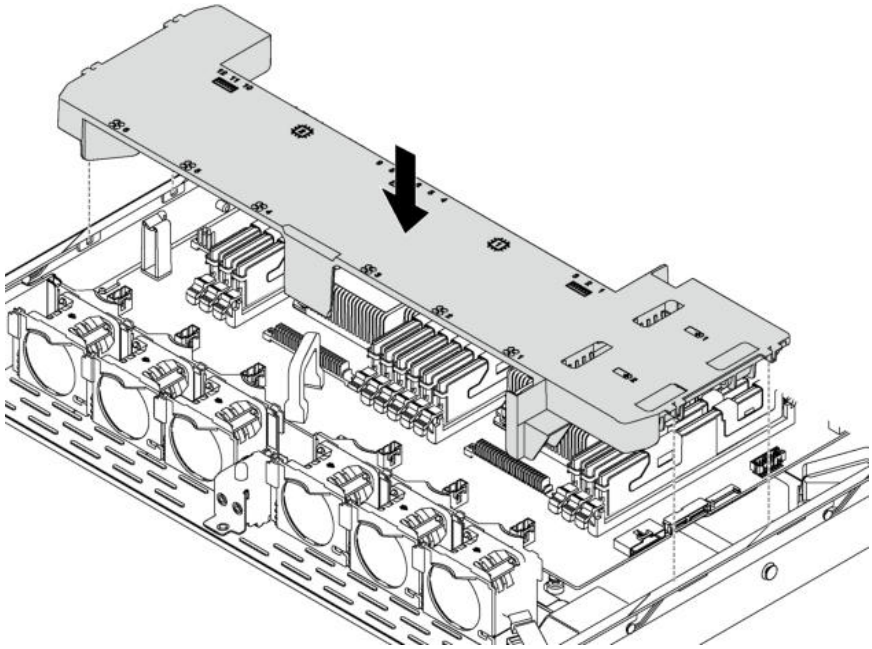


Figure 35. Air baffle installation

Step 1. Align the tabs on both sides of the air baffle with the corresponding slots on both sides of the chassis.

Step 2. Lower the air baffle into the server and press the air baffle down until it is securely seated.

After installing the air baffle:

1. If you have installed a RAID super capacitor module, connect it to the RAID adapter using the extension cable that comes with the RAID super capacitor module. See "Internal cable routing" on page 28.
2. Complete the parts replacement. See "Complete the parts replacement" on page 143.

RAID super capacitor module replacement

Use this information to remove and install a RAID super capacitor module.

Your server supports up to two RAID super capacitor modules. The RAID super capacitor holders are located underneath the air baffle.

Remove a RAID super capacitor module

Use this information to remove a RAID super capacitor module.

		
“**Read** the installation Guidelines” on page 41	“**Power off** the server for this task” on page 11	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing the RAID super capacitor module:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Locate the RAID super capacitor module, and disconnect its cable. The RAID super capacitor holders are located underneath the air baffle.
3. Remove the air baffle and turn it over. See “Remove the air baffle” on page 55.

To remove the RAID super capacitor module, complete the following steps:

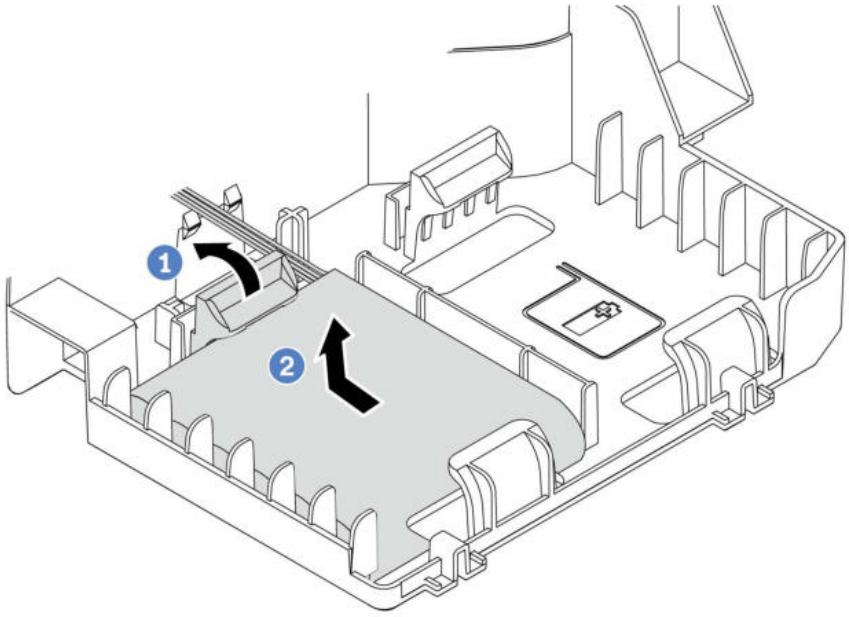


Figure 36. RAID super capacitor module removal

Step 1. Gently pivot the retaining clip as shown.

Step 2. Lift the RAID super capacitor up and remove it from the holder.

If you are instructed to return the old RAID super capacitor module, follow all packaging instructions and use any packaging materials that are provided.

Install a RAID super capacitor module

If your server has a RAID adapter with a super capacitor connector, you can install a RAID super capacitor module in your server.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11
	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43	

Before installing the RAID super capacitor module:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Remove the air baffle and turn it over. See “Remove the air baffle” on page 55.
3. Locate the RAID super capacitor holder.
4. Touch the static-protective package that contains the new RAID super capacitor module to any unpainted surface on the outside of the server. Then, take the new RAID super capacitor module out of the package and place it on a static-protective surface.

To install the RAID super capacitor module, complete the following steps:

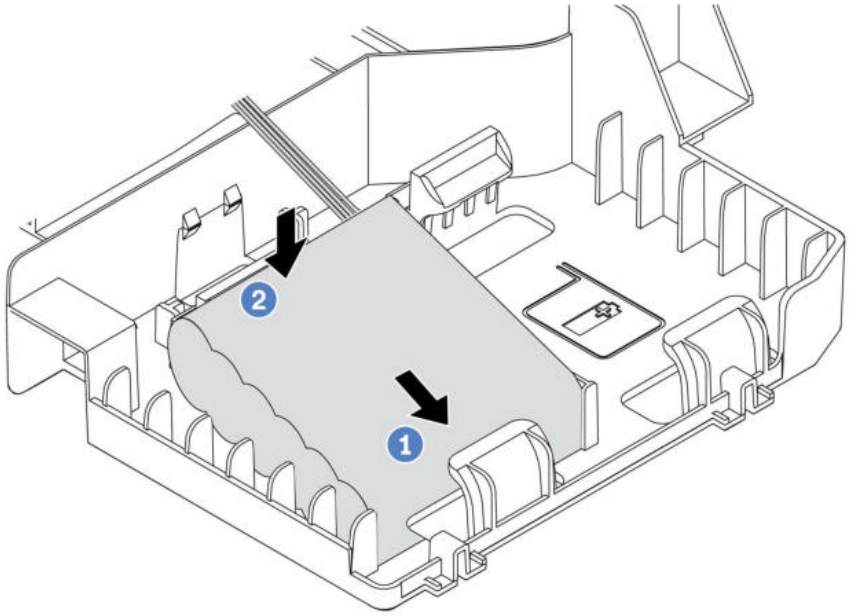


Figure 37. RAID super capacitor module installation

Step 1. Insert the RAID super capacitor module into the retaining clip at one side as shown.

Step 2. Press the RAID super capacitor module down on the other side until it snaps into place.

Step 3. Connect the RAID super capacitor module to the RAID adapter using an extension cable. See “Internal cable routing” on page 28.

Step 4. If your server has two RAID adapters each with a super capacitor connector, you can continue to install the second RAID super capacitor module.

After installing the RAID super capacitor module, complete the parts installation. See “Complete the parts replacement” on page 143.

System fan replacement

Use this information to remove and install a system fan.

S033



CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

S009



CAUTION:
To avoid personal injury, disconnect the fan cables before removing the fan from the device.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

Remove a system fan

Use this information to remove a system fan.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing a system fan:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Remove the air baffle. See “Remove the air baffle” on page 55.

To remove a system fan, complete the following steps:

Watch the procedure. A video of the removal process is available:

- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

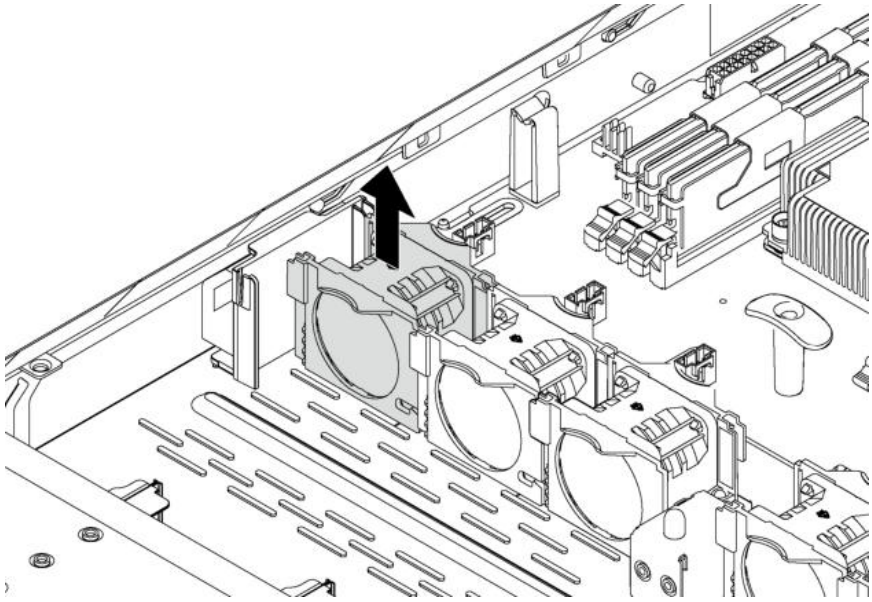


Figure 38. System fan removal

Step 1. Disconnect the system fan cable from the system board.

Step 2. Grasp the system fan with your index finger and thumb and carefully lift it straight up.

After removing the system fan:

1. Install a new fan to cover the fan bay.
2. If you are instructed to return the old system fan, follow all packaging instructions and use any packaging materials that are provided.

Install a system fan

Use this information to install a system fan.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before installing a system fan, touch the static-protective package that contains the new system fan to any unpainted surface on the outside of the server. Then, take the new system fan out of the package and place it on a static-protective surface.

To install a system fan, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

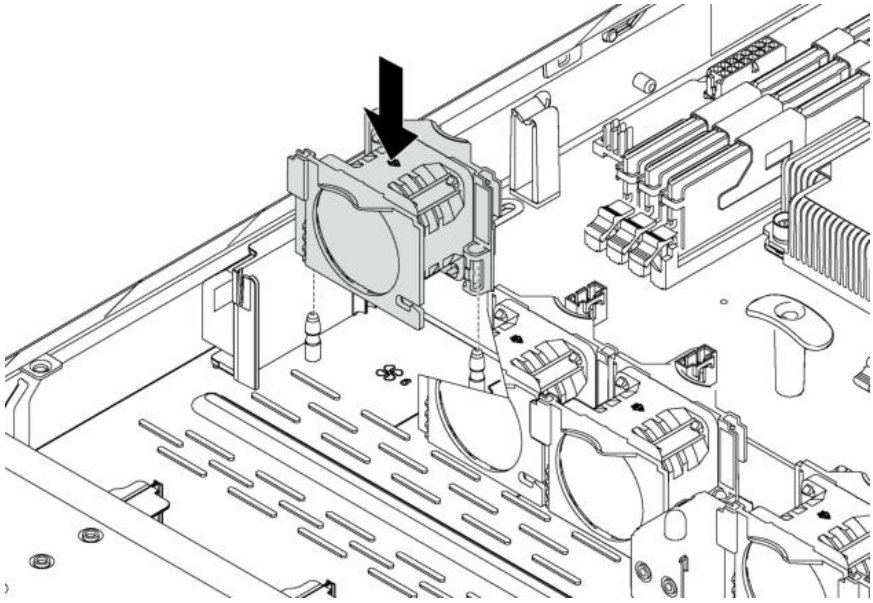


Figure 39. System fan installation

Step 1. Align the support holes of the system fan with the two pins in the chassis, and press it straight down until it is seated into place.

Note: Ensure that the system fan cable is at the side next to the system board.

Step 2. Connect the system fan cable to the system fan connector on the system board.

After installing the system fan, complete the parts replacement. See "Complete the parts replacement" on page 143.

Front I/O assembly replacement

Use this information to remove and install the front I/O assembly.

Remove the front I/O assembly

Use this information to remove the front I/O assembly.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11
	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43	

Before removing the front I/O assembly:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. If the security bezel is installed, remove it. See “Remove the security bezel” on page 48.
3. Disconnect cables of the front I/O assembly from the system board.

To remove the front I/O assembly, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Table 10. Front I/O assembly removal

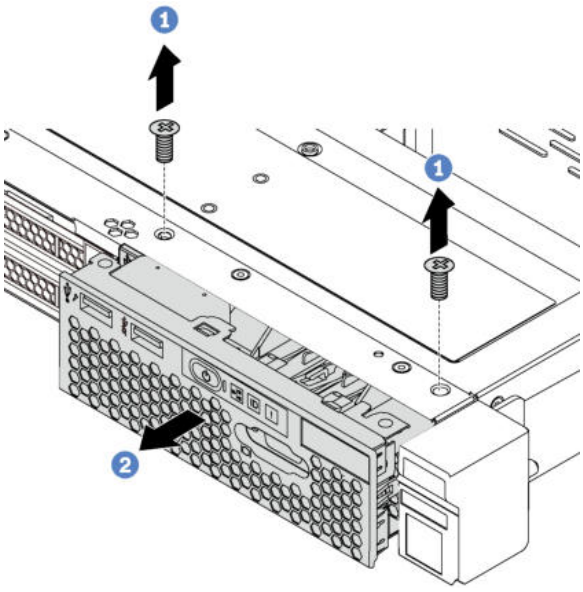


Figure 40. Server models with 2.5-inch drive bays

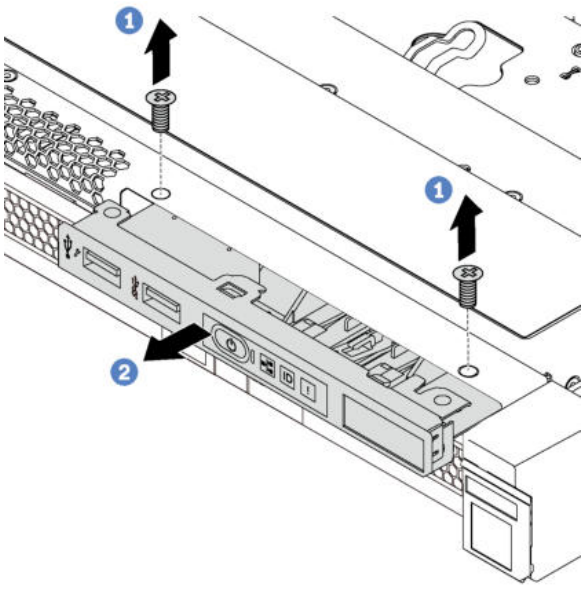


Figure 41. Server models with 3.5-inch drive bays

Step 1. Remove the screws that secure the front I/O assembly.

Step 2. Slide the front I/O assembly out of the assembly bay.

If you are instructed to return the old front I/O assembly, follow all packaging instructions and use any packaging materials that are provided.

Install the front I/O assembly

Use this information to install the front I/O assembly.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the front I/O assembly, touch the static-protective package that contains the new front I/O assembly to any unpainted surface on the outside of the server. Then, take new the front I/O assembly out of the package and place it on a static-protective surface.

To install the front I/O assembly, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Table 11. Front I/O assembly installation

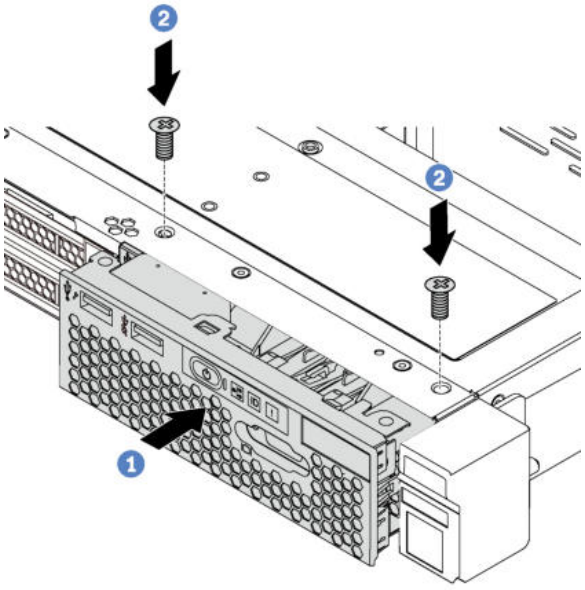


Figure 42. Server models with 2.5-inch drive bays

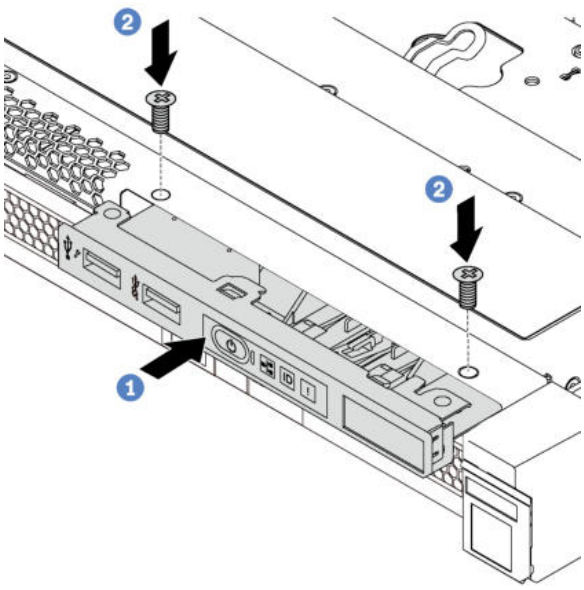


Figure 43. Server models with 3.5-inch drive bays

Step 1. Insert the front I/O assembly into the assembly bay.

Step 2. Install the screws to secure the front I/O assembly in place.

Step 3. Connect the cables of the front I/O assembly to the system board. See “Internal cable routing” on page 28.

After installing the front I/O assembly, complete the parts replacement. See “Complete the parts replacement” on page 143.

Hot-swap drive backplane replacement

Use this information to remove and install the hot-swap drive backplane.

Remove the backplane for four 3.5-inch hot-swap drives

Use this information to remove the backplane for four 3.5-inch hot-swap drives.

	"**Read** the installation Guidelines" on page 41	 "**Power off** the server for this task" on page 11	 "**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the backplane:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. Record the cable connections on the backplane and then disconnect cables from the backplane.
3. Remove all the installed drives and drive fillers (if any) from the drive bays. See "Remove a hot-swap drive" on page 73.

To remove the backplane, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

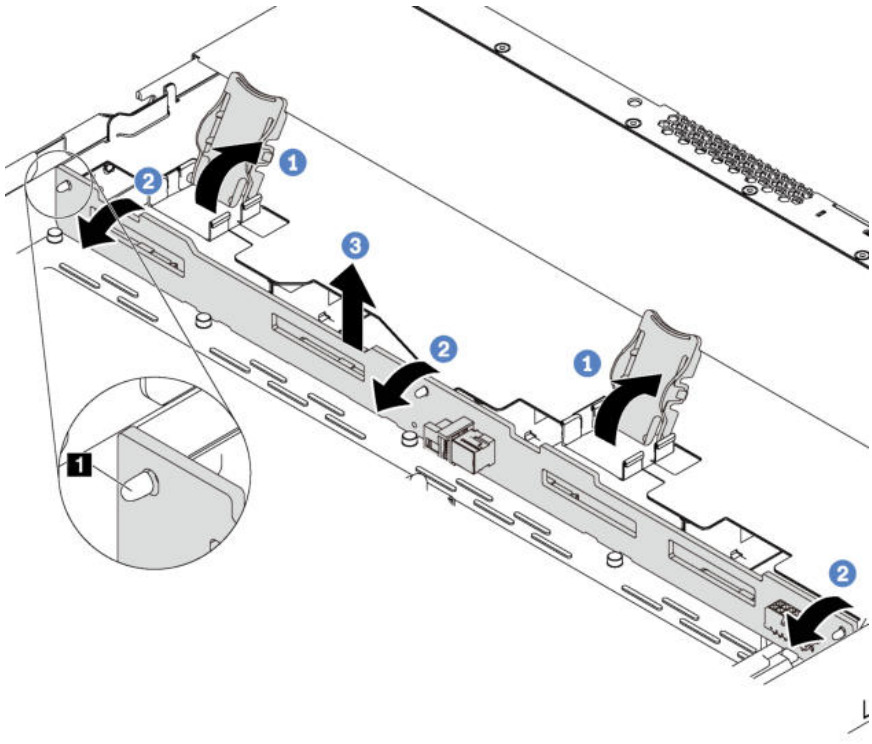


Figure 44. Backplane removal

Step 1. Open the release latches that secure the backplane.

Step 2. Pivot the backplane backward slightly to release it from the three pins 1 on the chassis.

Step 3. Carefully remove the backplane out of the chassis from under the front I/O assembly cables.

If you are instructed to return the old backplane, follow all packaging instructions and use any packaging materials that are provided.

Install the backplane for four 3.5-inch hot-swap drives

Use this information to install the backplane for four 3.5-inch hot-swap drives.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before installing the backplane, touch the static-protective package that contains the new backplane to any unpainted surface on the outside of the server. Then, take the new backplane out of the package and place it on a static-protective surface.

To install the backplane, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

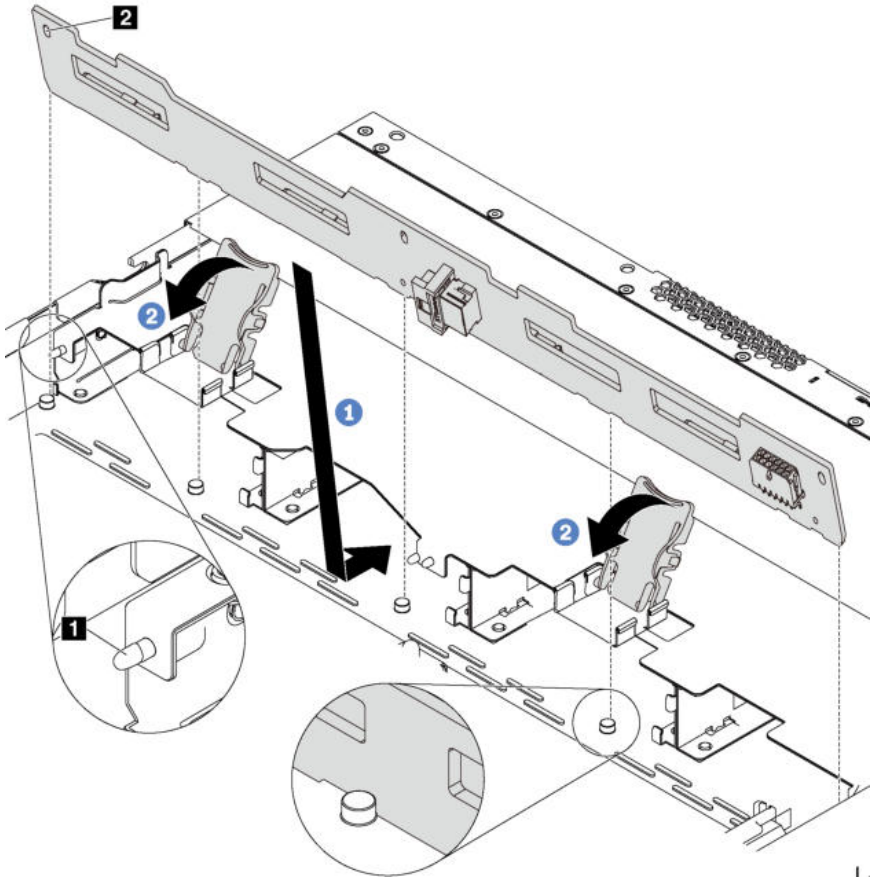


Figure 45. Backplane installation

Step 1. Put the backplane under the front I/O assembly cables, align it with the chassis, and lower it into the chassis. Put the backplane into place with it leaning backward slightly so that the three pins 1 on the chassis pass through the three holes 2 in the backplane.

Step 2. Close the release latches to secure the backplane in place.

After installing the backplane:

1. Connect cables to the backplane. See “Internal cable routing” on page 28.
2. Reinstall all the drives and drive fillers that you removed. See “Install a hot-swap drive” on page 74.
3. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Remove the backplane for eight 2.5-inch hot-swap drives

Use this information to remove the backplane for eight 2.5-inch hot-swap drives.



“**Read** the installation Guidelines” on page 41



“**Power off** the server for this task” on page 11



“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing the backplane:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Record the cable connections on the backplane and then disconnect cables from the backplane.
3. Remove all the installed drives and drive fillers (if any) from the drive bays. See “Remove a hot-swap drive” on page 73.

To remove the backplane, complete the following step:

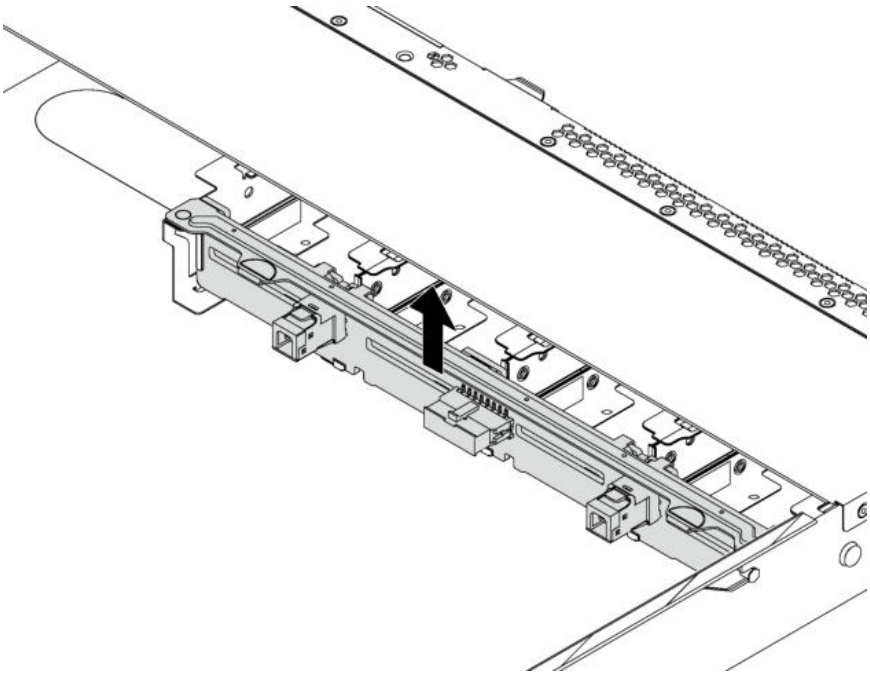


Figure 46. Backplane removal

Step 1. Grasp the backplane and carefully lift it out of the chassis.

If you are instructed to return the old backplane, follow all packaging instructions and use any packaging materials that are provided.

Install the backplane for eight 2.5-inch hot-swap drives

Use this information to install the backplane for eight 2.5-inch hot-swap drives.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the backplane, touch the static-protective package that contains the new backplane to any unpainted surface on the outside of the server. Then, take the new backplane out of the package and place it on a static-protective surface.

To install the backplane, complete the following steps:

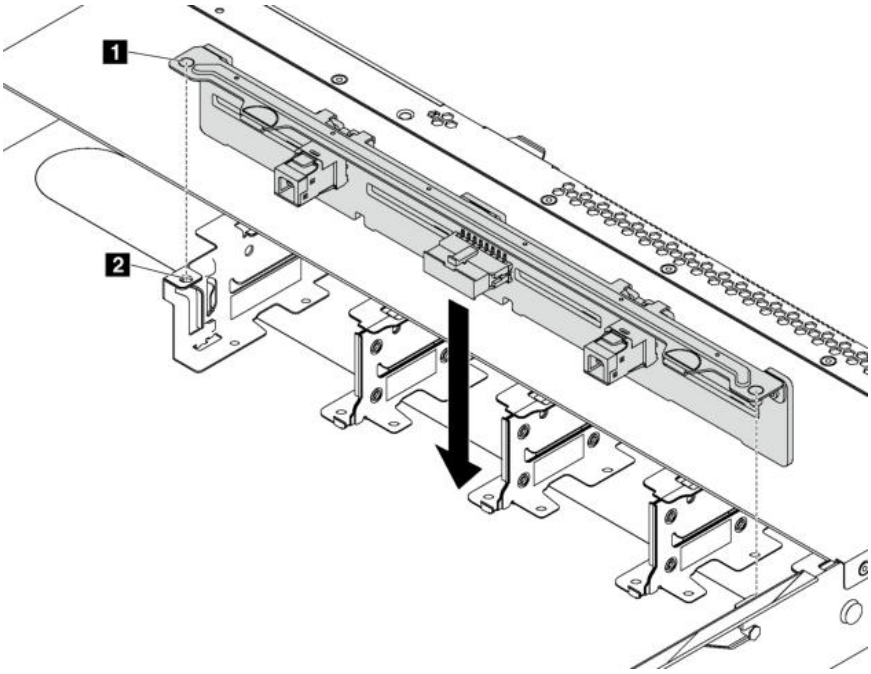


Figure 47. Backplane installation

Step 1. Align pins 1 on the backplane with the holes 2 in the chassis.

Step 2. Lower the backplane into the chassis. Ensure that the pins pass through the holes and the backplane is fully seated in place.

After installing the backplane:

1. Connect cables to the backplane. See “Internal cable routing” on page 28.
2. Reinstall all the drives and drive fillers that you removed. See “Install a hot-swap drive” on page 74.
3. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Simple-swap drive backplate assembly replacement

Use this information to remove and install the simple-swap drive backplate assembly.

Remove the simple-swap drive backplate assembly

Use this information to remove the simple-swap drive backplate assembly.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the simple-swap drive backplate assembly:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. Record the cable connections and disconnect cables of the simple-swap drive backplate assembly.
3. Remove all the installed drives and drive fillers (if any) from the drive bays. See "Remove a simple-swap drive" on page 76.

To remove the simple-swap drive backplate assembly, complete the following steps:

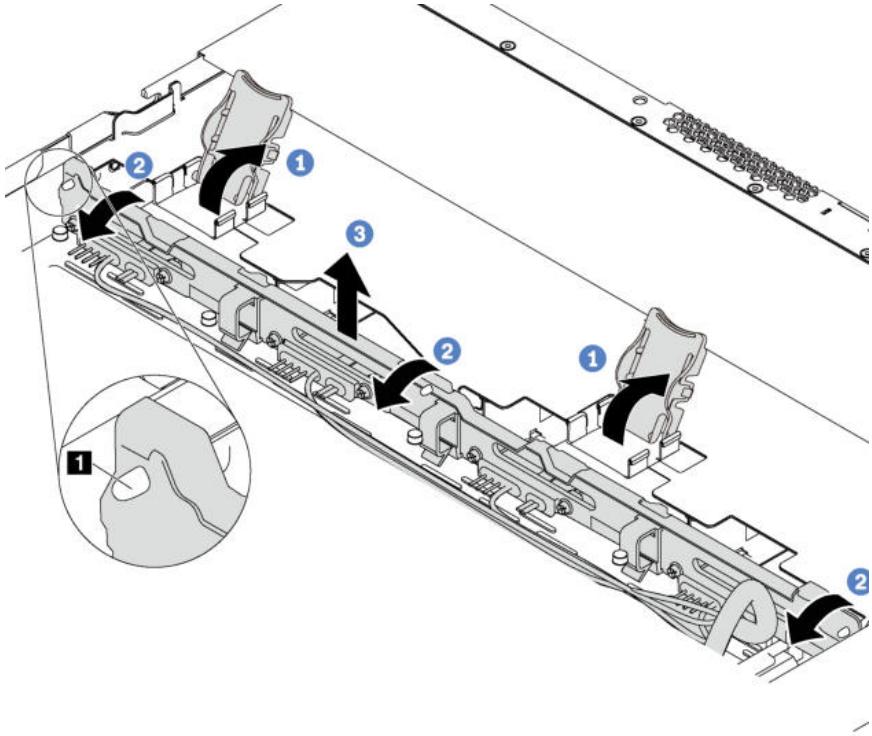


Figure 48. Simple-swap drive backplate assembly removal

Step 1. Open the release latches that secure the simple-swap drive backplate assembly.

Step 2. Pivot the simple-swap drive backplate assembly backward slightly to release it from the three pins 1 on the chassis.

Step 3. Carefully remove the backplate assembly out of the chassis from under the front I/O assembly cables.

If you are instructed to return the old simple-swap drive backplate assembly, follow all packaging instructions and use any packaging materials that are provided.

Install the simple-swap drive backplate assembly

Use this information to install the simple-swap drive backplate assembly.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the simple-swap drive backplate assembly, touch the static-protective package that contains the new backplate assembly to any unpainted surface on the outside of the server. Then, take the new backplate assembly out of the package and place it on a static-protective surface.

To install the simple-swap drive backplate assembly, complete the following steps:

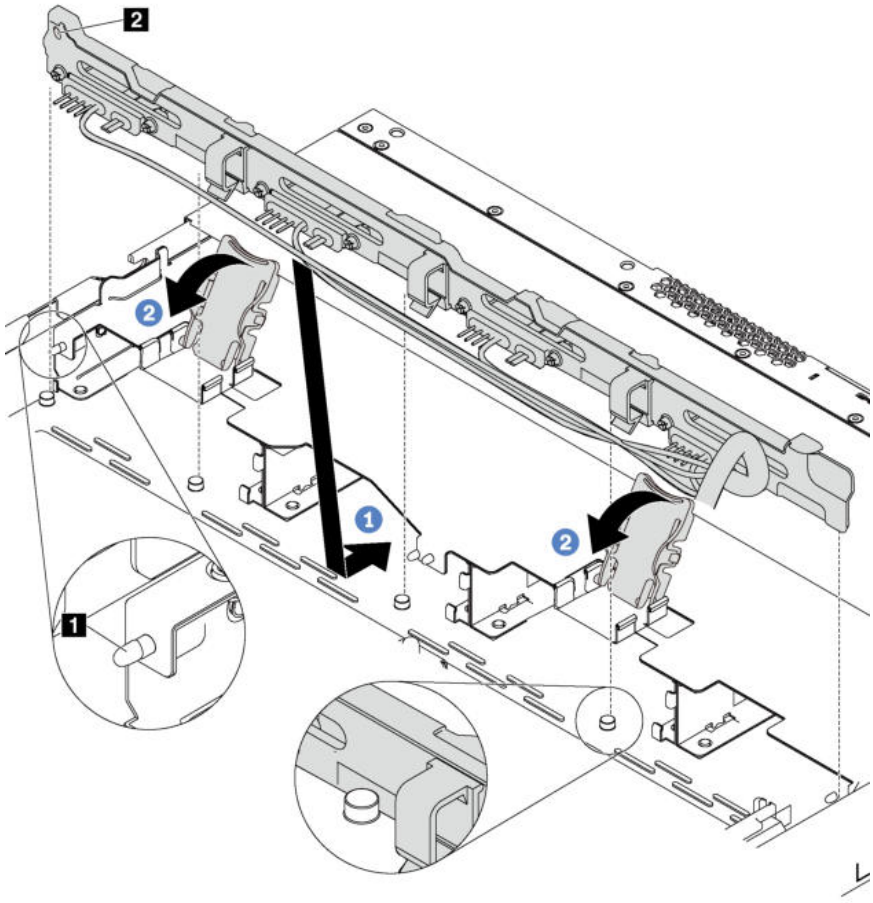


Figure 49. Simple-swap drive backplate assembly installation

Step 1. Put the backplate assembly under the front I/O assembly cables, align it with the chassis, and lower it into the chassis. Put the backplate assembly into place with it leaning backward slightly so that the three pins 1 on the chassis pass through the three holes 2 in the assembly.

Step 2. Close the release latches to secure the backplate assembly in place.

After installing the simple-swap drive backplate assembly:

1. Connect cables of the simple-swap drive backplate assembly to the system board. See “Internal cable routing” on page 28.
2. Reinstall all the drives and drive fillers that you removed. See “Install a simple-swap drive” on page 78.
3. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Hot-swap drive replacement

Use this information to remove and install a hot-swap drive. You can remove or install a hot-swap drive without powering off the server, which helps you avoid significant interruption to the operation of the system.

Notes:

- The term “hot-swap drive” refers to all the supported types of hot-swap hard disk drives (HDDs) and hot-swap solid-state drives (SSDs).
- Use any documentation that comes with the drive and follow those instructions in addition to the instructions in this topic. Ensure that you have all the cables and other equipment that are specified in the documentation that comes with the drive.
- The electromagnetic interference (EMI) integrity and cooling of the server are protected by having all drive bays covered or occupied. The vacant bays are either covered by an EMI-protective panel or occupied by drive fillers. When installing a drive, save the removed drive filler in case that you later remove the drive and need the drive filler to cover the place.
- To avoid damage to the drive connectors, ensure that the top cover is in place and fully closed whenever you install or remove a drive.

Remove a hot-swap drive

Use this information to remove a hot-swap drive.



“**Read** the installation Guidelines” on page 41



“**ATTENTION:**
Static Sensitive Device
Ground package before opening” on page 43

Before removing a hot-swap drive:

1. Ensure that you have back up data on your drive, especially if it is part of a RAID array.
   - Before you make changes to drives, drive controllers, drive backplanes, or drive cables, back up all important data that is stored on the drives.
   - Before you remove any component of a RAID array, back up all RAID configuration information.
2. Remove the security bezel. See “Remove the security bezel” on page 48.

Attention: To ensure that there is adequate system cooling, do not operate the server for more than two minutes without either a drive or a drive filler installed in each bay.

To remove a hot-swap drive, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Slide the release latch to the left to open the drive tray handle.

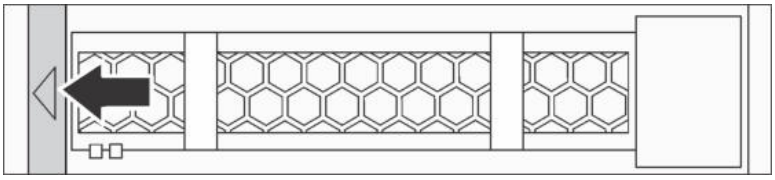


Figure 50. Opening the drive tray handle

Step 2. Grasp the handle and slide the drive out of the drive bay.

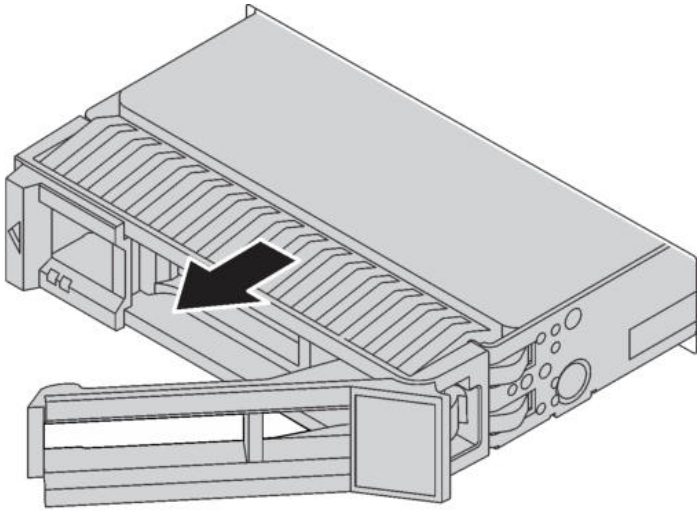


Figure 51. Sliding the drive out of the drive bay

Step 3. Install a drive filler or a new drive to cover the drive bay.

If you are instructed to return the old drive, follow all packaging instructions and use any packaging materials that are provided.

Install a hot-swap drive

Use this information to install a hot-swap drive.



"**Read** the installation Guidelines" on page 41



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Notes:

- For a list of supported drives, see http://www.lenovo.com/us/en/serverproven/.
- The drive bays are numbered to indicate the installation order (starting from number "0"). Follow the installation order when you install a drive. See "Front view" on page 13.
- You can mix drives of different types and different capacities in one system, but not in one RAID array. The following order is recommended when installing the drives:

  - Drive type priority: SAS SSD, SATA SSD, SAS HDD, SATA HDD
  - Drive capacity priority: the lowest capacity first
- The drives in a single RAID array must be the same type, same size, and same capacity.

Before installing a hot-swap drive:

1. If there is a drive filler installed, remove it and keep it in a safe place.
2. Touch the static-protective package that contains the new drive to any unpainted surface on the outside of the server. Then, take the new drive out of the package and place it on a static-protective surface.

To install a hot-swap drive, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

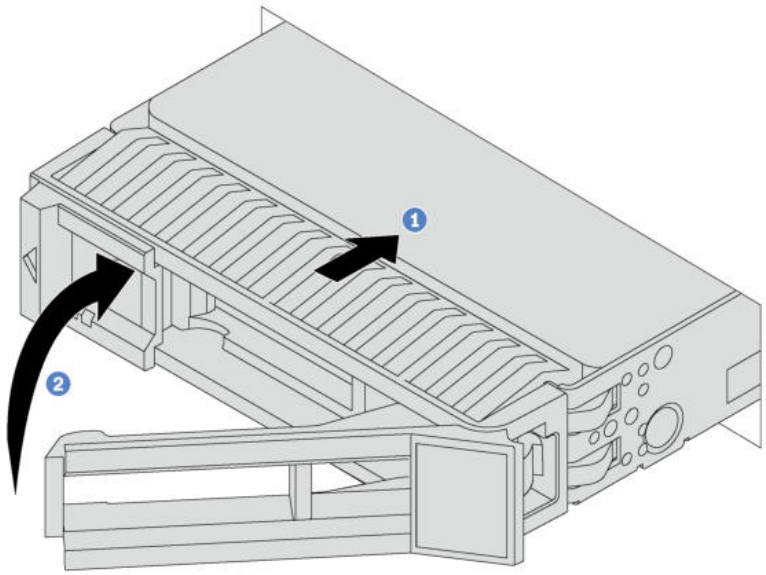


Figure 52. Hot-swap drive installation

Step 1. Ensure that the drive tray handle is in the open position. Slide the drive into the drive bay until it snaps into position.

Step 2. Close the drive tray handle to lock the drive in place.

Step 3. Check the drive status LED to verify that the drive is operating correctly.
- If the yellow drive status LED is lit continuously, that drive is faulty and must be replaced.
- If the green drive activity LED is flashing, the drive is being accessed.

Step 4. Continue to install additional hot-swap drives if necessary.

After installing all drives:

1. Reinstall the security bezel. See “Install the security bezel” on page 50.
2. Use the Lenovo XClarity Provisioning Manager to configure the RAID if necessary. For more information, see:

http://sysmgt.lenovofiles.com/help/topic/LXPM/RAID_setup.html

Simple-swap drive replacement

Use this information to remove and install a simple-swap drive.

Notes:

- The term “simple-swap drive” refers to all the supported types of simple-swap hard disk drives (HDDs) and simple-swap solid-state drives (SSDs).
- You must power off the server before installing or replacing a simple-swap drive.
- Use any documentation that comes with the drive and follow those instructions in addition to the instructions in this topic. Ensure that you have all the cables and other equipment that are specified in the documentation that comes with the drive.
- The electromagnetic interference (EMI) integrity and cooling of the server are protected by having all drive bays covered or occupied. The vacant bays are either covered by an EMI-protective panel or occupied by drive fillers. When installing a drive, save the removed drive filler in case that you later remove the drive and need the drive filler to cover the place.
- To avoid damage to the drive connectors, ensure that the top cover is in place and fully closed whenever you install or remove a drive.

Remove a simple-swap drive

Use this information to remove a simple-swap drive.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing a simple-swap drive:

1. Ensure that you have back up data on your drive, especially if it is part of a RAID array.
   - Before you make changes to drives, drive controllers, drive backplanes, or drive cables, back up all important data that is stored on the drives.
   - Before you remove any component of a RAID array, back up all RAID configuration information.
2. Remove the security bezel. See “Remove the security bezel” on page 48.

Attention: To make sure that there is adequate system cooling, do not operate the server for more than two minutes without either a drive or a drive filler installed in each bay.

To remove a simple-swap drive, complete the following steps:

Step 1. Use a screwdriver to unlock the handle lock 1. The handle opens automatically.

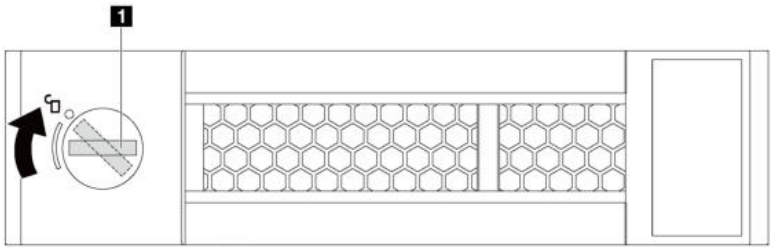


Figure 53. Opening the drive tray handle

Step 2. Grasp the handle and slide the drive out of the drive bay.

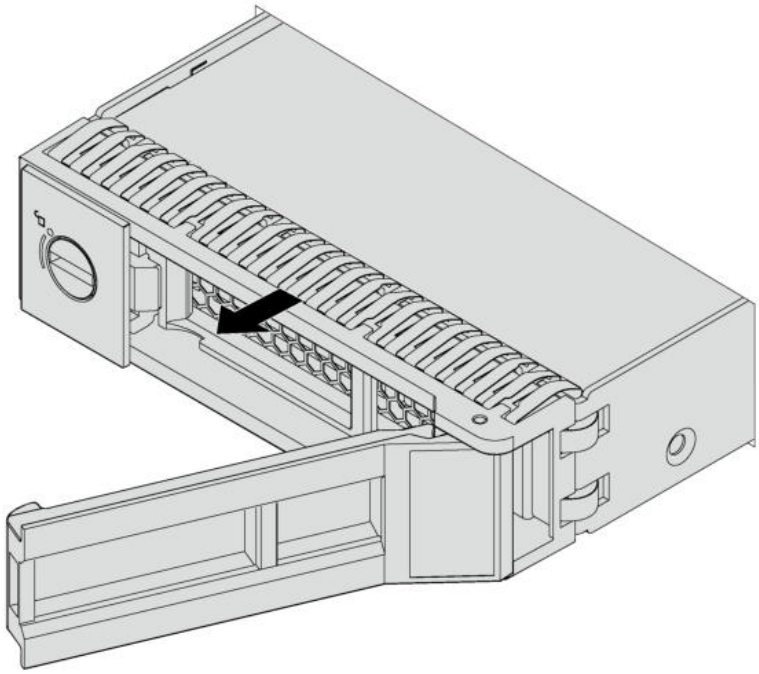


Figure 54. Sliding the drive out of the drive bay

Step 3. Install a drive filler or a new drive to cover the drive bay.

If you are instructed to return the old drive, follow all packaging instructions and use any packaging materials that are provided.

Install a simple-swap drive

Use this information to install a simple-swap drive.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Notes:

- For a list of supported drives, see http://www.lenovo.com/us/en/serverproven/.
- The drive bays are numbered to indicate the installation order (starting from number “0”). Follow the installation order when you install a drive. See “Front view” on page 13.
- You can mix drives of different types and different capacities in one system, but not in one RAID array. The following order is recommended when installing the drives:
  - Drive type priority: SATA SSD, SATA HDD
  - Drive capacity priority: the lowest capacity first
- The drives in a single RAID array must be the same type, same size, and same capacity.

Before installing a simple-swap drive:

1. If there is a drive filler installed, remove it and keep it in a safe place.
2. Touch the static-protective package that contains the new drive to any unpainted surface on the outside of the server. Then, take the new drive out of the package and place it on a static-protective surface.

To install a simple-swap drive, complete the following steps:

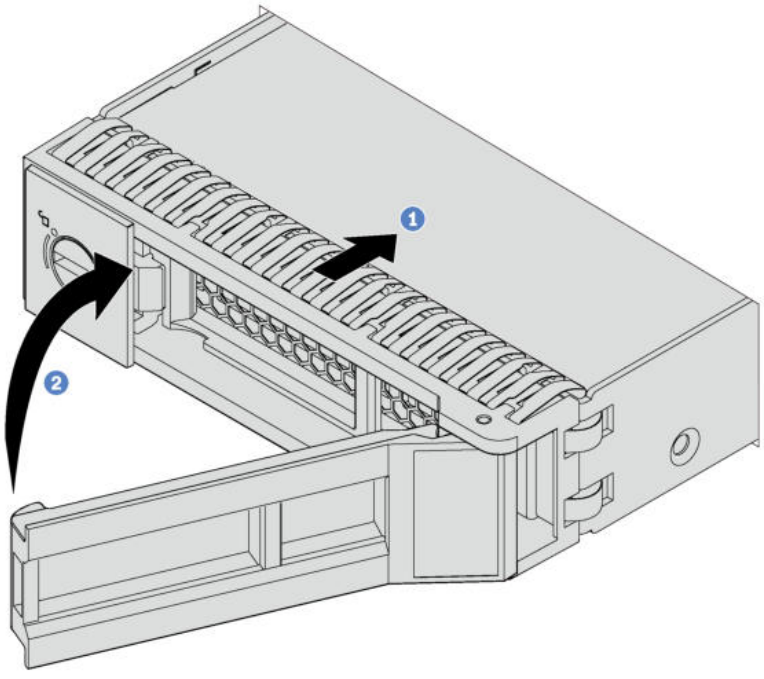


Figure 55. Simple-swap drive installation

Step 1. Ensure that the drive tray handle is in the open position. Slide the drive into the drive bay until it snaps into position.

Step 2. Close the drive tray handle to lock the drive in place.

Step 3. Continue to install additional simple-swap drives if necessary.

After you have installed all drives:

1. Reinstall the security bezel. See “Install the security bezel” on page 50.
2. Power on the server.
3. Use the Lenovo XClarity Provisioning Manager to configure the RAID if necessary. For more information, see:
   http://sysmgt.lenovofiles.com/help/topic/LXPM/RAID_setup.html

Memory module replacement

Use this information to remove and install a memory module.

Remove a memory module

Use this information to remove a memory module.



“**Read** the installation Guidelines” on page 41



“**Power off** the server for this task” on page 11



“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Attention:

- Disconnect all power cords for this task.
- Memory modules are sensitive to static discharge and require special handling. In addition to the standard guidelines for “Handling static-sensitive devices” on page 43:
  - Always wear an electrostatic-discharge strap when removing or installing memory modules. Electrostatic-discharge gloves can also be used.
  - Never hold two or more memory modules together so that they touch. Do not stack memory modules directly on top of each other during storage.
  - Never touch the gold memory module connector contacts or allow these contacts to touch the outside of the memory module connector housing.
  - Handle memory modules with care: never bend, twist, or drop a memory module.

Before removing a memory module:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Remove the air baffle. See “Remove the air baffle” on page 55.

To remove a memory module, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

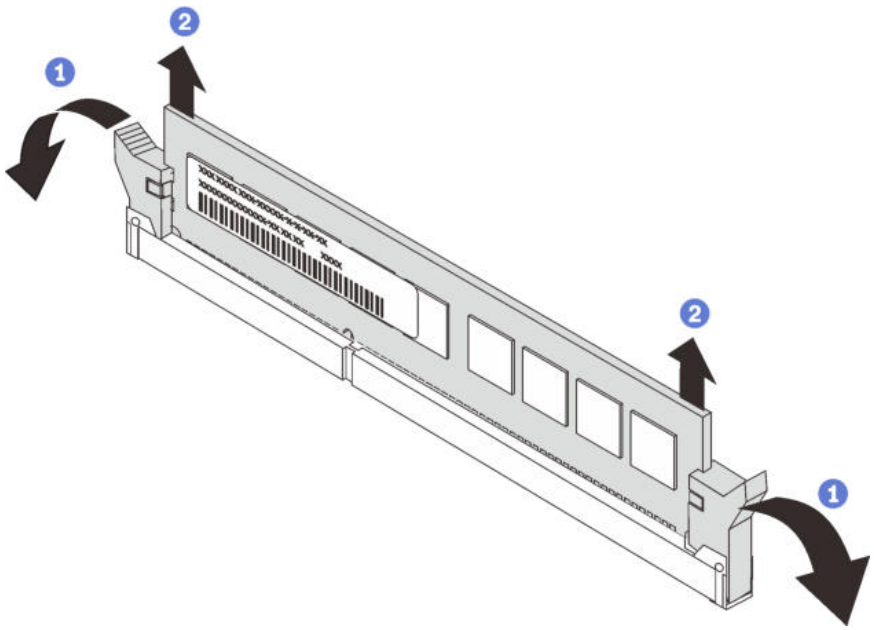


Figure 56. Memory module removal

Step 1. Open the retaining clips on each end of the memory module slot.

Attention: To avoid breaking the retaining clips or damaging the memory module slots, handle the clips gently.

Step 2. Grasp the memory module at both ends and carefully lift it out of the slot.

Step 3. Install a memory module filler or a new memory module to cover the slot.

If you are instructed to return the old memory module, follow all packaging instructions and use any packaging materials that are provided.

Memory module installation rules

Memory modules must be installed in a specific order based on the memory configuration that you implement on your server.

Your server supports up to 6 memory modules when one processor is installed, and up to 12 memory modules when two processors are installed. It supports the following types of memory modules depending on the processors installed:

For Intel Xeon SP Gen 1 processors

- Minimum: 8 GB
- Maximum:
  - 384 GB using registered DIMMs (RDIMMs)
  - 768 GB using load-reduced DIMMs (LRDIMMs)
- Type (depending on the model):
  - TruDDR4 2666, single-rank or dual-rank, 8 GB/16 GB/32 GB RDIMMs
  - TruDDR4 2666, quad-rank, 64 GB LRDIMMs
- Slots: 12 slots

For Intel Xeon SP Gen 2 processors

- Minimum: 8 GB
- Maximum: 768 GB
- Type (depending on the model):
  - TruDDR4 2666, single-rank or dual-rank, 16 GB/32 GB RDIMMs
  - TruDDR4 2933, single-rank or dual-rank, 8 GB/16 GB/32 GB/64 GB RDIMMs
- Slots: 12 slots

For a list of supported memory, see:
http://www.lenovo.com/us/en/serverproven/

Notes: Before installing a memory module, ensure that all memory modules to be installed must be the same type. Your server supports the following types of memory modules:

- DDR4 RDIMM with ECC technology
- DDR4 LRDIMM with ECC technology

The following illustration helps you to locate the memory module slots on the system board.

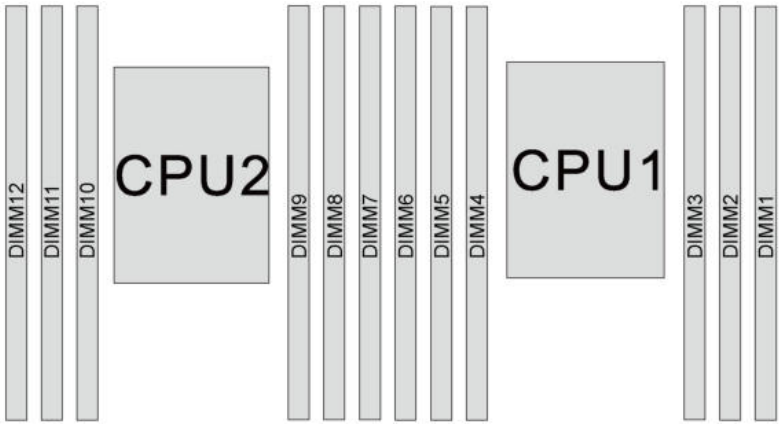


Figure 57. Memory module slots on the system board

The following memory configurations are available:
- “Independent mode” on page 81
- “Mirroring mode” on page 82
- “Rank sparing mode” on page 83

Independent mode

Independent mode provides high performance memory capability. You can populate all channels with no matching requirements. Individual channels can run at different memory module timings, but all channels must run at the same interface frequency.

The following table shows the memory module population sequence for independent mode when only one processor (CPU1) is installed.

Note: If there are three identical memory modules to be installed for CPU1, and the three memory modules have the same Lenovo part number, install the three memory modules in slots 1, 2, and 3.

Table 12. Independent mode with one processor

Total memory modules	Processor 1						Total memory modules
	6	5	4	3	2	1	
1				3			**1**
2			4	3			**2**
3			4	3	2		**3**
4		5	4	3	2		**4**
5		5	4	3	2	1	**5**
6	6	5	4	3	2	1	**6**

The following table shows the memory module population sequence for independent mode when two processors (CPU1 and CPU2) are installed.

Notes:

- If there are three identical memory modules to be installed for CPU1, and the three memory modules have the same Lenovo part number, install the three memory modules in slots 1, 2, and 3.
- If there are three identical memory modules to be installed for CPU2, and the three memory modules have the same Lenovo part numbers, install the three memory modules in slots 7, 8, and 9.

Table 13. Independent mode with two processors

Total memory modules	Processor 2						Processor 1						Total memory modules
	12	11	10	9	8	7	6	5	4	3	2	1	
2				9						3			**2**
3				9					4	3			**3**
4			10	9					4	3			**4**
5			10	9					4	3	2		**5**
6			10	9	8				4	3	2		**6**
7			10	9	8			5	4	3	2		**7**
8		11	10	9	8			5	4	3	2		**8**
9		11	10	9	8			5	4	3	2	1	**9**
10		11	10	9	8	7		5	4	3	2	1	**10**
11		11	10	9	8	7	6	5	4	3	2	1	**11**
12	12	11	10	9	8	7	6	5	4	3	2	1	**12**

Mirroring mode

In mirroring mode, each memory module in a pair must be identical in size and architecture. The channels are grouped in pairs with each channel receiving the same data. One channel is used as a backup of the other, which provides redundancy.

Note: All memory modules to be installed must be the same type with the same capacity, frequency, voltage, and rank.

The following table shows the memory module population sequence for mirroring mode when one processor (CPU1) is installed.

Table 14. Mirroring mode with one processor

Total memory modules	Processor 1						Total memory modules
	6	5	4	3	2	1	
2				3	2		**2**
3				3	2	1	**3**
4		5	4	3	2		**4**
6	6	5	4	3	2	1	**6**

The following table shows the memory module population sequence for mirroring mode when two processors (CPU1 and CPU2) are installed.

Table 15. Mirroring mode with two processors

Total memory modules	Processor 2						Processor 2						Total memory modules
	12	11	10	9	8	7	6	5	4	3	2	1	
4				9	8					3	2		**4**
5				9	8					3	2	1	**5**
6				9	8	7				3	2	1	**6**
8		11	10	9	8			5	4	3	2		**8**
9				9	8	7	6	5	4	3	2	1	**9**
10		11	10	9	8		6	5	4	3	2	1	**10**
12	12	11	10	9	8	7	6	5	4	3	2	1	**12**

Rank sparing mode

In rank sparing mode, one rank of a memory module works as the spare rank for the other ranks on the same channel. The spare rank is not available as system memory.

Notes:

- All memory modules to be installed must be the same type with the same capacity, frequency, voltage, and number of ranks.
- Single-rank memory modules do not support rank sparing mode.

Table 16. Rank sparing mode with one processor

Total memory modules	Processor 1						Total memory modules
	6	5	4	3	2	1	
1				3			**1**
2			4	3			**2**
3			4	3	2		**3**
4		5	4	3	2		**4**

Table 16. Rank sparing mode with one processor (continued)

Total memory modules	Processor 1						Total memory modules
	6	5	4	3	2	1	
5		5	4	3	2	1	**5**
6	6	5	4	3	2	1	**6**

The following table shows the memory module population sequence for rank sparing mode when two processors (CPU1 and CPU2) are installed.

Table 17. Rank sparing mode with two processors

Total memory modules	Processor 2						Processor 1						Total memory modules
	12	11	10	9	8	7	6	5	4	3	2	1	
2				9						3			**2**
3				9					4	3			**3**
4			10	9					4	3			**4**
5			10	9					4	3	2		**5**
6			10	9	8				4	3	2		**6**
7			10	9	8			5	4	3	2		**7**
8		11	10	9	8			5	4	3	2		**8**
9		11	10	9	8			5	4	3	2	1	**9**
10		11	10	9	8	7		5	4	3	2	1	**10**
11		11	10	9	8	7	6	5	4	3	2	1	**11**
12	12	11	10	9	8	7	6	5	4	3	2	1	**12**

Install a memory module

Use this information to install a memory module.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Attention:

- Disconnect all power cords for this task.
- Memory modules are sensitive to static discharge and require special handling. Refer to the standard guidelines for "Handling static-sensitive devices" on page 43:
  - Always wear an electrostatic-discharge strap when removing or installing memory modules. Electrostatic-discharge gloves can also be used.
  - Never hold two or more memory modules together so that they do not touch each other. Do not stack memory modules directly on top of each other during storage.
  - Never touch the gold memory module connector contacts or allow these contacts to touch the outside of the memory module connector housing.
  - Handle memory modules with care: never bend, twist, or drop a memory module.
  - Do not use any metal tools (such as jigs or clamps) to handle the memory modules, because the rigid metals may damage the memory modules.
  - Do not insert memory modules while holding packages or passive components, which can cause package cracks or detachment of passive components by the high insertion force.

Before installing a memory module:

1. Touch the static-protective package that contains the new memory module to any unpainted surface on the outside of the server. Then, take the new memory module out of the package and place it on a static-protective surface.
2. Locate the memory module slot on the system board by referring to "Memory module installation rules" on page 80. Ensure that you observe the installation rules and sequence.

To install a memory module, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

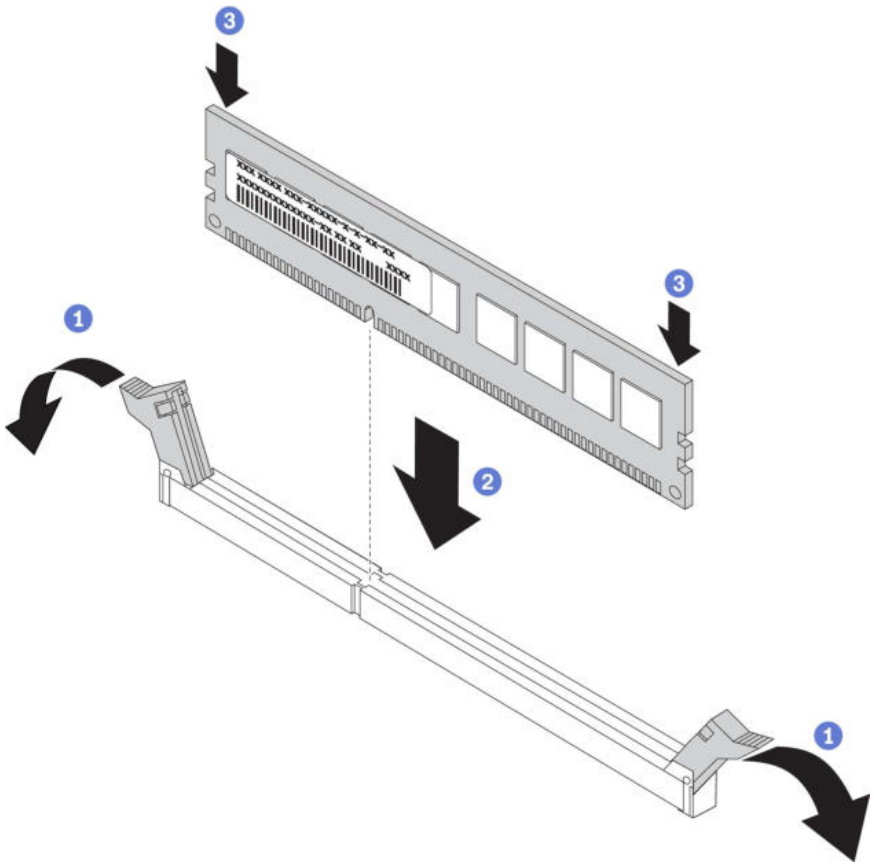


Figure 58. Memory module installation

Step 1. Open the retaining clips on each end of the memory module slot.

Attention: To avoid breaking the retaining clips or damaging the memory module slots, open and close the clips gently.

Step 2. Align the memory module with the slot, and gently place the memory module on the slot with both hands.

Step 3. Firmly press both ends of the memory module straight down into the slot until the retaining clips snap into the locked position.

Note: If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. In this case, open the retaining clips, remove the memory module, and then reinsert it.

After installing a memory module, complete the parts installation. See “Complete the parts replacement” on page 143.

CMOS battery replacement

Use this information to remove and install the CMOS battery.

Remove the CMOS battery

Use this information to remove the CMOS battery.

	"**Read** the installation Guidelines" on page 41	 "**Power off** the server for this task" on page 11	 "**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

The following tips describe information that you must consider when removing the CMOS battery.

- Lenovo has designed this product with your safety in mind. The lithium CMOS battery must be handled correctly to avoid possible danger. If you replace the CMOS battery, you must adhere to the following instructions.

  Note: In the U.S., call 1-800-IBM-4333 for information about battery disposal.
- If you replace the original lithium battery with a heavy-metal battery or a battery with heavy-metal components, be aware of the following environmental consideration. Batteries and accumulators that contain heavy metals must not be disposed of with normal domestic waste. They will be taken back free of charge by the manufacturer, distributor, or representative, to be recycled or disposed of in a proper manner.
- To order replacement batteries, call 1-800-IBM-SERV within the U.S., and 1-800-465-7999 or 1-800-465-6666 within Canada. Outside the U.S. and Canada, call your support center or business partner.

  Note: After you replace the CMOS battery, you must reconfigure the server and reset the system date and time.

S004



CAUTION:
When replacing the lithium battery, use only Lenovo specified part number or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of. *Do not:*

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

To remove the CMOS battery, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Remove the top cover. See “Remove the top cover” on page 52.

Step 2. Locate the CMOS battery, see “System board components” on page 23.

Step 3. Press the battery clip as shown and carefully lift CMOS battery out of the socket.

Attention: Do not tilt or push the CMOS battery using excessive force. Failing to remove the CMOS battery properly might damage the socket on the system board. Any damage to the socket might require replacing the system board.

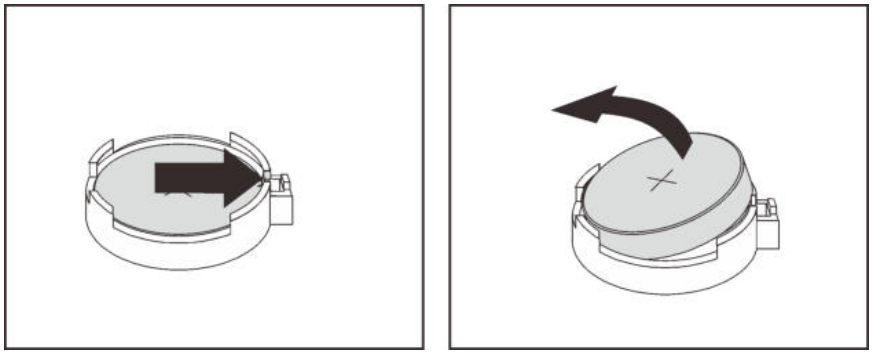


Figure 59. CMOS battery removal

After removing the CMOS battery:

1. Install a new CMOS battery.
2. Dispose of the CMOS battery as required by local ordinances or regulations.

Install the CMOS battery

Use this information to install the CMOS battery.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

The following tips describe information that you must consider when installing the CMOS battery.

- Lenovo has designed this product with your safety in mind. The lithium battery must be handled correctly to avoid possible danger. If you install the CMOS battery, you must adhere to the following instructions.

  Note: In the U. S., call 1-800-IBM-4333 for information about battery disposal.
- If you replace the original lithium battery with a heavy-metal battery or a battery with heavy-metal components, be aware of the following environmental consideration. Batteries and accumulators that contain heavy metals must not be disposed of with normal domestic waste. They will be taken back free of charge by the manufacturer, distributor, or representative, to be recycled or disposed of in a proper manner.
- To order replacement batteries, call 1-800-IBM-SERV within the U.S., and 1-800-465-7999 or 1-800-465-6666 within Canada. Outside the U.S. and Canada, call your support center or business partner.

  Note: After you install the CMOS battery, you must reconfigure the server and reset the system date and time.

S004



CAUTION:
When replacing the lithium battery, use only Lenovo specified part number or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of. *Do not:*

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To

remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

To install the CMOS battery, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Touch the static-protective package that contains the new CMOS battery to any unpainted surface on the outside of the server. Then, take the new CMOS battery out of the package and place it on a static-protective surface.

Step 2. Install the new CMOS battery. Ensure that the battery is seated in place.

Attention: Do not tilt or push the CMOS battery using excessive force. Any damage to the socket might require replacing the system board.

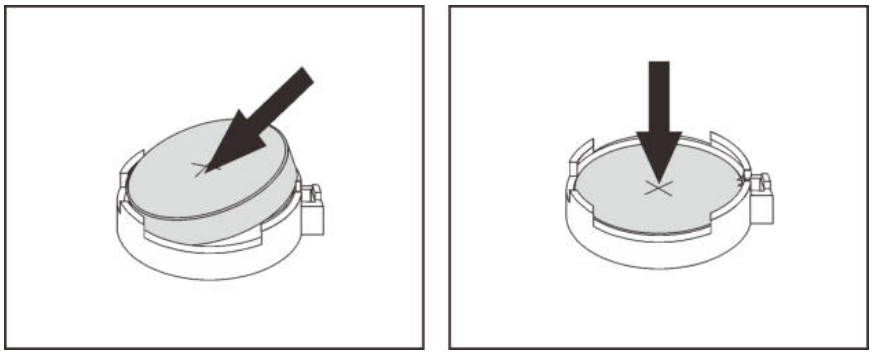


Figure 60. CMOS battery installation

After installing the CMOS battery:

1. Complete the parts installation. See “Complete the parts replacement” on page 143.
2. Use the Setup utility to set the date, time, and any passwords.

TCM/TPM adapter replacement (for Chinese Mainland only)

Use this information to remove and install the TCM/TPM adapter (sometimes called a daughter card).

Remove the TCM/TPM adapter (for Chinese Mainland only)

Use this information to remove the TCM/TPM adapter.

	“**Read** the installation Guidelines” on page 41	
	“**Power off** the server for this task” on page 11	
	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43	

To remove the TCM/TPM adapter, complete the following steps:

Step 1. Remove the top cover. See “Remove the top cover” on page 52.

Step 2. Locate the TCM/TPM connector on the system board, press the release latch on the TCM/TPM adapter, and lift it straight up.

Notes:

- Carefully handle the TCM/TPM adapter by its edges.
- Your TCM/TPM adapter might look slightly different from the illustration.

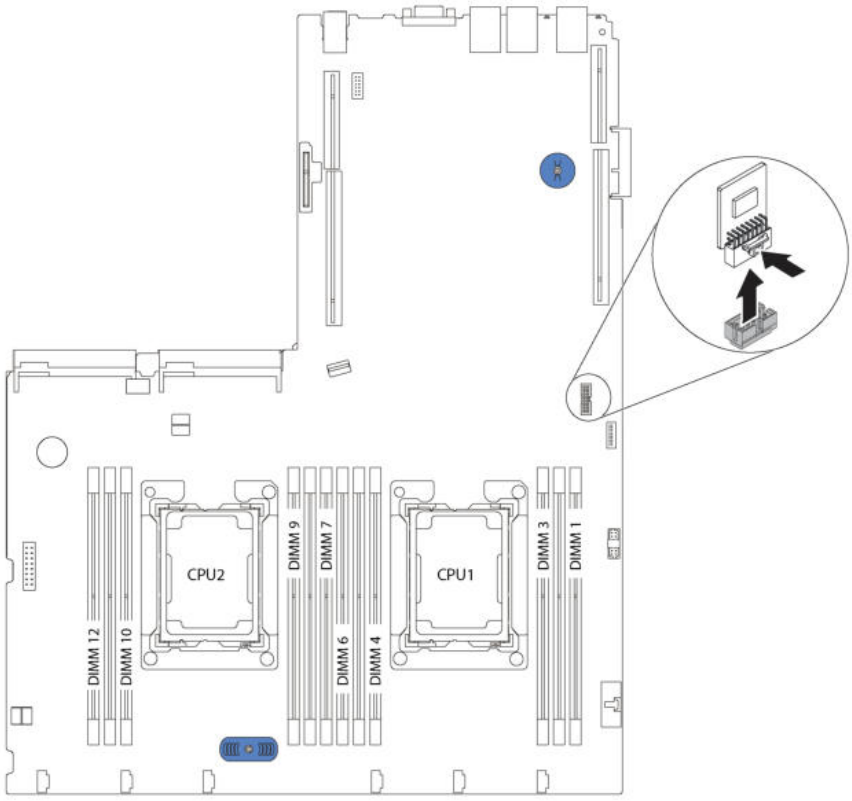


Figure 61. TCM/TPM adapter removal

If you are instructed to return the old TCM/TPM adapter, follow all packaging instructions and use any packaging materials that are provided.

Install the TCM/TPM adapter (for Chinese Mainland only)

Use this information to install the TCM/TPM adapter.

	"**Read** the installation Guidelines" on page 41	
	"**Power off** the server for this task" on page 11	
		"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before installing the TCM/TPM adapter, touch the static-protective package that contains the new TCM/TPM adapter to any unpainted surface on the outside of the server. Then, take the new TCM/TPM adapter out of the package and place it on a static-protective surface.

To install the TCM/TPM adapter, complete the following steps:

Step 1. Locate the TCM/TPM connector on the system board.

Step 2. Insert the TCM/TPM adapter into the TCM/TPM connector on the system board.

Notes:

- Carefully handle the TCM/TPM adapter by its edges.

- Your TCM/TPM adapter might look slightly different from the illustration.

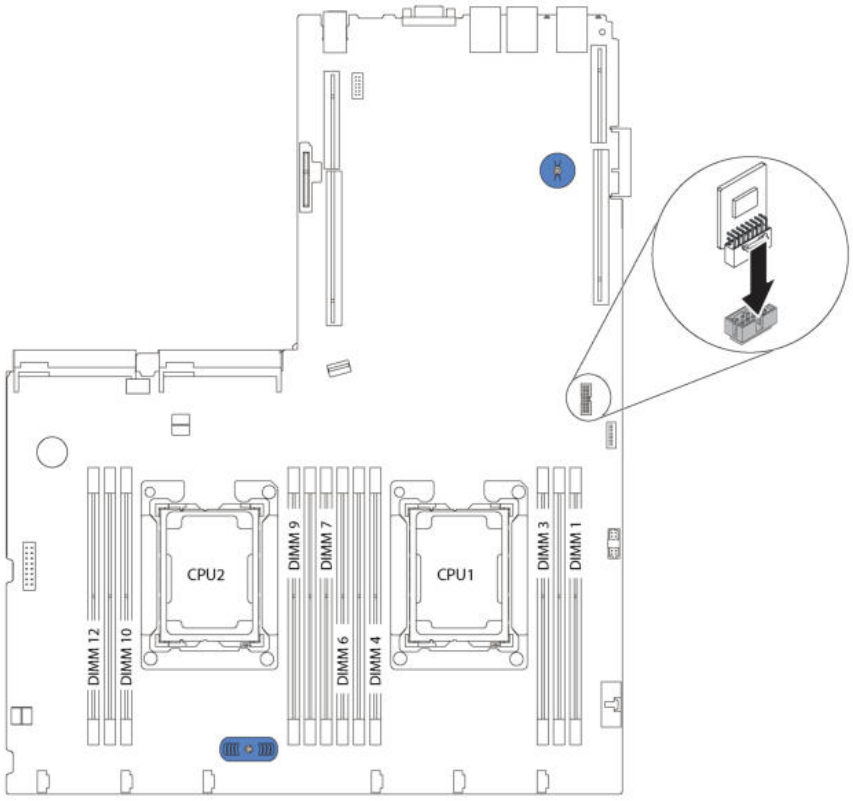


Figure 62. TCM/TPM adapter installation

After installing the TCM/TPM adapter, complete the parts replacement. See “Complete the parts replacement” on page 143.

Hot-swap power supply replacement

Use this information to remove and install the hot-swap power supply.

Remove a hot-swap power supply

Use this information to remove a hot-swap power supply.

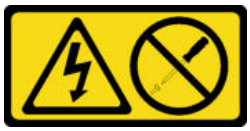


"**Read** the installation Guidelines" on page 41



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

S035



CAUTION:
Never remove the cover on a power supply or any part that has this label attached. Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

S001



DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect any equipment that will be attached to this product to properly wired outlets .**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	**To Disconnect:**
1. Turn everything OFF. 2. Attach all cables to devices. 3. Attach signal cables to connectors. 4. Attach power cords to outlet. 5. Turn device ON.	1. Turn everything OFF. 2. Remove power cords from outlet. 3. Remove signal cables from connectors. 4. Remove all cables from devices.



Figure 63. Hot-swap power supply label on the cover

Attention: This type of power supply is hot-swap only when two power supplies are installed for redundancy. If only one power supply is installed, you must power off the server before removing the power supply.

The following tips describe the information that you must consider when you remove a power supply with dc input.

CAUTION:

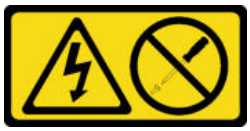
- **240 V dc input (input range: 180-300 V dc) is supported in Chinese Mainland ONLY. Power supply with 240 V dc input cannot support hot plugging power cord function. Before removing the power supply with dc input, please turn off server or disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the power cord.**
- **In order for the ThinkSystem products to operate error free in both a DC or AC electrical environment, a TN-S earthing system which complies to 60364-1 IEC 2005 standard has to be present or installed.**



在直流输入状态下，若电源供应器插座不支持热插拔功能，请务必不要对设备电源线进行热插拔。此操作可能导致设备损坏及数据丢失。因错误执行热插拔导致的设备故障或损坏，不属于保修范围。

NEVER CONNECT AND DISCONNECT THE POWER SUPPLY CABLE AND EQUIPMENT WHILE YOUR EQUIPMENT IS POWERED ON WITH DC SUPPLY (hot-plugging). Otherwise you may damage the equipment and result in data loss, the damages and losses result from incorrect operation of the equipment will not be covered by the manufacturers' warranty.

S035



CAUTION:
Never remove the cover on a power supply or any part that has this label attached. Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

S019



CAUTION:
The power-control button on the device does not turn off the electrical current supplied to the device. The device also might have more than one connection to dc power. To remove all electrical current from the device, ensure that all connections to dc power are disconnected at the dc power input terminals.

S029



DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded power source.**
- **Connect to properly wired power sources any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached ac power cords, dc power sources, network connections, telecommunications systems, and serial cables before you open the device covers, unless you are instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	**To Disconnect:**
1. Turn OFF all power sources and equipment that is to be attached to this product. 2. Attach signal cables to the product. 3. Attach power cords to the product. • For ac systems, use appliance inlets. • For dc systems, ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety. 4. Attach signal cables to other devices. 5. Connect power cords to their sources. 6. Turn ON all the power sources.	1. Turn OFF all power sources and equipment that is to be attached to this product. • For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit. • For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables. 2. Remove the signal cables from the connectors. 3. Remove all cables from the devices.

To remove a hot-swap power supply, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. If the server is in a rack, adjust the cable management arm (CMA) to gain access to the power supply.

If you have installed the 1U CMA Upgrade Kit for Toolless Slide Rail or Toolless Slide Rail Kit with 1U CMA, do the following:

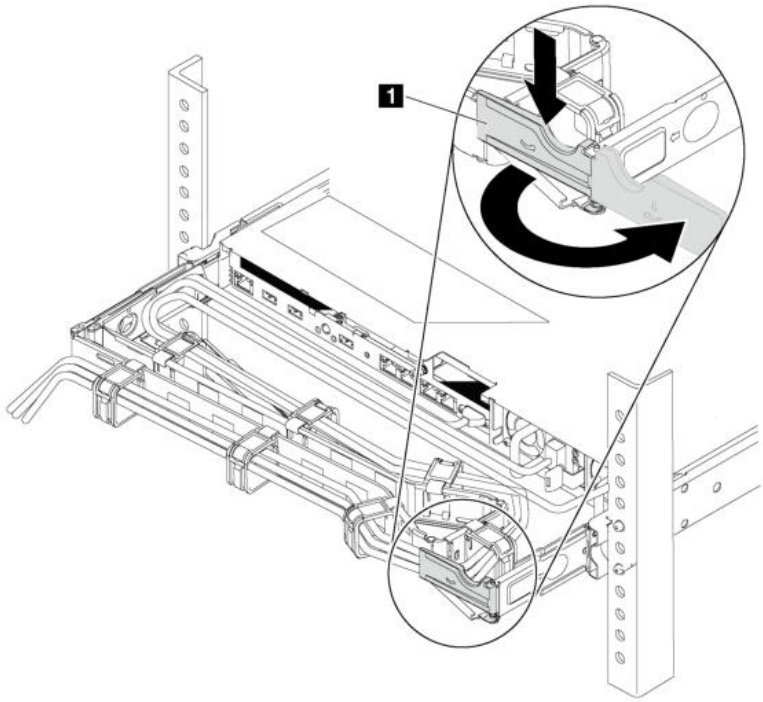


Figure 64. CMA adjustment

a. Press down the stop bracket 1 and rotate it to the open position.
b. Rotate the CMA out of the way to gain access to the power supply.

Step 2. Disconnect the power cord from the hot-swap power supply.

Note: If you are replacing two power supplies, do the power supply replacement one by one to ensure that the power supply to the server is not interrupted. Do not disconnect the power cord from the secondly replaced power supply until the power output LED for the firstly replaced power supply is lit. For the location of the power output LED, refer to “Rear view LEDs” on page 21.

Step 3. Press the release tab toward the handle and carefully pull the handle at the same time to slide the hot-swap power supply out of the chassis.

Notes: Slightly pull the power supply upwards when sliding the power supply out of the chassis, if you have installed one of the following CMA kits:

- 1U CMA Upgrade Kit for Toolless Slide Rail
- Toolless Slide Rail Kit with 1U CMA

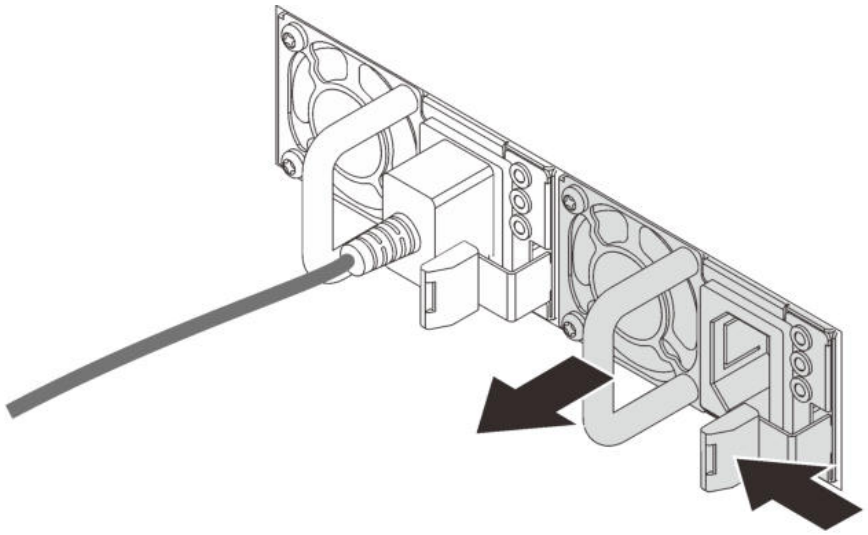


Figure 65. Hot-swap power supply removal

After removing the power supply:

- Install a power supply filler or a new power supply to cover the power supply bay.

  Important: To ensure proper cooling during normal server operation, both of the power supply bays must be occupied. This means that each bay must have a power supply installed; or one has a power supply installed and the other has a power supply filler installed.
- If you are instructed to return the old power supply, follow all packaging instructions and use any packaging materials that are provided.

Install a hot-swap power supply

Use this information to install a hot-swap power supply.

	“**Read** the installation Guidelines” on page 41
	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

The following tips describe the type of power supply that the server supports and other information that you must consider when you install a power supply:

- The standard shipping has only one power supply installed in the server. For redundancy and hot-swap support, you must install an additional hot-swap power supply. Certain customized models might be shipped with two power supplies installed.
- Ensure that the devices that you are installing are supported. For a list of supported optional devices for the server, go to:
  http://www.lenovo.com/us/en/serverproven/

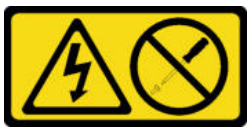
Notes:

- Ensure that the two power supplies installed on the server have the same wattage.
- If you are replacing the existing power supply with a new power supply of different wattage, attach the power rating label that comes with this option onto the existing label on the top cover near the power supply.



Figure 66. Hot-swap power supply label on the cover

S035



CAUTION:
Never remove the cover on a power supply or any part that has this label attached. Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

S002



CAUTION:

The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

S001



DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect any equipment that will be attached to this product to properly wired outlets .**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	**To Disconnect:**
1. Turn everything OFF. 2. Attach all cables to devices. 3. Attach signal cables to connectors. 4. Attach power cords to outlet. 5. Turn device ON.	1. Turn everything OFF. 2. Remove power cords from outlet. 3. Remove signal cables from connectors. 4. Remove all cables from devices.

The following tips describe the information that you must consider when you install a power supply with dc input.

CAUTION:

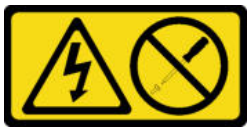
- **240 V dc input (input range: 180-300 V dc) is supported in Chinese Mainland ONLY. Power supply with 240 V dc input cannot support hot plugging power cord function. Before removing the power supply with dc input, please turn off server or disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the power cord.**
- **In order for the ThinkSystem products to operate error free in both a DC or AC electrical environment, a TN-S earthing system which complies to 60364-1 IEC 2005 standard has to be present or installed.**



在直流输入状态下，若电源供应器插座不支持热插拔功能，请务必不要对设备电源线进行热插拔。此操作可能导致设备损坏及数据丢失。因错误执行热插拔导致的设备故障或损坏，不属于保修范围。

NEVER CONNECT AND DISCONNECT THE POWER SUPPLY CABLE AND EQUIPMENT WHILE YOUR EQUIPMENT IS POWERED ON WITH DC SUPPLY (hot-plugging). Otherwise you may damage the equipment and result in data loss, the damages and losses result from incorrect operation of the equipment will not be covered by the manufacturers' warranty.

S035



CAUTION:
Never remove the cover on a power supply or any part that has this label attached. Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

S019



CAUTION:
The power-control button on the device does not turn off the electrical current supplied to the device. The device also might have more than one connection to dc power. To remove all electrical current from the device, ensure that all connections to dc power are disconnected at the dc power input terminals.

S029



DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded power source.**
- **Connect to properly wired power sources any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached ac power cords, dc power sources, network connections, telecommunications systems, and serial cables before you open the device covers, unless you are instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
2. Attach signal cables to the product.
3. Attach power cords to the product.
   - For ac systems, use appliance inlets.
   - For dc systems, ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety.
4. Attach signal cables to other devices.
5. Connect power cords to their sources.
6. Turn ON all the power sources.

To Disconnect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
   - For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.
   - For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.
2. Remove the signal cables from the connectors.
3. Remove all cables from the devices.

To install a hot-swap power supply, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Touch the static-protective package that contains the new power supply to any unpainted surface on the outside of the server. Then, take the new power supply out of the package and place it on a static-protective surface.

Step 2. If the server is in a rack, adjust the CMA to gain access to the power supply bay.

If you have installed the 1U CMA Upgrade Kit for Toolless Slide Rail or Toolless Slide Rail Kit with 1U CMA, do the following:

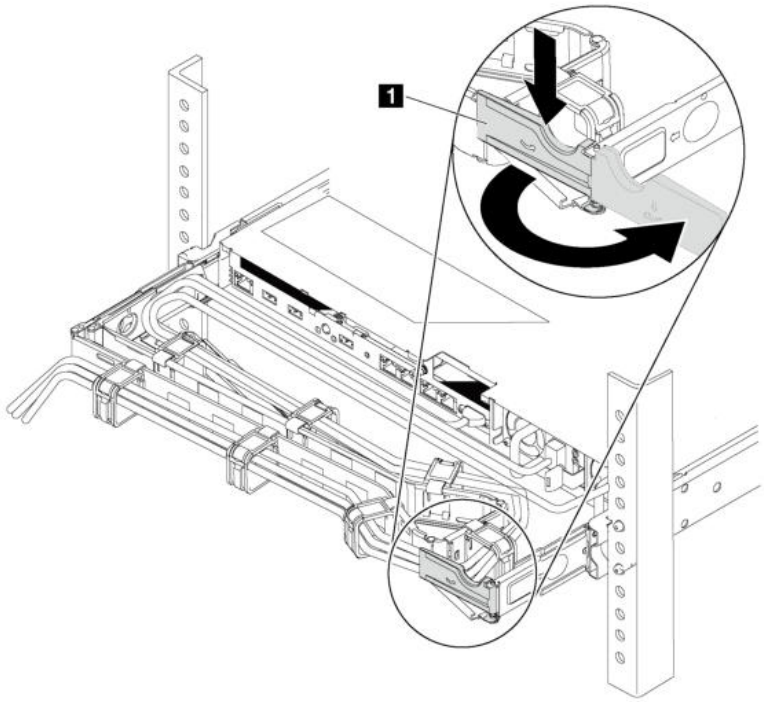


Figure 67. CMA adjustment

a. Press down the stop bracket 1 and rotate it to the open position.
b. Rotate the CMA out of the way to gain access to the power supply bay.

Step 3. If there is a power supply filler installed, remove it.

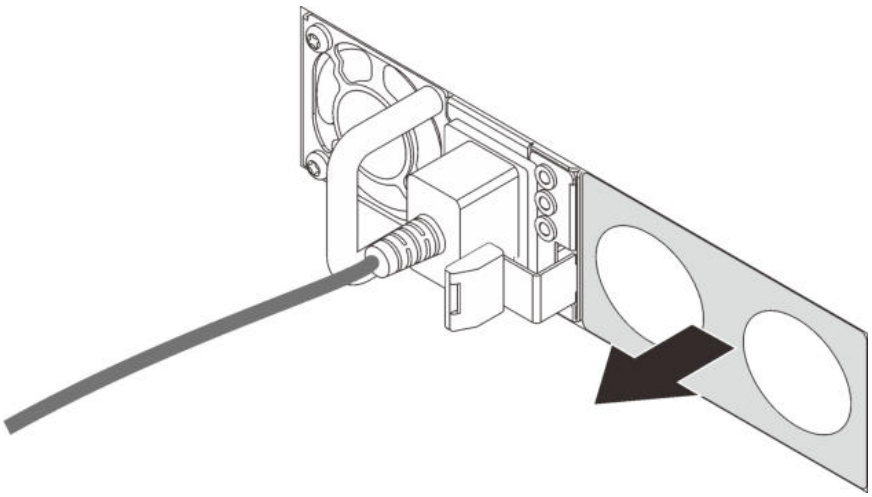


Figure 68. Hot-swap power supply filler removal

Step 4. Slide the new hot-swap power supply into the bay until the release latch clicks into place.

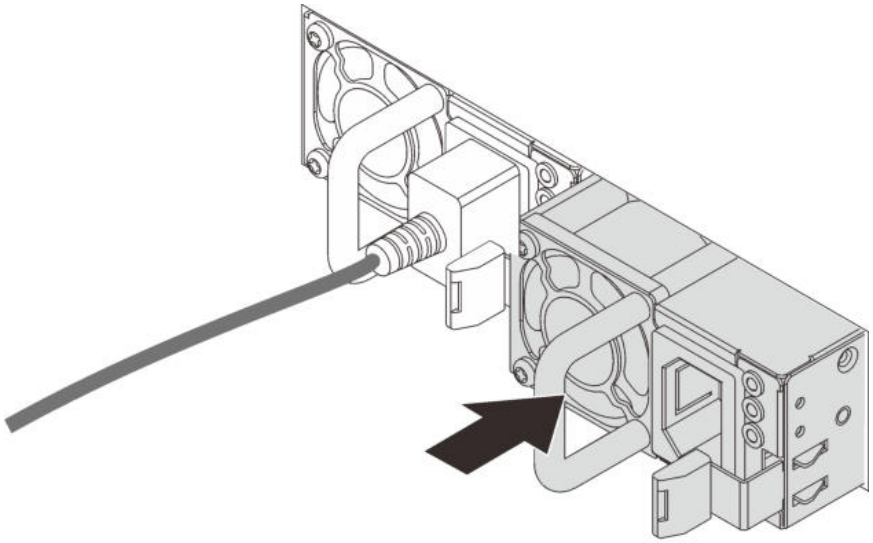


Figure 69. Hot-swap power supply installation

After installing the power supply:

1. Connect the power cord to the new power supply and ensure that it is connected to a properly grounded electrical outlet.
2. If the server is powered off, power on the server. Ensure that both the power input LED and the power output LED on the power supply are lit, indicating that the power supply is operating properly.

PCIe adapter replacement

Use this information to remove and install a PCIe adapter.

The PCIe adapter can be a host bus adapter (HBA), a PCIe RAID adapter, an Ethernet adapter, and any other supported PCIe adapters. For information about the PCIe slots and supported PCIe adapters, see “Rear view” on page 17.

Notes:

- Depending on the specific type, the PCIe adapter might look different from the illustrations in this topic.
- Use any documentation that comes with the PCIe adapter and follow those instructions in addition to the instructions in this topic.

Remove a PCIe adapter

Use this information to remove a PCIe adapter.



“**Read** the installation Guidelines” on page 41



“**Power off** the server for this task” on page 11



“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing a PCIe adapter:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Remove the riser assembly. See “Remove a riser adapter” on page 107.

To remove a PCIe adapter, complete the following steps:

Table 18. PCIe adapter removal

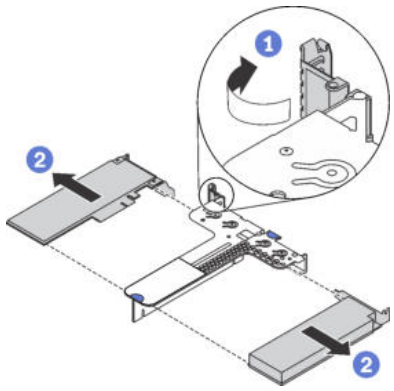


Figure 70. Riser 1 assembly (LP+LP)

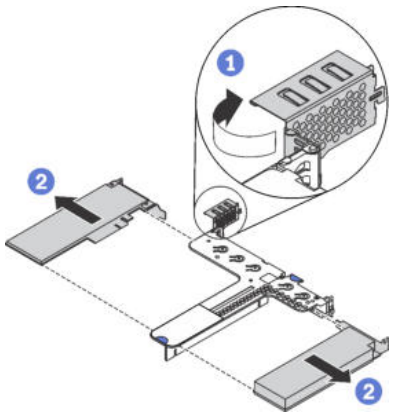


Figure 71. Riser 1 assembly (LP +FHHL)

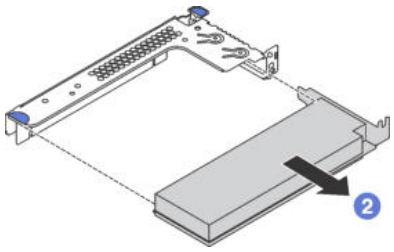


Figure 72. Riser 2 assembly (LP)

Step 1. (Skip this step for riser 2 assembly.) Pivot the latch on the riser bracket to the open position.

Step 2. Grasp the PCIe adapter by its edges and carefully pull it out of the PCIe slot on the riser card.

If you are instructed to return the old PCIe adapter, follow all packaging instructions and use any packaging materials that are provided.

Install a PCIe adapter

Use this information to install a PCIe adapter.

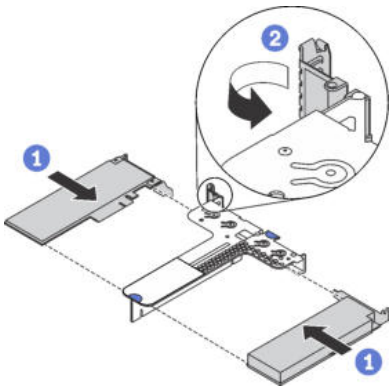
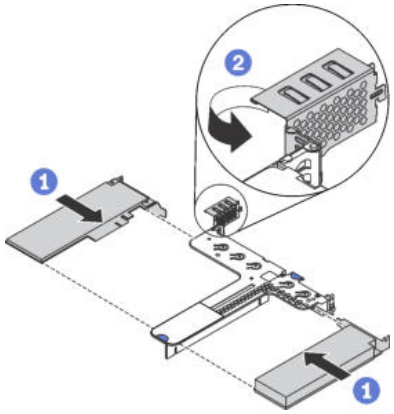
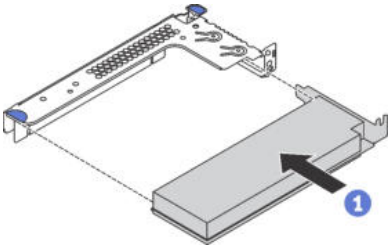
	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing a PCIe adapter,

1. Locate the correct PCIe slot for the PCIe adapter. For information about the PCIe slots and supported PCIe adapters, see “Rear view” on page 17.
2. Touch the static-protective package that contains the new PCIe adapter to any unpainted surface on the outside of the server. Then, take the new PCIe adapter out of the package and place it on a static-protective surface.

To install a PCIe adapter, complete the following steps:

Table 19. PCIe adapter installation

 *Figure 73. Riser 1 assembly (LP+LP)*	 *Figure 74. Riser 1 assembly (LP +FHHL)*	 *Figure 75. Riser 2 assembly (LP)*

Step 1. Align the PCIe adapter with the PCIe slot on the riser card. Then, carefully press the PCIe adapter straight into the slot until it is securely seated and its bracket also is secured.

Step 2. (Skip this step for riser 2 assembly.) Pivot the latch on the riser bracket to the closed position.

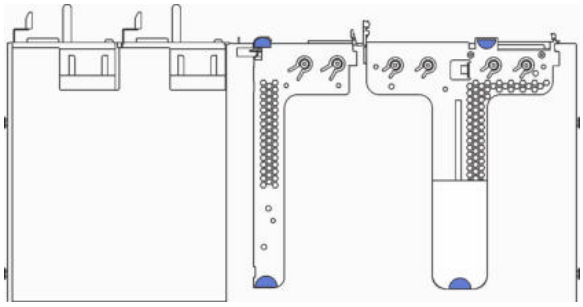
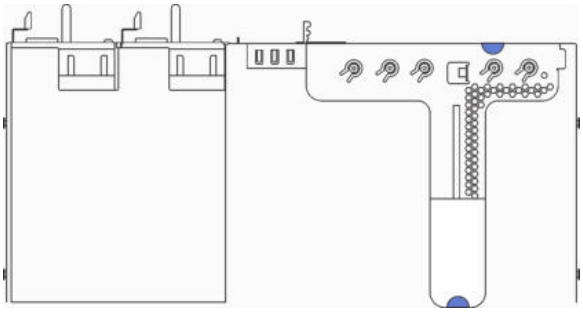
After installing the PCIe adapter:

1. Reinstall the riser assembly. See “Install a riser adapter” on page 109.
2. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Riser card replacement

Use this information to remove and install a riser card.

Your server comes with one of the following riser assembly configurations:

Configuration 1	Configuration 2
 • Riser 1 assembly: LP + LP • Riser 2 assembly: LP (available on some models)	 • Riser 1 assembly: LP + FHHL

For information about the supported riser cards for each configuration, see “Rear view” on page 17.

There are three types of riser assemblies. The removal and installation procedure of the riser card is similar for all types of riser assemblies. The following procedures are based on the riser assembly in configuration 2.

Remove a riser card

Use this information to remove a riser card.

		
“**Read** the installation Guidelines” on page 41	“**Power off** the server for this task” on page 11	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

To remove a riser card, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Note: The riser assembly you want to remove might be different from the illustrations below, but the removal method is the same.

Step 1. Remove the top cover. See “Remove the top cover” on page 52.

Step 2. Grasp the riser assembly by its edges and carefully lift it up.

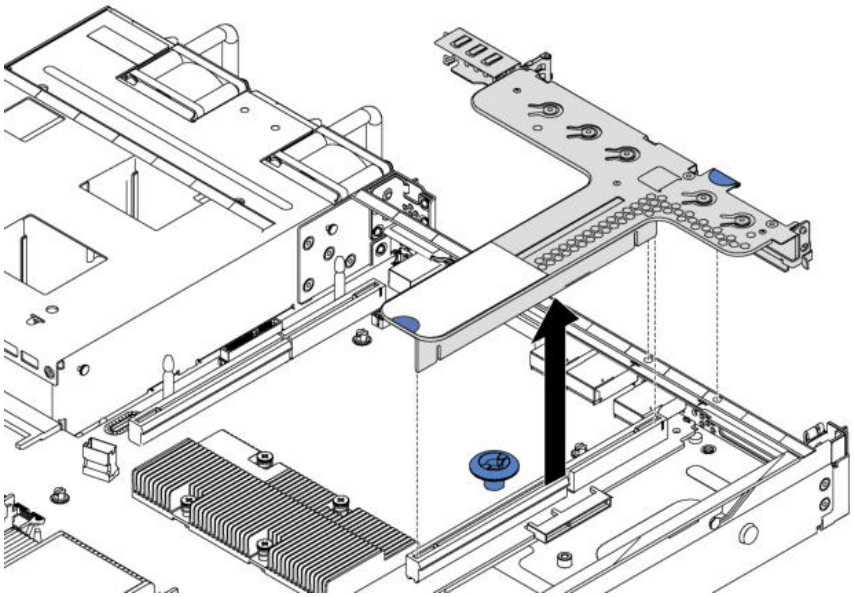


Figure 76. Riser assembly removal

Step 3. If there is any PCIe adapter installed on the riser card, record the cable connections first. Then, disconnect all cables from the PCIe adapter and completely remove the riser assembly out of the chassis.

Step 4. Remove the PCIe adapter that is installed on the riser card. See “Remove a PCIe adapter” on page 105.

Step 5. Remove the two screws that secure the riser card to the bracket. Then, remove the riser card.

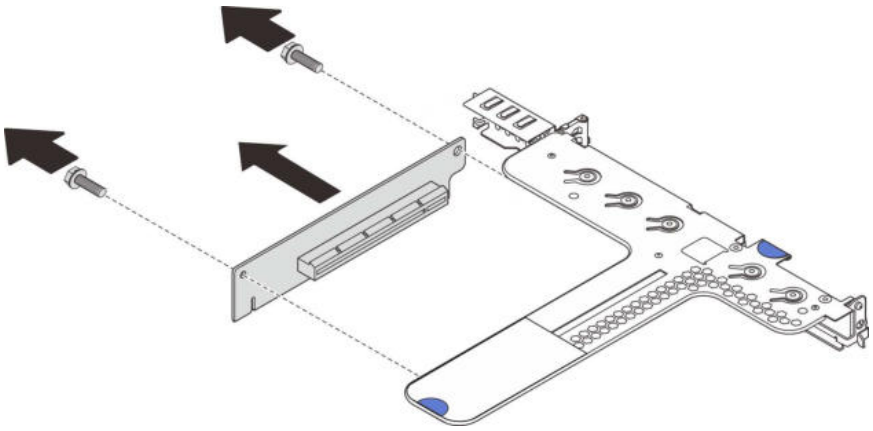


Figure 77. Riser card removal

If you are instructed to return the old riser card, follow all packaging instructions and use any packaging materials that are provided.

Install a riser card

Use this information to install a riser card.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

To install a riser card, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Note: The riser assembly you want to install might be different from the illustrations below, but the installation method is the same.

Step 1. Touch the static-protective package that contains the new riser card to any unpainted surface on the outside of the server. Then, take the new riser card out of the package and place it on a static-protective surface.

Step 2. Note the notch 1 on the riser card and ensure that the orientation of the riser card is correct as shown. Then, align the screw holes in the new riser card with the corresponding ones in the bracket and install the two screws to secure the riser card to the bracket.

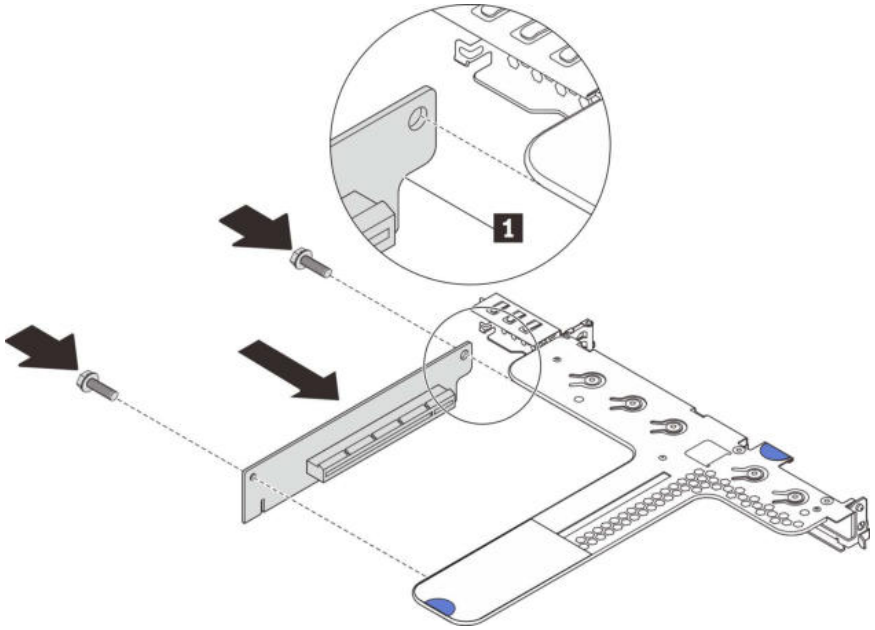


Figure 78. Riser card installation

Step 3. Install a PCIe adapter on the riser card. See “Install a PCIe adapter” on page 106.

Step 4. Connect cables to the PCIe adapter on the riser card. See “Internal cable routing” on page 28.

Step 5. Position the riser assembly on the chassis. Align the two pins on the bracket with the two holes in the chassis and align the riser card with the riser slot on the system board. Then, carefully press the riser assembly straight down into the slot until it is fully seated.

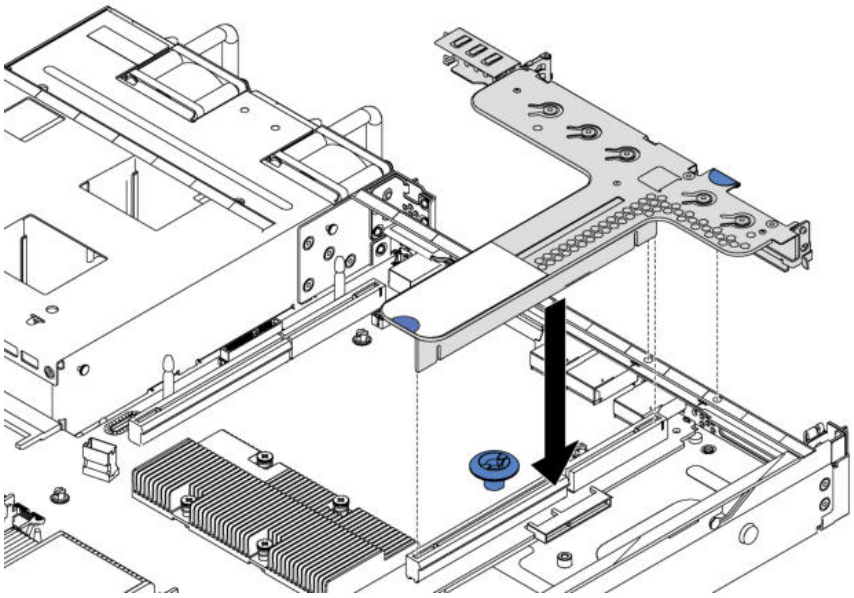


Figure 79. Riser assembly installation

After installing the riser card, complete the parts replacement. See “Complete the parts replacement” on page 143.

M.2 backplane and M.2 drive replacement

Use this information to remove and install the M.2 backplane and M.2 drive (an assembled M.2 backplane and M.2 drive is also known as M.2 module).

Remove the M.2 backplane and M.2 drive

Use this information to remove the M.2 backplane and M.2 drive.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the M.2 backplane and M.2 drive:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. For easier operation, remove the riser assembly next to the M.2 backplane. See "Remove a riser adapter" on page 107.

To remove the M.2 backplane and M.2 drive, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Grasp the M.2 backplane at both ends and pull it straight up to remove it from the system board.

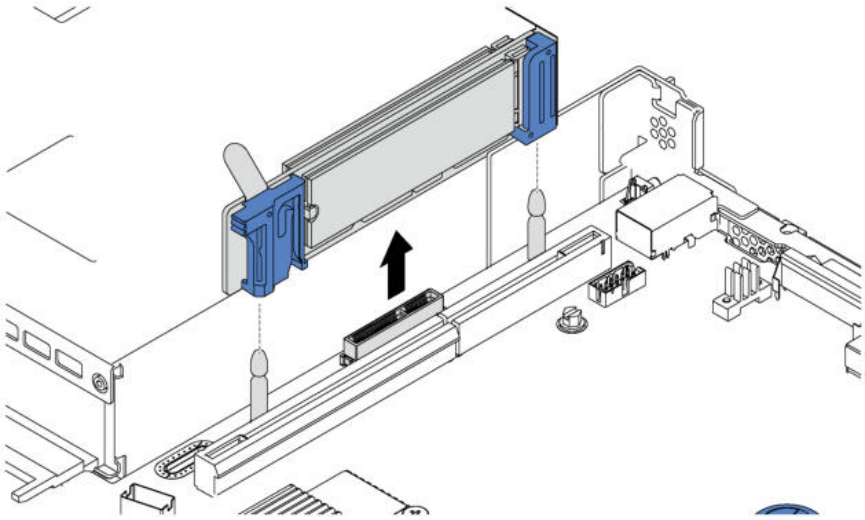


Figure 80. M.2 backplane removal

Step 2. Remove the M.2 drive from the M.2 backplane.

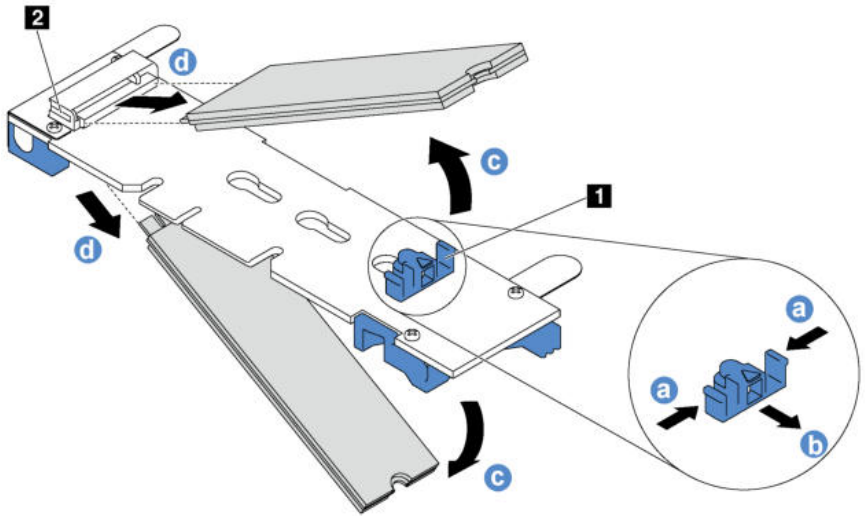


Figure 81. M.2 drive removal

a. Press both sides of the retainer **1**.
b. Slide the retainer backward to loosen the M.2 drive from the M.2 backplane.

   Note: If the M.2 backplane has two M.2 drives, they will both release outward when you slide the retainer backward.
c. Rotate the M.2 drive away from the M.2 backplane.
d. Pull it away from the connector **2** at an angle of approximately 30 degrees.

If you are instructed to return the old M.2 backplane or M.2 drive, follow all packaging instructions and use any packaging materials that are provided.

Adjust the retainer on the M.2 backplane

Use this information to adjust the retainer on the M.2 backplane.

Before adjusting the retainer on the M.2 backplane, locate the correct keyhole that the retainer should be installed into to accommodate the particular size of the M.2 drive you wish to install.

To adjust the retainer on the M.2 backplane, complete the following steps:

Watch the procedure. A video of the adjustment process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

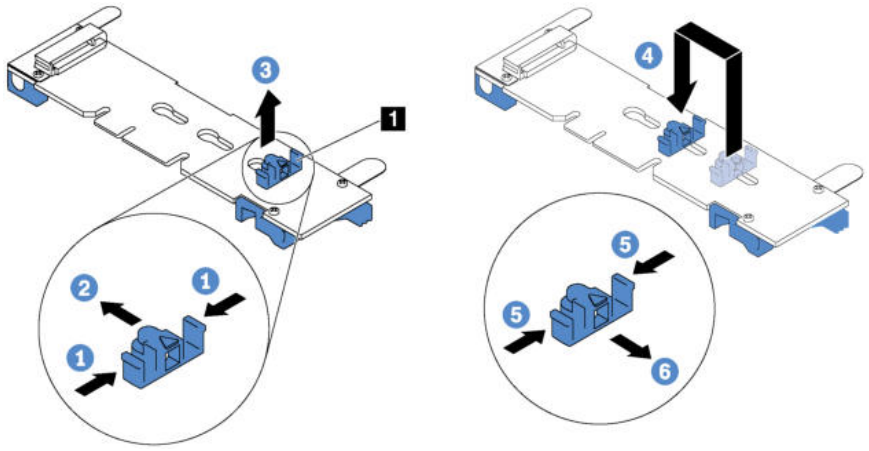


Figure 82. M.2 retainer adjustment

Step 1. Press both sides of the retainer **1**.

Step 2. Move the retainer forward until it is in the large opening of the keyhole.

Step 3. Take the retainer out of the keyhole.

Step 4. Insert the retainer into the correct keyhole.

Step 5. Press both sides of the retainer.

Step 6. Slide the retainer backwards until it is seated in place.

Install the M.2 backplane and M.2 drive

Use this information to install the M.2 backplane and M.2 drive.

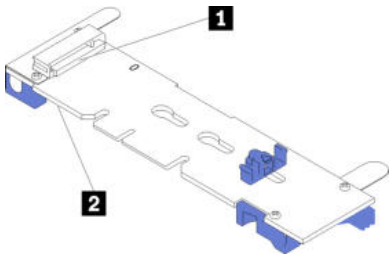
		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before installing the M.2 backplane and M.2 drive:

1. Touch the static-protective package that contains the new M.2 backplane and M.2 drive to any unpainted surface on the outside of the server. Then, take the new M.2 backplane and M.2 drive out of the package and place them on a static-protective surface.
2. Adjust the retainer on the M.2 backplane to accommodate the particular size of the M.2 drive you wish to install. See "Adjust the retainer on the M.2 backplane" on page 113.
3. Locate the connector on each side of the M.2 backplane.

   Notes:

   - Some M.2 backplanes support two identical M.2 drives. When two M.2 drives are installed, align and support both M.2 drives when sliding the retainer forward to secure the M.2 drives.
   - Install the M.2 drive in slot 0 first.



1 Slot 0
2 Slot 1

Figure 83. M.2 drive slot

To install the M.2 backplane and M.2 drive, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

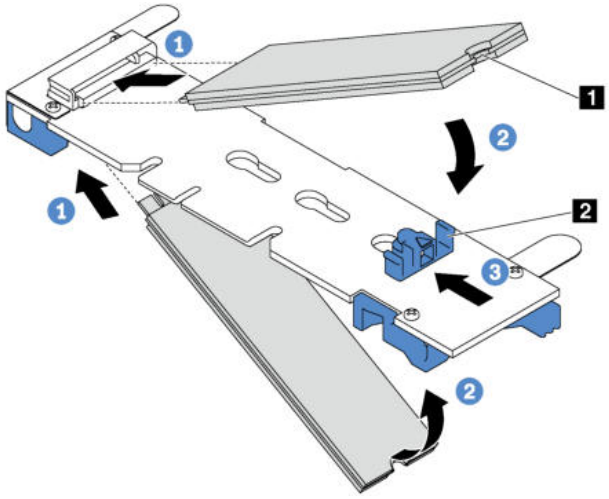


Figure 84. M.2 drive installation

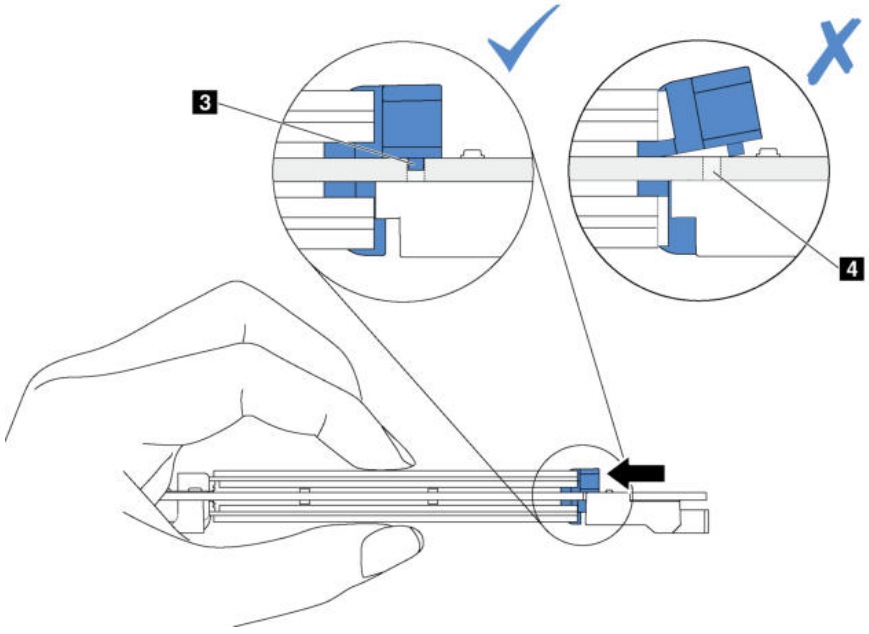
Step 1. Insert the M.2 drive at an angle of approximately 30 degrees into the connector.

Note: If your M.2 backplane supports two M.2 drives, insert the M.2 drives into the connectors at both sides.

Step 2. Rotate the M.2 drive down until the notch 1 catches on the lip of the retainer 2.

Step 3. Slide the retainer forward (toward the connector) to secure the M.2 drive into place.

Attention: When sliding the retainer forward, ensure that the two nubs 3 on the retainer enter the small holes 4 on the M.2 backplane. Once they enter the holes, you will hear a soft “click” sound.



Step 4. Align the blue plastic supports at each end of the M.2 backplane with the guide pins on the system board. Then, insert the M.2 backplane into the M.2 slot on the system board and press it down to fully seat it.

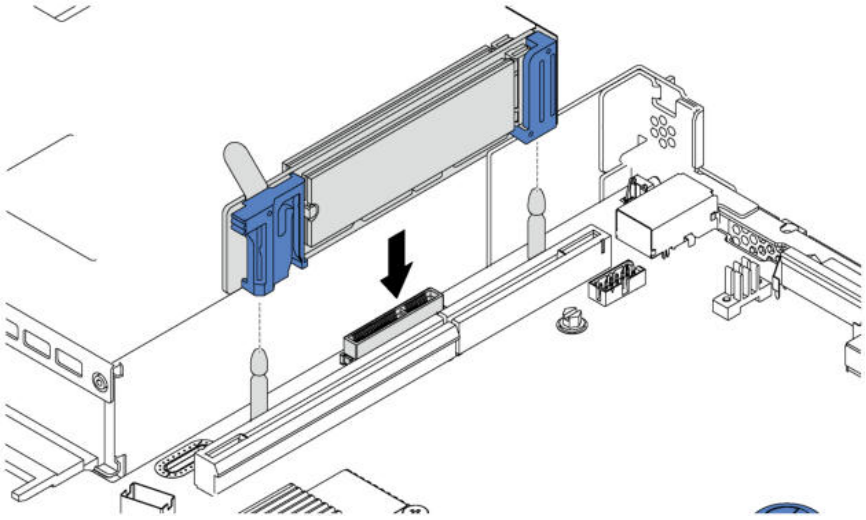


Figure 85. M.2 backplane installation

After installing the M.2 drive and M.2 backplane:

1. Reinstall the riser assembly next to the M.2 backplane. See “Install a riser adapter” on page 109.
2. Complete the parts replacement. See “Complete the parts replacement” on page 143.
3. Use the Lenovo XClarity Provisioning Manager to configure the RAID. For more information, see: http://sysmgt.lenovofiles.com/help/topic/LXPM/RAID_setup.html

Serial port module replacement

Use this information to remove and install the serial port module.

Note: The serial port module is available only on some models.

Remove the serial port module

Use this information to remove the serial port module.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

To remove the serial port module, complete the following steps:

Note: The serial port module might be installed on riser 1 assembly or riser 2 assembly. The following steps are based on the scenario that the serial port module is installed on riser 2 assembly. The removal procedure is the same for the serial port module installed on riser 1 assembly.

Step 1. Remove the top cover. See "Remove the top cover" on page 52.

Step 2. Disconnect the cable of the serial port module from the system board.

Step 3. Grasp the riser 2 assembly with the serial port module and carefully lift the riser assembly out of the server.

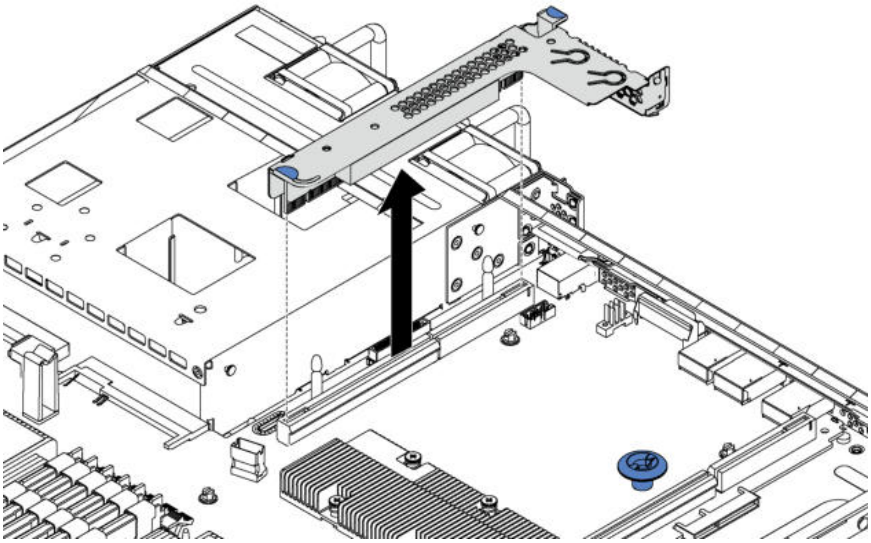


Figure 86. Riser assembly removal

Step 4. Slide the serial port module out of the bracket.

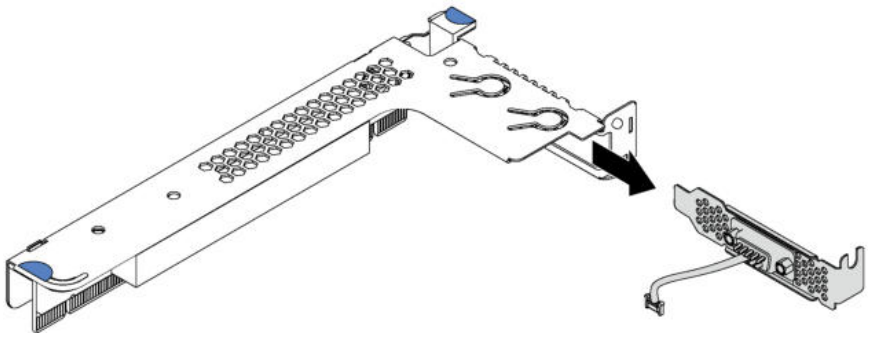


Figure 87. Serial port module removal

After removing the serial port module:

1. Install a new serial port module, a filler, or a PCIe adapter to cover the place.
2. If you are instructed to return the old serial port module, follow all packaging instructions and use any packaging materials that are provided.

Install the serial port module

Use this information to install the serial port module.

		
“**Read** the installation Guidelines” on page 41	“**Power off** the server for this task” on page 11	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the serial port module, touch the static-protective package that contains the new serial port module to any unpainted surface out of the server. Then, take the new serial port module out of the package and place it on a static-protective surface.

To install the serial port module, complete the following steps:

Note: The serial port module can be installed on riser 1 assembly or riser 2 assembly. The following steps are based on the scenario that the serial port module is to be installed on riser 2 assembly. The installation procedure is the same for the serial port module to be installed on riser 1 assembly.

Step 1. Locate the riser assembly and remove it from the server.

Step 2. If the riser assembly is covered with a PCIe slot bracket, remove the bracket first. Then, install the serial port module into the riser assembly.

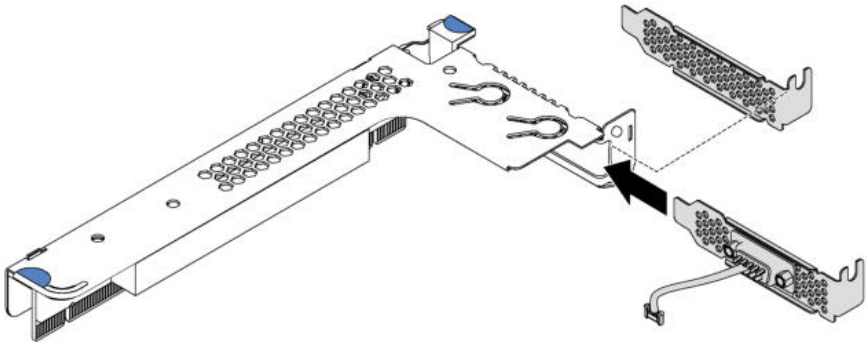


Figure 88. Serial port module installation

Step 3. Insert the riser assembly into the riser slot on the system board. Ensure that the riser assembly is fully seated.

Step 4. Connect the cable of the serial port module to serial-port-module connector on the system board. To locate the connector, see “System board components” on page 23. If the serial port module is installed in PCIe slot 1, route the cable of the serial port module as shown.

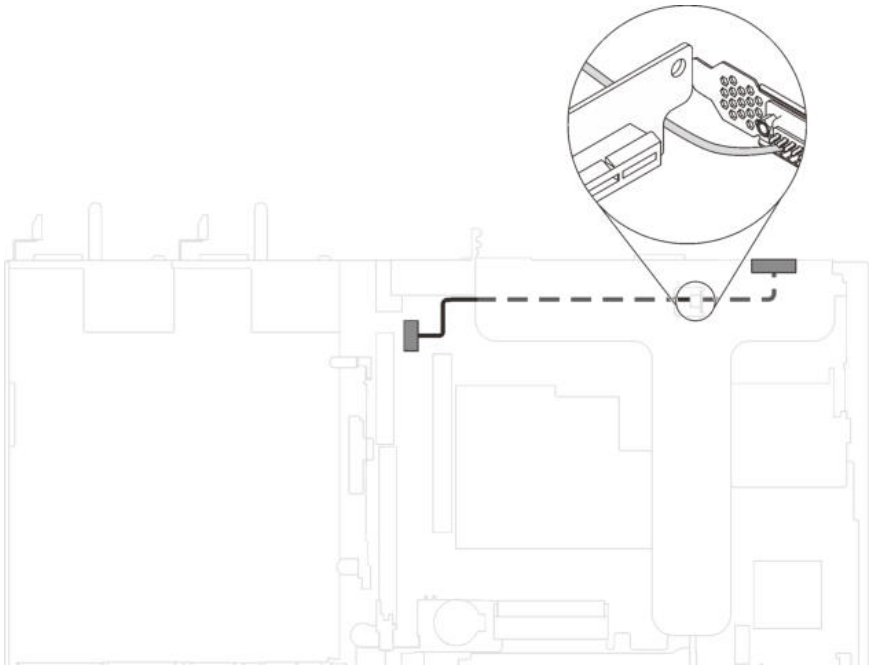


Figure 89. Cable routing for serial port module installed in PCIe slot 1

After installing the serial port module:

1. Complete the parts replacement. See “Complete the parts replacement” on page 143.
2. To enable the serial port module, do one of the following according to the installed operating system:
   - For Linux operating system:

     Open the ipmitool and enter the following command to disable the Serial over LAN (SOL) feature:

     ```
     -I lanplus -H IP -U USERID -P PASSWORD sol deactivate
     ```

   - For Microsoft Windows operating system:
     a. Open the ipmitool and enter the following command to disable the SOL feature:

        ```
        -I lanplus -H IP -U USERID -P PASSWORD sol deactivate
        ```

     b. Open Windows PowerShell and enter the following command to disable the Emergency Management Services (EMS) feature:

        ```
        Bcdedit /ems no
        ```

     c. Restart the server to ensure that the EMS setting takes effect.

LOM adapter replacement

Use this information to remove and install the LOM adapter.

Remove the LOM adapter

Use this information to remove the LOM adapter.

	"**Read** the installation Guidelines" on page 41	 "**Power off** the server for this task" on page 11
	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43	

Before removing the LOM adapter:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. If riser 1 assembly is installed, remove it to access the LOM adapter slot.

To remove the LOM adapter, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

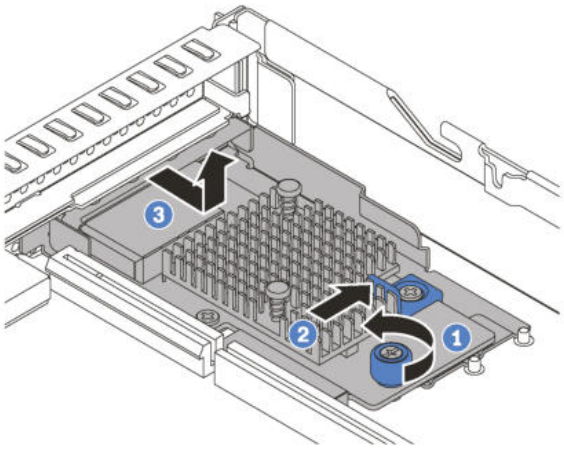


Figure 90. LOM adapter removal

Step 1. Loosen the thumbscrew that secures the LOM adapter.

Step 2. Push the LOM adapter out of the connector on the system board.

Step 3. Slide the LOM adapter as shown and lift the LOM adapter out of the chassis.

If you are instructed to return the old LOM adapter, follow all packaging instructions and use any packaging materials that are provided.

Install the LOM adapter

Use this information to install the LOM adapter.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the LOM adapter:

1. If riser 1 assembly is installed, remove it to access the LOM adapter slot.
2. Touch the static-protective package that contains the new LOM adapter to any unpainted surface on the outside of the server. Then, take the new LOM adapter out of the package and place it on a static-protective surface.

To install the LOM adapter, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

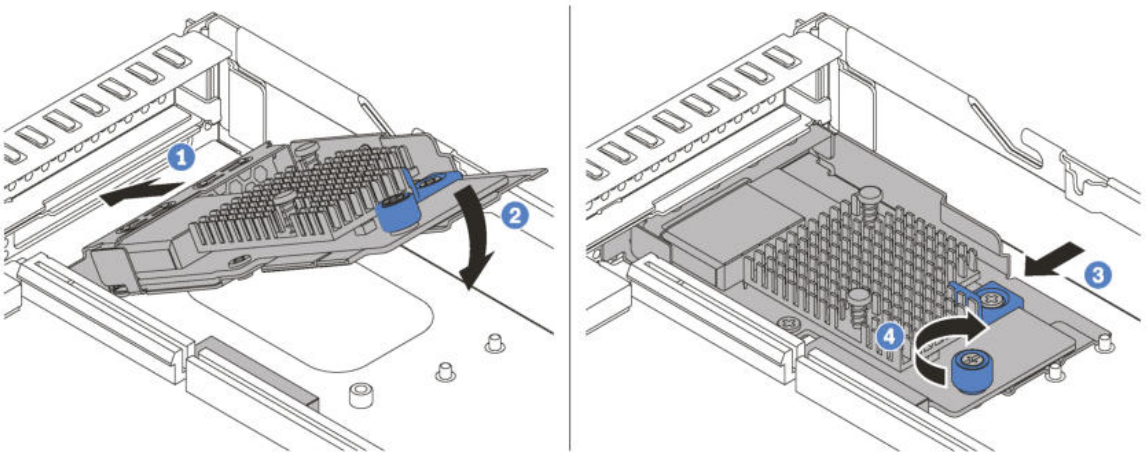


Figure 91. LOM adapter installation

Step 1. Insert the LOM adapter into the rear of the chassis at an angle as shown.

Step 2. Lower the LOM adapter and slide it to the rear of the chassis until the LOM adapter stops.

Step 3. Push the LOM adapter as shown to insert it into the connector on the system board.

Step 4. Tighten the thumbscrew to secure the LOM adapter.

After installing the LOM adapter, complete the parts replacement. See “Complete the parts replacement” on page 143.

Processor and heat sink replacement

Use the following procedures to replace an assembled processor and heat sink, known as a processor-heat-sink module (PHM), a processor, or a heat sink.

Attention:

- Before you begin replacing a processor, make sure that you have an alcohol cleaning pad (part number 00MP352) and gray thermal grease (part number 41Y9292).
- Cascade Lake processors are supported on the system board with part number 01PE840. If you use the system board with part number 00MX681, update your system firmware to the latest level before installing a Cascade Lake processor. Otherwise, the system cannot be powered on.

Important: The processor in your server can throttle, temporarily lowering speed to reduce heat output, in response to thermal conditions. In instances where the throttling period is of extremely short duration (100 ms or less), the only indication will be an entry in the event log. In these instances the event can be ignored and processor replacement is not required.

Remove a processor and heat sink

This task has instructions for removing an assembled processor and heat sink, known as a processor-heat-sink module (PHM), a processor, and a heat sink. All of these tasks require a Torx T30 driver.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Attention:

- Intel Xeon SP Gen 2 processors are supported on the system board with part number 01PE840. If you use the system board with part number 00MX681, update your system firmware to the latest level before installing a Intel Xeon SP Gen 2 processor. Otherwise, the system cannot be powered on.
- Each processor socket must always contain a cover or a PHM. When removing or installing a PHM, protect empty processor sockets with a cover.
- Do not touch the processor socket or processor contacts. Processor-socket contacts are very fragile and easily damaged. Contaminants on the processor contacts, such as oil from your skin, can cause connection failures.
- Remove and install only one PHM at a time. If the system board supports multiple processors, install the PHMs starting with the first processor socket.
- Do not allow the thermal grease on the processor or heat sink to come in contact with anything. Contact with any surface can compromise the thermal grease, rendering it ineffective. Thermal grease can damage components, such as electrical connectors in the processor socket. Do not remove the grease cover from a heat sink until you are instructed to do so.

Before you remove a PHM:

Note: The heat sink, processor, and processor retainer for your system might be different than those shown in the illustrations.

1. Remove the top cover. See "Remove the top cover" on page 52.
2. Remove the air baffle. See "Remove the air baffle" on page 55.
3. Remove any parts and disconnect any cables that might impede your access to the PHM.

Complete the following steps to remove a PHM.

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Remove the PHM from the system board.

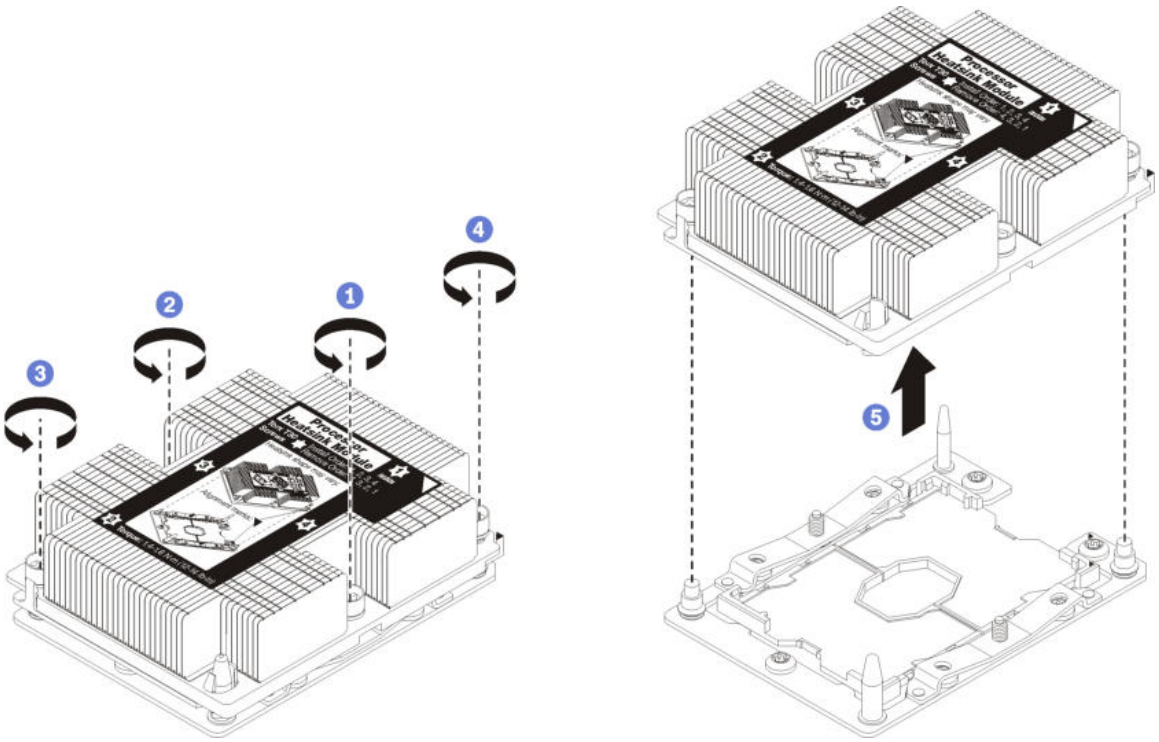


Figure 92. Removing a PHM

Attention: To prevent damage to components, make sure that you follow the indicated loosening sequence.

a. Fully loosen the Torx T30 captive fasteners on the processor-heat-sink module *in the removal sequence shown* on the heat-sink label.

b. Lift the processor-heat-sink module from the processor socket.

After you remove a PHM:

- If you are removing the PHM as part of a system board replacement, set the PHM aside.
- If you are replacing the processor or heat sink, separate the processor and its retainer from the heat sink.

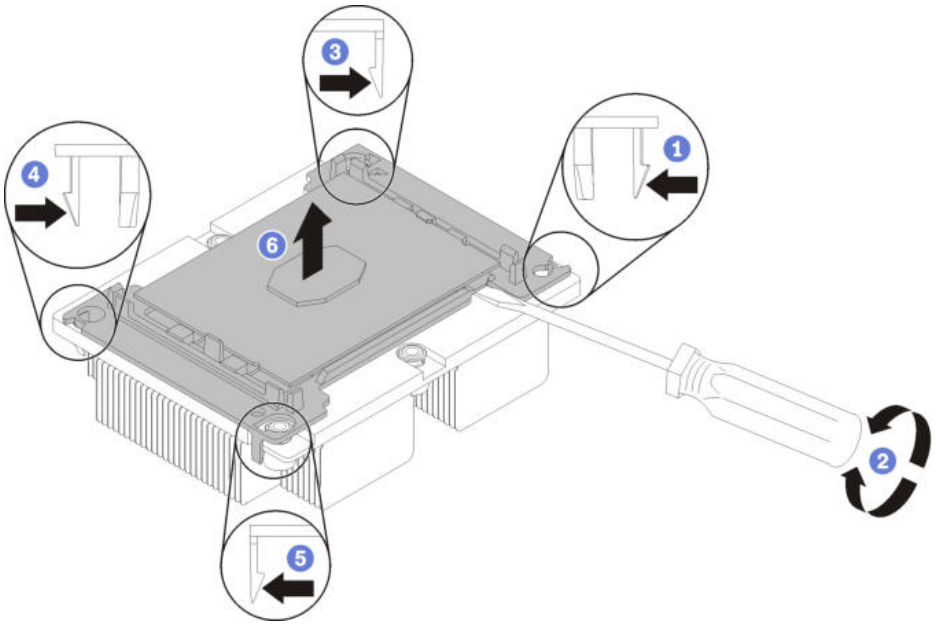


Figure 93. Separating a heat sink from a processor

1. Press the retaining clip at the corner of the processor retainer closest to the pry point; then, gently pry this corner of the retainer away from the heat sink with a flat-bladed screwdriver, using a twisting motion to break the processor-to-heat-sink seal.
2. Release the remaining retaining clips and lift the processor and retainer from the heat sink.
3. After separating the processor and retainer from the heat sink, hold the processor and retainer with the thermal-grease side down and the processor-contact side up to prevent the processor from falling out of the retainer.

   Note: The processor retainer will be removed and discarded in a later step and replaced with a new one.

- If you are replacing the processor, you will be reusing the heat sink. Wipe the thermal grease from the bottom of the heat sink using an alcohol cleaning pad.
- If you are replacing the heat sink, you will be reusing the processor. Wipe the thermal grease from the top of the processor using an alcohol cleaning pad.

If you are instructed to return the processor or heat sink, follow all packaging instructions and use any packaging materials that are provided.

Install a processor and heat sink

This task has instructions for installing an assembled processor and heat sink, known as a processor-heat-sink module (PHM), a processor, and a heat sink. All of these tasks require a Torx T30 driver.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Attention:

- Intel Xeon SP Gen 2 processors are supported on the system board with part number 01PE840. If you use the system board with part number 00MX681, update your system firmware to the latest level before installing a Intel Xeon SP Gen 2 processor. Otherwise, the system cannot be powered on.
- Each processor socket must always contain a cover or a PHM. When removing or installing a PHM, protect empty processor sockets with a cover.
- Do not touch the processor socket or processor contacts. Processor-socket contacts are very fragile and easily damaged. Contaminants on the processor contacts, such as oil from your skin, can cause connection failures.
- Remove and install only one PHM at a time. If the system board supports multiple processors, install the PHMs starting with the first processor socket.
- Do not allow the thermal grease on the processor or heat sink to come in contact with anything. Contact with any surface can compromise the thermal grease, rendering it ineffective. Thermal grease can damage components, such as electrical connectors in the processor socket. Do not remove the grease cover from a heat sink until you are instructed to do so.

Notes:

- PHMs are keyed for the socket where they can be installed and for their orientation in the socket.
- See http://www.lenovo.com/us/en/serverproven/ for a list of processors supported for your server. All processors on the system board must have the same speed, number of cores, and frequency.
- If you are going to install one of the following processors, replace your heat sink with a heat pipe heat sink (part number: 01KP650 or 01KP651):
  - Intel Xeon Platinum 8156 4C 105W 3.6 GHz processor
  - Intel Xeon Platinum 8256 4C 105W 3.8 GHz processor
  - Intel Xeon Gold 5120T 14C 105W 2.2 GHz processor
  - Intel Xeon Gold 5122 4C 105W 3.6 GHz processor
  - Intel Xeon Gold 5217 8C 115W 3.0 GHz processor
  - Intel Xeon Gold 5218T 16C 105W 2.1GHz processor
  - Intel Xeon Gold 5220T 18C 105W 2.2 GHz processor
  - Intel Xeon Gold 5222 4C 105W 3.8 GHz processor
  - Intel Xeon Gold 6126T 12C 125W 2.6 GHz processor
  - Intel Xeon Gold 6128 6C 115W 3.4 GHz processor
  - Intel Xeon Gold 6130T 16C 125W 2.1 GHz processor
  - Intel Xeon Gold 6138T 20C 125W 2.0 GHz processor
  - Intel Xeon Gold 6230N 20C 125W 2.3 GHz processor
  - Intel Xeon Gold 6230T 20C 125W 2.1 GHz processor
  - Intel Xeon Gold 6238T 22C 125W 1.9 GHz processor

- Before you install a new PHM or replacement processor, update your system firmware to the latest level. See “Firmware updates” on page 7.
- Installing an additional PHM can change the memory requirements for your system. See “Memory module installation rules” on page 80 for a list of processor-to-memory relationships.
- Optional devices available for your system might have specific processor requirements. See the documentation that comes with the optional device for information.

Before you install a PHM:

Note: The heat sink, processor, and processor retainer for your system might be different than those shown in the illustrations.

1. Remove the existing PHM, if one is installed. See “Remove a processor and heat sink” on page 123.

   Note: Replacement processors come with both rectangular and square processor retainers. A rectangular retainer comes attached to the processor. The square retainer can be discarded.

2. If you are replacing a heat sink, replace the processor retainer. *Processor retainers should not be reused.*
   a. Remove the old processor retainer.

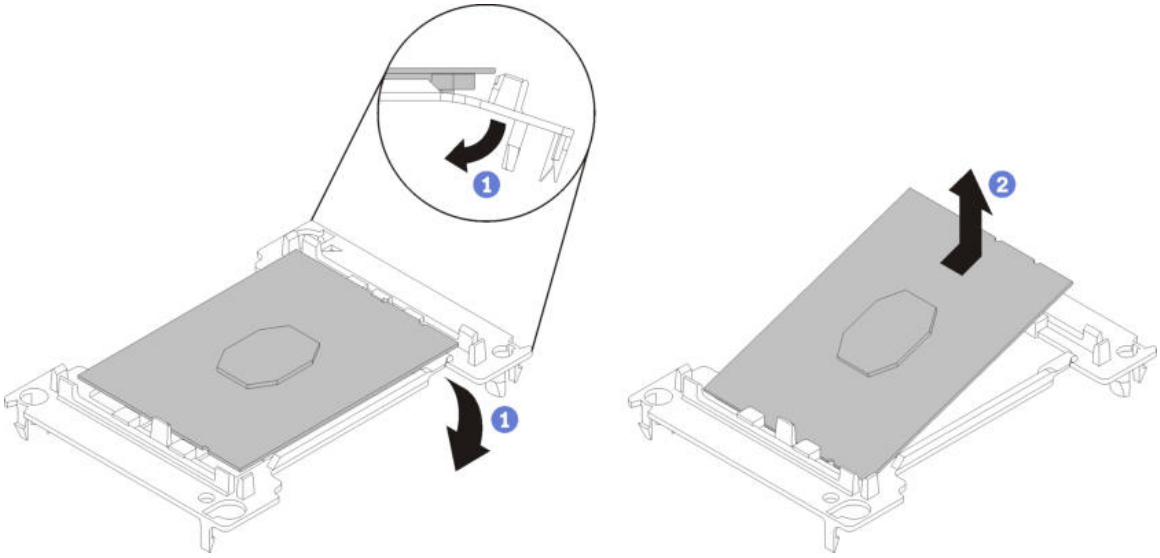


Figure 94. Removing a processor retainer

Note: When the processor is out of its retainer, hold the processor by the long edges to prevent touching the contacts or the thermal grease, if it is applied.

With the processor-contact side up, flex the ends of the retainer down and away from the processor to release the retaining clips; then, remove the processor from the retainer. Discard the old retainer.

   b. Install a new processor retainer.

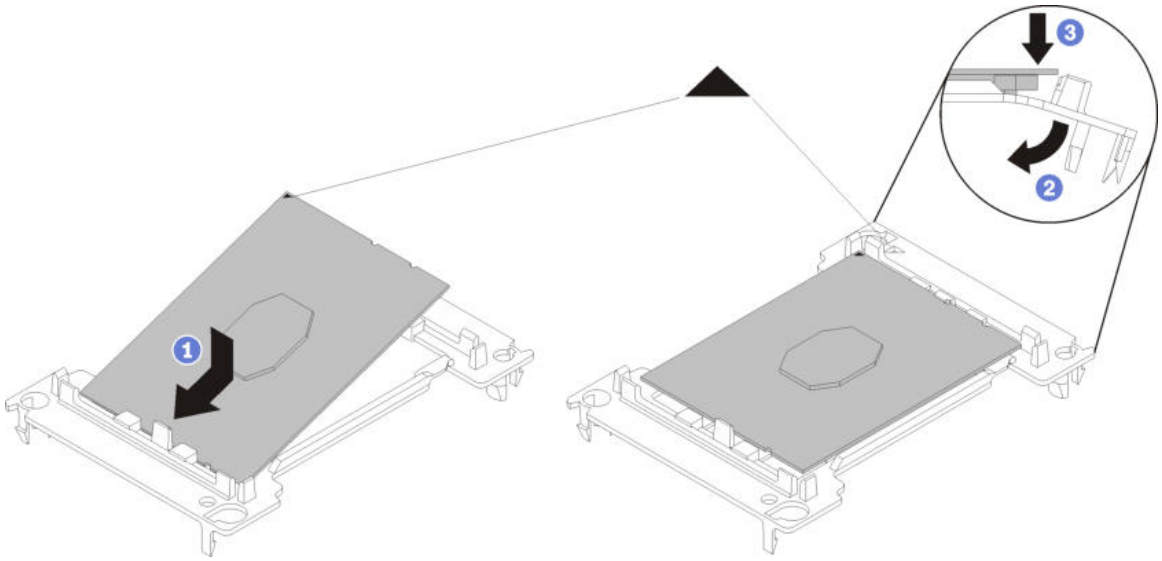


Figure 95. Installing a processor retainer

1) Position the processor on the new retainer so that the triangular marks align; then, insert the unmarked end of the processor into the retainer.
2) Holding the inserted end of the processor in place, flex the opposite end of the retainer down and away from the processor until you can press the processor under the clip on the retainer.

   To prevent the processor from falling out of the retainer after it is inserted, keep the processor-contact side up and hold the processor-retainer assembly by the sides of the retainer.
3) If there is any old thermal grease on the processor, gently clean the top of the processor using an alcohol cleaning pad.

   Note: If you are applying new thermal grease on the top of the processor, make sure to do it after the alcohol has fully evaporated.

3. If you are replacing a processor:
   a. Remove the processor identification label from the heat sink and replace it with the new label that comes with the replacement processor.
   b. Apply the new thermal grease on the top of the new processor with syringe by forming four uniformly spaced dots, while each dot consists of about 0.1 ml of thermal grease.

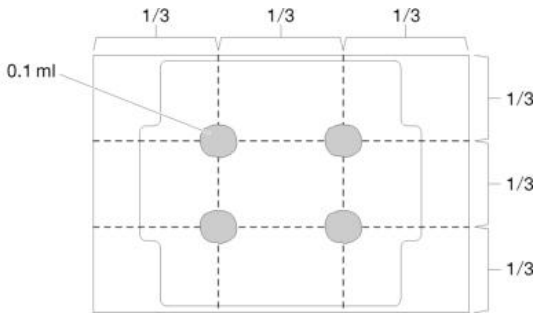


Figure 96. Proper shape of the thermal grease

4. If you are replacing a heat sink, remove the processor identification label from the old heat sink and place it on the new heat sink in the same location. The label is on the side of the heat sink closet to the triangular alignment mark.

If you are unable to remove the label and place it on the new heat sink, or if the label is damaged during transfer, write the processor serial number from the processor identification label on the new heat sink in the same location as the label would be placed using a permanent marker.

5. Assemble the processor and heat sink, if these components are separate.

   Notes:

   - If you are replacing a processor, install the heat sink onto the processor and retainer while the processor and retainer are in the shipping tray.
   - If you are replacing a heat sink, remove the heat sink from its shipping tray and place the processor and retainer in the opposite half of the heat sink shipping tray with the processor-contact side down. To prevent the processor from falling out of the retainer, hold the processor-retainer assembly by its sides with the processor-contact side up until you turn it over to fit in the shipping tray.

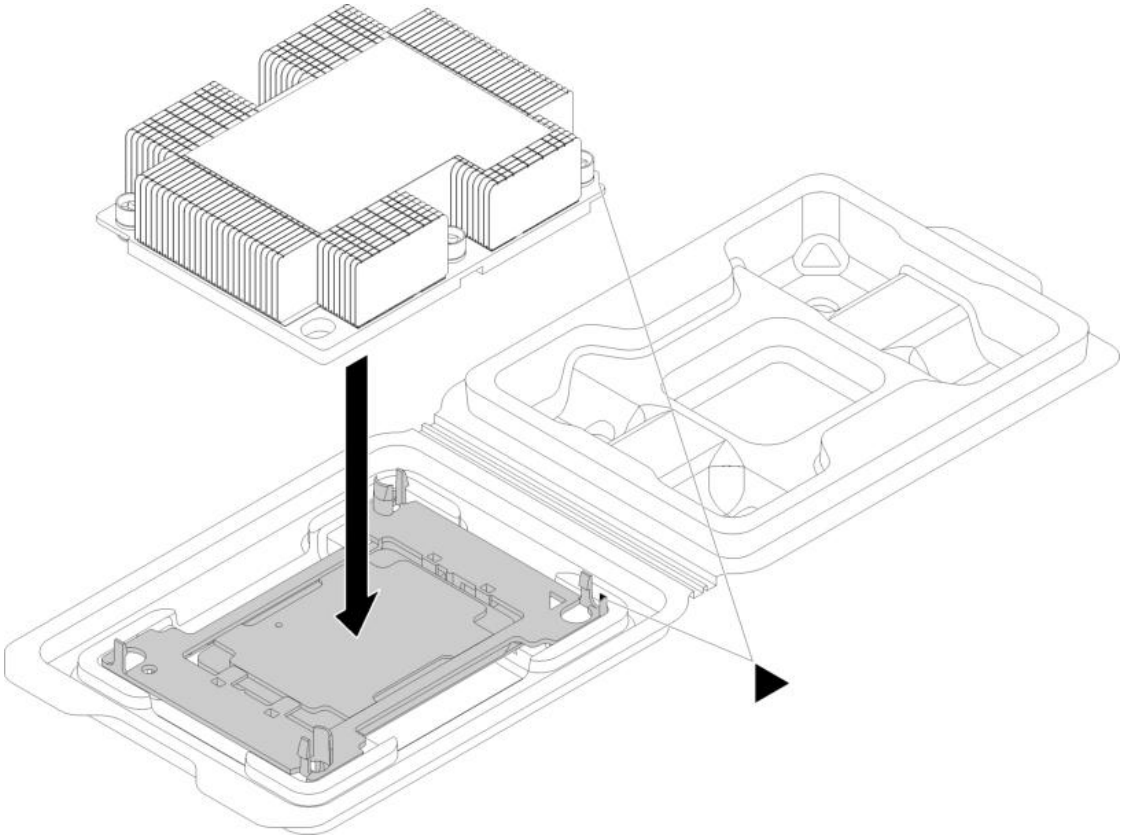


Figure 97. Assembling a PHM in the shipping tray

   a. Align the triangular marks on the processor retainer and the heat sink or align the triangular mark on the processor retainer with the notched corner of the heat sink.
   b. Insert the processor-retainer clips into the holes on the heat sink.
   c. Press the retainer into place until the clips at all four corners engage.

Complete the following steps to install a PHM.

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Remove the processor socket cover, if one is installed on the processor socket, by placing your fingers in the half-circles at each end of the cover and lifting it from the system board.

Step 2. Install the processor-heat-sink module on the system board.

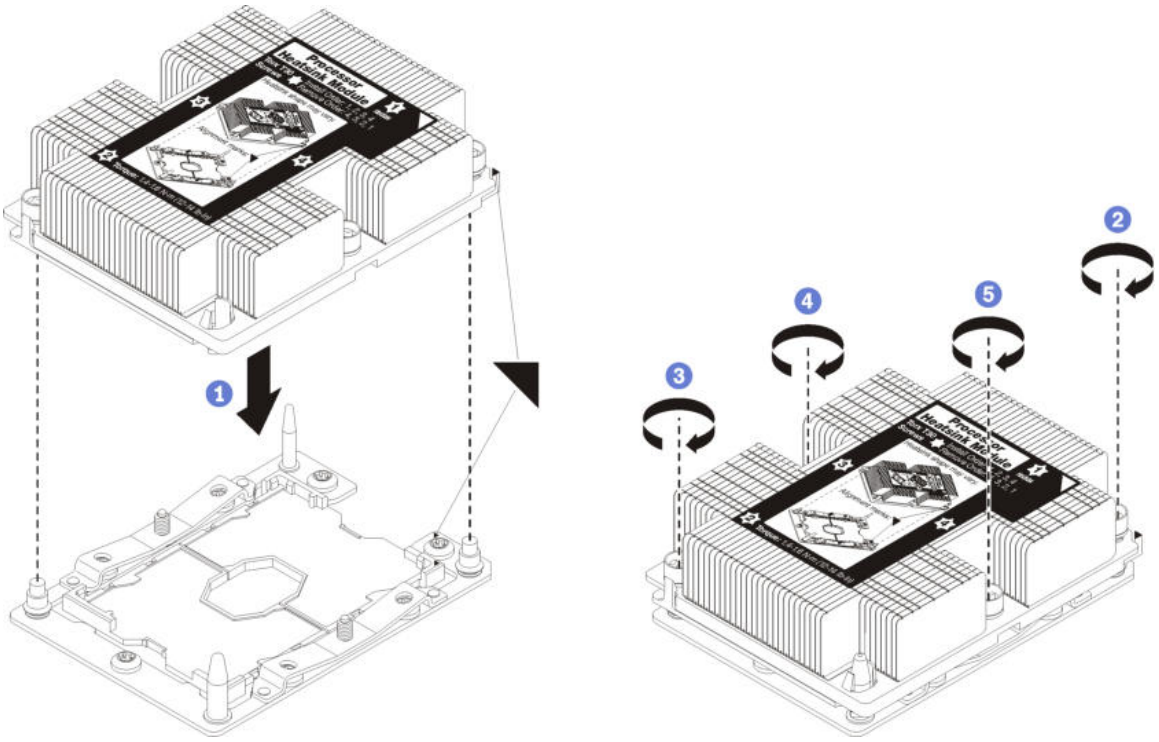


Figure 98. Installing a PHM

a. Align the triangular marks and guide pins on the processor socket with the PHM; then, insert the PHM into the processor socket.

Attention: To prevent damage to components, make sure that you follow the indicated tightening sequence.

b. Fully tighten the Torx T30 captive fasteners *in the installation sequence shown* on the heat-sink label. Tighten the screws until they stop; then, visually inspect to make sure that there is no gap between the screw shoulder beneath the heat sink and the processor socket. (For reference, the torque required for the nuts to fully tighten is 1.4 — 1.6 newton-meters, 12 — 14 inch-pounds).

After you install a PHM:

1. Complete the parts replacement. See “Complete the parts replacement” on page 143.

System board replacement

Use this information to remove and install the system board.

Important: Before you return the system board, make sure that you install the CPU socket dust covers from the new system board. To replace a CPU socket dust cover:

1. Take a dust cover from the CPU socket assembly on the new system board and orient it correctly above the CPU socket assembly on the removed system board.
2. Gently press down the dust cover legs to the CPU socket assembly, pressing on the edges to avoid damage to the socket pins. You might hear a click on the dust cover is securely attached.
3. **Make sure** that the dust cover is securely attached to the CPU socket assembly.

S017



CAUTION:
Hazardous moving fan blades nearby. Keep fingers and other body parts away.

S012



CAUTION:
Hot surface nearby.

Remove the system board

Use this information to remove the system board.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the system board:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. Record where the cables are connected to the system board; then, disconnect them.

   Attention: Disengage all latches, cable clips, release tabs, or locks on cable connectors beforehand. Failing to release them before removing the cables will damage the cable connectors on the system board. Any damage to the cable connectors may require replacing the system board.
3. Remove any of the following components that are installed on the system board and put them in a safe, static-protective place. See the related topics in Chapter 3 "Hardware replacement procedures" on page 41.
   - Air baffle

- System fans
- Processor-heat-sink module (PHM)

  Note: Do not disassemble the PHM.
- DIMMs
- CMOS battery
- PCIe adapters
- Riser assembly
- M.2 backplane
- LOM adapter
- TCM/TPM (for Chinese Mainland only)

4. Pull out the power supplies a little bit. Ensure that they are disconnected from the system board.

To remove the system board, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

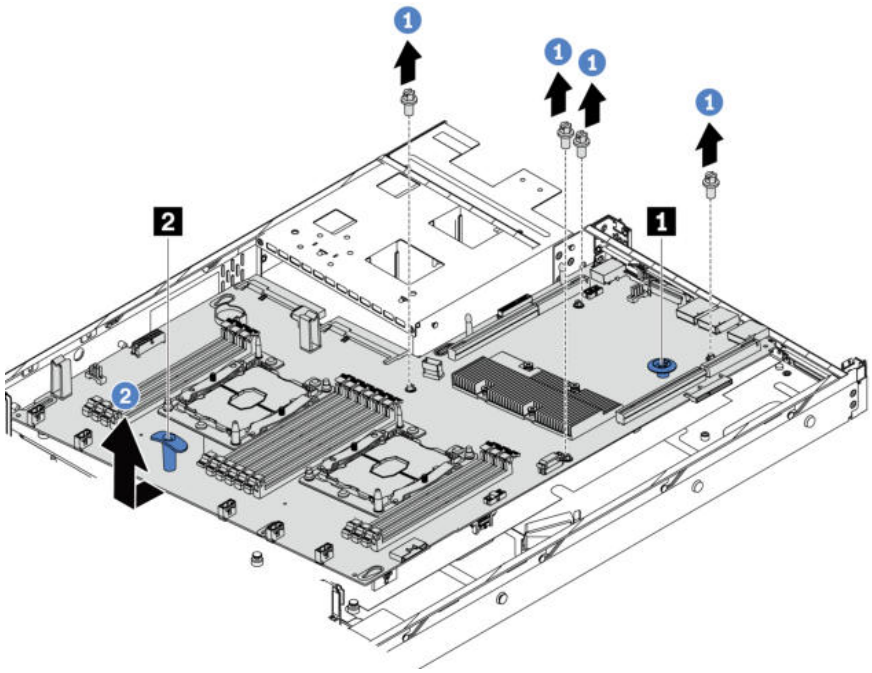


Figure 99. System board removal

Step 1. Remove the screws that secure the system board, and put the screws in a safe place.

Step 2. Grasp the system board by the release pin 1 and the lift handle 2 at the same time and gently slide the system board to the front of the server. Then lift and tilt the system board upwards to remove it from the server.

If you are instructed to return the old system board, follow all packaging instructions and use any packaging materials that are provided.

Important: Before you return the system board, make sure that you install the CPU socket dust covers from the new system board. To replace a CPU socket dust cover:

1. Take a dust cover from the CPU socket assembly on the new system board and orient it correctly above the CPU socket assembly on the removed system board.
2. Gently press down the dust cover legs to the CPU socket assembly, pressing on the edges to avoid damage to the socket pins. You might hear a click on the dust cover is securely attached.
3. **Make sure** that the dust cover is securely attached to the CPU socket assembly.

Install the system board

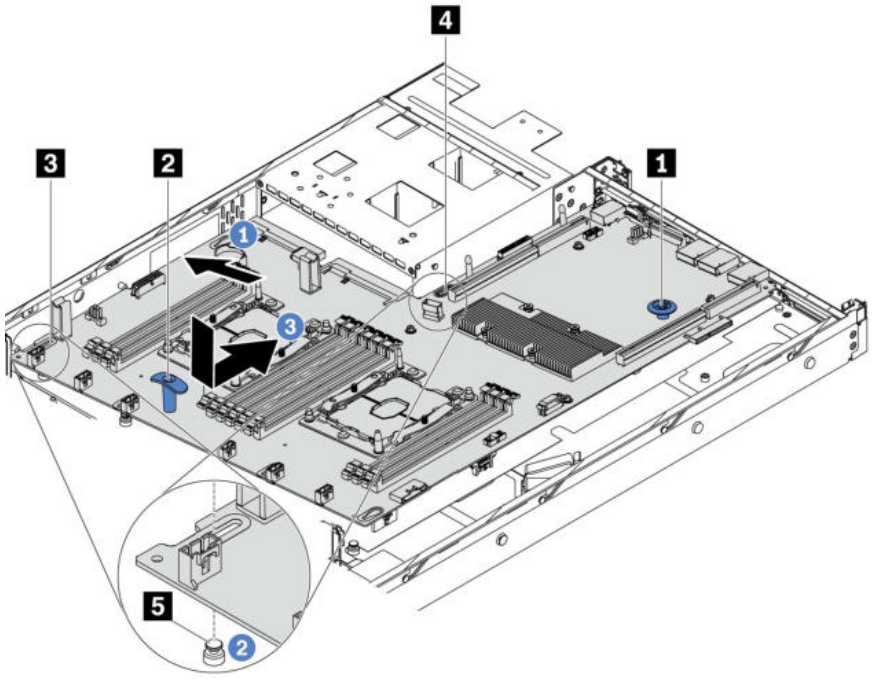
Use this information to install the system board.

	"**Read** the installation Guidelines" on page 41	 "**Power off** the server for this task" on page 11
	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43	

Before installing the system board, touch the static-protective package that contains the new system board to any unpainted surface on the outside of the server. Then, take the new system board out of the package and place it on a static-protective surface.

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

To install the system board, complete the following steps:



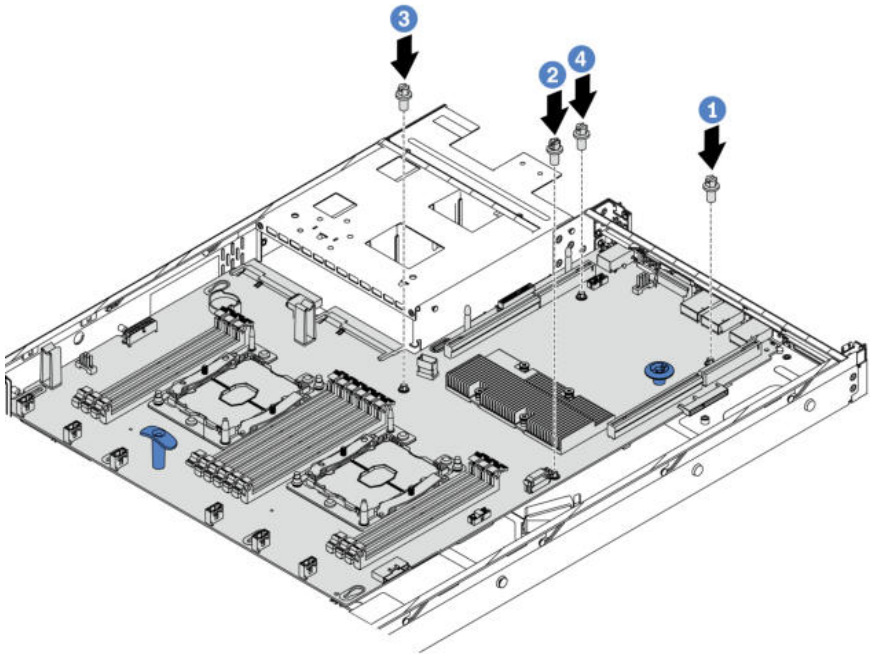
Step 1. Grasp the system board by the release pin 1 and the lift handle 2 at the same time, and tilt the system board at an angle of approximately 20 degrees as shown.

Step 2. Align the hole 3 on the system board with the corresponding mounting stud 5 on the chassis first, and then align the hole 4 by the same way.

Note: Before you align the two holes, prevent the system board from touching the mounting studs on the chassis.

Step 3. Lower the system board into the chassis and slide it to the rear of the chassis until it clicks into position.

Step 4. Install the four screws in the following sequence.



After installing the system board:

1. Push the power supplies into the bays until they click into place.
2. Install any components that you removed from the failing system board. See the related topics in Chapter 3 “Hardware replacement procedures” on page 41.
3. Complete the parts replacement. See “Complete the parts replacement” on page 143.
4. Update the Universally Unique Identifier (UUID) and DMI/SMBIOS data with new vital product data (VPD). Use the Lenovo XClarity Provisioning Manager to update the UUID and DMI/SMBIOS data. See “Update the Universal Unique Identifier (UUID)” on page 135 and “Update the DMI/SMBIOS data” on page 137.
5. Enable TPM/TCM. See “Enable TPM/TCM” on page 139.
6. Optionally, enable Secure Boot.

Update the Universal Unique Identifier (UUID)

The Universal Unique Identifier (UUID) must be updated when the system board is replaced. Use the Lenovo XClarity Provisioning Manager to update the UUID in the UEFI-based server. Lenovo XClarity Essentials OneCLIcan be used to update the UUID in the UEFI-based server as a command line option. Lenovo XClarity Essentials OneCLI is an online tool that supports several operating systems; make sure that you download the version for your operating system.

1. Start the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface.
2. From the System Summary page, click **Update VPD**.
3. Update the UUID.

   Note: You can use Lenovo XClarity Essentials OneCLI to update the UUID for the server.

To download Lenovo XClarity Essentials OneCLI, go to the following site:

https://datacentersupport.lenovo.com/solutions/HT116433

Lenovo XClarity Essentials OneCLI sets the UUID in the Lenovo XClarity Controller. Select one of the following methods to access the Lenovo XClarity Controller and set the UUID:

- Operate from the target system, such as LAN or keyboard console style (KCS) access
- Remote access to the target system (TCP/IP based)

Step 1. Copy and unpack the OneCLI package, which also includes other required files, to the server. Make sure that you unpack the OneCLI and the required files to the same directory.

Step 2. After you have OneCLI in place, use the following command syntax to set the UUID:

```
onecli config set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value> [access_method]
```

Where:

<uuid_value>
Up to 16-byte hexadecimal value assigned by you.

[access_method]
The access method that you selected to use from the following methods:

- Online authenticated LAN access, type the command:

  Example that does not use the user ID and password default values:
  ```
  onecli config set SYSTEM_PROD_DATA.SYsInfoUUID <uuid_value> --user <user_id>
  --password <password>
  ```

  Example that uses the user ID and password default values:
  ```
  onecli config set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>
  ```

- Online KCS access (unauthenticated and user restricted):

  You do not need to specify a value for *access_method* when you use this access method.

  Example:
  ```
  onecli config set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>
  ```

  Note: The KCS access method uses the IPMI/KCS interface, which requires that the IPMI driver be installed.

- Remote LAN access, type the command:

  Note: When using the remote LAN/WAN access method to access Lenovo XClarity Controller from a client, the *host* and the *xcc_external_ip* address are required parameters.

  ```
  [--imm xcc_user_id:xcc_password@xcc_external_ip]
  ```

  or

  ```
  [--bmc xcc_user_id:xcc_password@xcc_external_ip]
  ```

  Where:

  xcc_external_ip
  The BMC/IMM/XCC external IP address. There is no default value. This parameter is required.

  xcc_user_id
  The BMC/IMM/XCC account name (1 of 12 accounts). The default value is USERID.

  xcc_password
  The BMC/IMM/XCC account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

Note: BMC, IMM, or XCC external IP address, account name, and password are all valid for this command.

Example that does use the user ID and password default values:
```
onecli config set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>
```

Step 3. Restart the Lenovo XClarity Controller.

Step 4. Restart the server.

Update the DMI/SMBIOS data

The Desktop Management Interface (DMI) must be updated when the system board is replaced. Use the Lenovo XClarity Provisioning Manager to update the DMI in the UEFI-based server. Lenovo XClarity Essentials OneCLIcan be used to update the UUID in the UEFI-based server as a command line option. Lenovo XClarity Essentials OneCLI is an online tool that supports several operating systems; make sure that you download the version for your operating system.

1. Start the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface.
2. From the System Summary page, click **Update VPD**.
3. Update the asset tag information.

Note: You can use Lenovo XClarity Essentials OneCLI to update the asset tag for the server.

To download Lenovo XClarity Essentials OneCLI, go to the following site:

https://datacentersupport.lenovo.com/solutions/HT116433

Lenovo XClarity Essentials OneCLI sets the DMI in the Lenovo XClarity Controller. Select one of the following methods to access the Lenovo XClarity Controller and set the DMI:

- Operate from the target system, such as LAN or keyboard console style (KCS) access
- Remote access to the target system (TCP/IP based)

Step 1. After you haveLenovo XClarity Essentials OneCLI in place, type the following commands to set the DMI:
```
onecli config set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model> [access_method]
onecli config set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n> [access_method]
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag> [access_method]
```

Where:

<m/t_model>
The server machine type and model number. Type `mtm xxxxyyy`, where *xxxx* is the machine type and *yyy* is the server model number.

<s/n>
The serial number on the server. Type `sn zzzzzzz`, where *zzzzzzz* is the serial number.

<asset_method>
The server asset tag number. Type `asset aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa`, where *aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa* is the asset tag number.

[access_method]
The access method that you select to use from the following methods:

- Online authenticated LAN access, type the command:

```
[--imm xcc_user_id:xcc_password@xcc_internal_ip]
```

or

```
[--bmc xcc_user_id:xcc_password@xcc_internal_ip]
```

Where:

xcc_internal_ip
The BMC/IMM/XCC internal LAN/USB IP address. The default value is 169.254.95.118.

xcc_user_id
The BMC/IMM/XCC account name (1 of 12 accounts). The default value is USERID.

xcc_password
The BMC/IMM/XCC account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

Notes:

1. BMC, IMM, or XCC internal LAN/USB IP address, account name, and password are all valid for this command.
2. If you do not specify any of these parameters, OneCLI will use the default values. When the default values are used and OneCLI is unable to access the Lenovo XClarity Controller using the online authenticated LAN access method, OneCLI will automatically use the unauthenticated KCS access method.

Examples that do use the user ID and password default values:

```
onecli config set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model>
onecli config set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n>
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
```

- Online KCS access (unauthenticated and user restricted): You do not need to specify a value for *access_method* when you use this access method.

  Note: The KCS access method uses the IPMI/KCS interface, which requires that the IPMI driver be installed.

  The following commands are examples of not using the user ID and password default values:

  ```
  onecli config set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model>
  onecli config set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n>
  onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
  ```

- Remote LAN access, type the command:

  Note: When using the remote LAN/WAN access method to access Lenovo XClarity Controller from a client, the *host* and the *xcc_external_ip* address are required parameters.

  ```
  [--imm xcc_user_id:xcc_password@xcc_external_ip]
  ```
  or
  ```
  [--bmc xcc_user_id:xcc_password@xcc_external_ip]
  ```

  Where:

  xcc_external_ip
  The BMC/IMM/XCC IP address. There is no default value. This parameter is required.

  xcc_user_id
  The BMC/IMM/XCC account (1 of 12 accounts). The default value is USERID.

  xcc_password

The BMC/IMM/XCC account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

Note: BMC, IMM, or XCC internal LAN/USB IP address, account name, and password are all valid for this command.

Examples that do use the user ID and password default values:

```
onecli config set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model> --host <xcc_ip>
onecli config set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n> --host <xcc_ip>
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag> --host <xcc_ip>
```

Step 2. Reset IMM to the factory defaults. Go to https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_resettingthexcc.html for more information.

Step 3. Reset the Lenovo XClarity Controller to the factory defaults. Go to https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_resettingthexcc.html for more information.

Enable TPM/TCM

The server supports Trusted Platform Module (TPM), Version 1.2 or Version 2.0.

Note: For customers in Chinese Mainland, integrated TPM is not supported. However, customers in Chinese Mainland can install a Trusted Cryptographic Module (TCM) adapter or a TPM adapter (sometimes called a daughter card).

When a system board is replaced, you must make sure that the TPM/TCM policy is set correctly.

CAUTION:
Take special care when setting the TPM/TCM policy. If it is not set correctly, the system board can become unusable.

Set the TPM/TCM policy

By default, a replacement system board is shipped with the TPM/TCM policy set to **undefined**. You must modify this setting to match the setting that was in place for the system board that is being replaced.

You can set the TPM/TCM policy from Lenovo XClarity Provisioning Manager.

Complete the following steps to set the TPM/TCM policy.

Step 1. Start the server and when prompted, press F1 to display Lenovo XClarity Provisioning Manager.

Step 2. If the power-on Administrator password is required, enter the password.

Step 3. From the System Summary page, click **Update VPD**.

Step 4. Set the policy to one of the following settings.

- **TCM enabled - China only**. Customers in Chinese Mainland should choose this setting if a TCM adapter is installed.
- **NationZ TPM 2.0 enabled - China only**. Customers in Chinese Mainland should choose this setting if a NationZ TPM 2.0 adapter is installed.
- **TPM enabled - ROW**. Customers outside of Chinese Mainland should choose this setting.
- **Permanently disabled**. Customers in Chinese Mainland should use this setting if no TPM or TCM adapter is installed.

Although the setting **undefined** is available as a policy setting, it should not be used.

Notes: You can use Lenovo XClarity Essentials OneCLI to update the TPM/TCM policy. Please note that a Local IPMI user and password must be setup in Lenovo XClarity Controller for remote accessing to the target system.

1. Read TpmTcmPolicyLock to check whether the TPM_TCM_POLICY has been locked:
   `OneCli.exe config show imm.TpmTcmPolicyLock --override --imm <userid>:<password>@<ip_address>`

   Note: The imm.TpmTcmPolicyLock value must be 'Disabled', which means TPM_TCM_POLICY is NOT locked and changes to the TPM_TCM_POLICY are permitted. If the return code is ‘Enabled’ then no changes to the policy are permitted. The planar may still be used if the desired setting is correct for the system being replaced.
2. Configure the TPM_TCM_POLICY into XCC:
   - For the customer in Chinese Mainland with no TCM:
     `OneCli.exe config set imm.TpmTcmPolicy "NeitherTpmNorTcm" --override --imm <userid>:<password>@<ip_address>`
   - For the customer in Chinese Mainland that has installed TCM module on the original system (TCM module should be moved to the FRU prior to changing policy)
     `OneCli.exe config set imm.TpmTcmPolicy "TcmOnly" --override --imm <userid>:<password>@<ip_address>`
   - For the customer outside of Chinese Mainland:
     `OneCli.exe config set imm.TpmTcmPolicy "TpmOnly" --override --imm <userid>:<password>@<ip_address>`
3. Issue reset command to reset system:
   `OneCli.exe misc ospower reboot --imm <userid>:<password>@<ip_address>`
4. Read back the value to check whether the change has been accepted:
   `OneCli.exe config show imm.TpmTcmPolicy --override --imm <userid>:<password>@<ip_address>`

   Notes:
   - If the read back value is matched it means the TPM_TCM_POLICY has been set correctly.

     imm.TpmTcmPolicy is defined as below:
     - Value 0 use string “Undefined” , which means UNDEFINED policy.
     - Value 1 use string “NeitherTpmNorTcm”, which means TPM_PERM_DISABLED.
     - Value 2 use string “TpmOnly”, which means TPM_ALLOWED.
     - Value 4 use string “TcmOnly”, which means TCM_ALLOWED.
   - Below 4 steps must also be used to ‘lock’ the TPM_TCM_POLICY when using OneCli/ASU commands:
5. Read TpmTcmPolicyLock to check whether the TPM_TCM_POLICY has been locked , command as below:

   `OneCli.exe config show imm.TpmTcmPolicyLock --override --imm <userid>:<password>@<ip_address>`

   The value must be 'Disabled', it means TPM_TCM_POLICY is NOT locked and must be set.
6. Lock the TPM_TCM_POLICY:
   `OneCli.exe config set imm.TpmTcmPolicyLock"Enabled"--override --imm <userid>:<password>@<ip_address>`
7. Issue reset command to reset system, command as below:
   `OneCli.exe misc ospower reboot --imm <userid>:<password>@<ip_address>`

   During the reset, UEFI will read the value from imm.TpmTcmPolicyLock, if the value is 'Enabled' and the imm.TpmTcmPolicy value is invalid, UEFI will lock the TPM_TCM_POLICY setting.

   The valid value for imm.TpmTcmPolicy includes 'NeitherTpmNorTcm', 'TpmOnly' and 'TpmOnly'.

If the imm.TpmTcmPolicy is set as 'Enabled' but imm.TpmTcmPolicy value is invalid, UEFI will reject the 'lock' request and change imm.TpmTcmPolicy back to 'Disabled'.

8. Read back the value to check whether the ‘Lock’ is accepted or rejected. command as below:

   ```
   OneCli.exe config show imm.TpmTcmPolicy --override --imm <userid>:<password>@<ip_address>
   ```

   Note: If the read back value is changed from'Disabled' to 'Enabled' that means the TPM_ TCM_POLICY has been locked successfully. There is no method to unlock a policy once it has been set other than replacing system board.

   imm.TpmTcmPolicyLockis defined as below:

   Value 1 use string “Enabled" , which means lock the policy. Other values are not accepted.

   Procedure also requires that Physical Presence is enabled. The Default value for FRU will be enabled.
   ```
   PhysicalPresencePolicyConfiguration.PhysicalPresencePolicy=Enable
   ```

Assert Physical Presence

Before you can assert Physical Presence, the Physical Presence Policy must be enabled. By default, the Physical Presence Policy is enabled with a timeout of 30 minutes.

If the Physical Presence Policy is enabled, you can assert Physical Presence through the Lenovo XClarity Controller or through hardware jumpers on the system board.

Notes: If the Physical Presence Policy has been disabled:

1. Set the hardware Physical Presence jumper on the system board to assert Physical Presence.
2. Enable the Physical Presence Policy using either F1 (UEFI Settings) or Lenovo XClarity Essentials OneCLI.

Assert Physical Presence through the Lenovo XClarity Controller

Complete the following steps to assert Physical Presence through the Lenovo XClarity Controller:

1. Log in to the Lenovo XClarity Controller interface.

   For information about logging in to the Lenovo XClarity Controller, see:

   http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/dw1lm_c_chapter2_openingandusing.html
2. Click **BMC Configuration → Security** and verify that Physical Presence is set to **assert**.

Assert Physical Presence through the hardware

You can also assert hardware Physical Presence through the use of a jumper on the system board. For more information about asserting hardware Physical Presence through the use of a jumper, see “System board switches and jumpers” on page 25

Set the TPM version

To be able to set the TPM version, Physical Presence must be asserted.

The Lenovo XClarity Provisioning Manager or the Lenovo XClarity Essentials OneCLI can be used to set the TPM version.

To set the TPM version:

1. Download and install Lenovo XClarity Essentials OneCLI.
   a. Go to http://datacentersupport.lenovo.com and navigate to the support page for your server.

b. Click **Drivers & Software**.

c. Navigate to the version of Lenovo XClarity Essentials OneCLI for your operating system and download the package.

2. Run the following command to set the TPM version:

   Note: You can change the TPM version from 1.2 to 2.0 and back again. However, you can toggle between versions a maximum of 128 times.

   To set the TPM version to version 2.0:
   ```
   OneCli.exe config set TrustedComputingGroup.DeviceOperation "Update to TPM2.0 compliant"
              --bmc userid:password@ip_address
   ```

   To set the TPM version to version 1.2:
   ```
   OneCli.exe config set TrustedComputingGroup.DeviceOperation "Update to TPM1.2 compliant"
             --bmc userid:password@ip_address
   ```

   where:

   - *<userid>:<password>* are the credentials used to access the BMC (Lenovo XClarity Controller interface) of your server. The default user ID is USERID, and the default password is PASSW0RD (zero, not an uppercase o)
   - *<ip_address>* is the IP address of the BMC.

   For more information about the Lenovo XClarity Essentials OneCLI **set** command, see:

   http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_set_command.html

3. Alternatively, you can use the following Advanced Settings Utility (ASU) commands:

   To set the TPM version to version 2.0:
   ```
   asu64 set TPMVersion.TPMVersion "Update to TPM2.0 compliant" --host <ip_address>
             --user <userid> --password <password>  --override
   ```

   To set the TPM version to version 1.2:
   ```
   asu64 set TPMVersion.TPMVersion "Update to TPM1.2 compliant" --host <ip_address>
             --user <userid> --password <password>  --override
   ```

   where:

   - *<userid>* and *<password>* are the credentials used to the BMC (Lenovo XClarity Controller interface) of your server. The default user ID is USERID, and the default password is PASSW0RD (zero, not an uppercase o)
   - *<ip_address>* is the IP address of the BMC.

Enable UEFI Secure Boot

Optionally, you can enable UEFI Secure Boot.

Physical Presence must be asserted if you are going to enable UEFI Secure Boot. See “Assert Physical Presence” on page 141.

For information about accessing the Lenovo XClarity Controller interface, see:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/dw1lm_c_chapter2_openingandusing.html

There are two methods available to enable UEFI Secure Boot:

- From Lenovo XClarity Provisioning Manager

  To enable UEFI Secure Boot from Lenovo XClarity Provisioning Manager:

1. Start the server and when prompted, press F1 to display Lenovo XClarity Provisioning Manager.
2. If the power-on Administrator password is required, enter the password.
3. From the UEFI Setup page, click **System Settings → Security → Secure Boot**.
4. Enable Secure Boot and save the settings.

- From Lenovo XClarity Essentials OneCLI

  To enable UEFI Secure Boot from Lenovo XClarity Essentials OneCLI:

  1. Download and install Lenovo XClarity Essentials OneCLI.

     To download Lenovo XClarity Essentials OneCLI, go to the following site:

     https://datacentersupport.lenovo.com/solutions/HT116433

  2. Run the following command to enable Secure Boot:

     ```
     OneCli.exe config set SecureBootConfiguration.SecureBootSetting Enabled  --override
                      --bmc <userid>:<password>@<ip_address>
     ```

     where:

     – *<userid>:<password>* are the credentials used to access the BMC (Lenovo XClarity Controller interface) of your server. The default user ID is USERID, and the default password is PASSW0RD (zero, not an uppercase o)

     – *<ip_address>* is the IP address of the BMC.

     For more information about the Lenovo XClarity Essentials OneCLI **set** command, see:

     http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_set_command.html

Complete the parts replacement

Use this information to complete the parts replacement.

To complete the parts replacement, do the following:

1. Ensure that all components have been reassembled correctly and that no tools or loose screws are left inside your server.
2. Properly route and secure the cables in the server. See “Internal cable routing” on page 28.
3. If you have removed the top cover, reinstall it. See “Install the top cover” on page 54.
4. Reconnect external cables and power cords to the server.

   Attention: To avoid component damage, connect the power cords last.
5. Update the server configuration if necessary.
   - Download and install the latest device drivers: http://datacentersupport.lenovo.com
   - Update the system firmware. See “Firmware updates” on page 7.
   - Use the Lenovo XClarity Provisioning Manager to update the UEFI configuration. For more information, see: http://sysmgt.lenovofiles.com/help/topic/LXPM/UEFI_setup.html
   - Use the Lenovo XClarity Provisioning Manager to configure the RAID if you have installed or removed a hot-swap drive, a RAID adapter, or the M.2 backplane and M.2 drive. For more information, see: http://sysmgt.lenovofiles.com/help/topic/LXPM/RAID_setup.html

Note: Make sure the latest version of ThinkSystem M.2 with Mirroring Enablement Kit Firmware is applied to avoid virtual disk/array missing after system board replacement.

Chapter 4. Problem determination

Use the information in this section to isolate and resolve issues that you might encounter while using your server.

Lenovo servers can be configured to automatically notify Lenovo Support if certain events are generated. You can configure automatic notification, also known as Call Home, from management applications, such as the Lenovo XClarity Administrator. If you configure automatic problem notification, Lenovo Support is automatically alerted whenever a server encounters a potentially significant event.

To isolate a problem, you should typically begin with the event log of the application that is managing the server:

- If you are managing the server from the Lenovo XClarity Administrator, begin with the Lenovo XClarity Administrator event log.
- If you are managing the server from the Chassis Management Module 2, begin with the Chassis Management Module 2 event log.
- If you are using some other management application, begin with the Lenovo XClarity Controller event log.

Event logs

An *alert* is a message or other indication that signals an event or an impending event. Alerts are generated by the Lenovo XClarity Controller or by UEFI in the servers. These alerts are stored in the Lenovo XClarity Controller Event Log. If the server is managed by the Chassis Management Module 2 or by the Lenovo XClarity Administrator, alerts are automatically forwarded to those management applications.

Note: For a listing of events, including user actions that might need to be performed to recover from an event, see the *Messages and Codes Reference*, which is available at:http://thinksystem.lenovofiles.com/help/topic/7X07/pdf_files.html

Lenovo XClarity Administrator event log

If you are using Lenovo XClarity Administrator to manage server, network, and storage hardware, you can view the events from all managed devices through the XClarity Administrator.

© Copyright Lenovo 2017, 2020

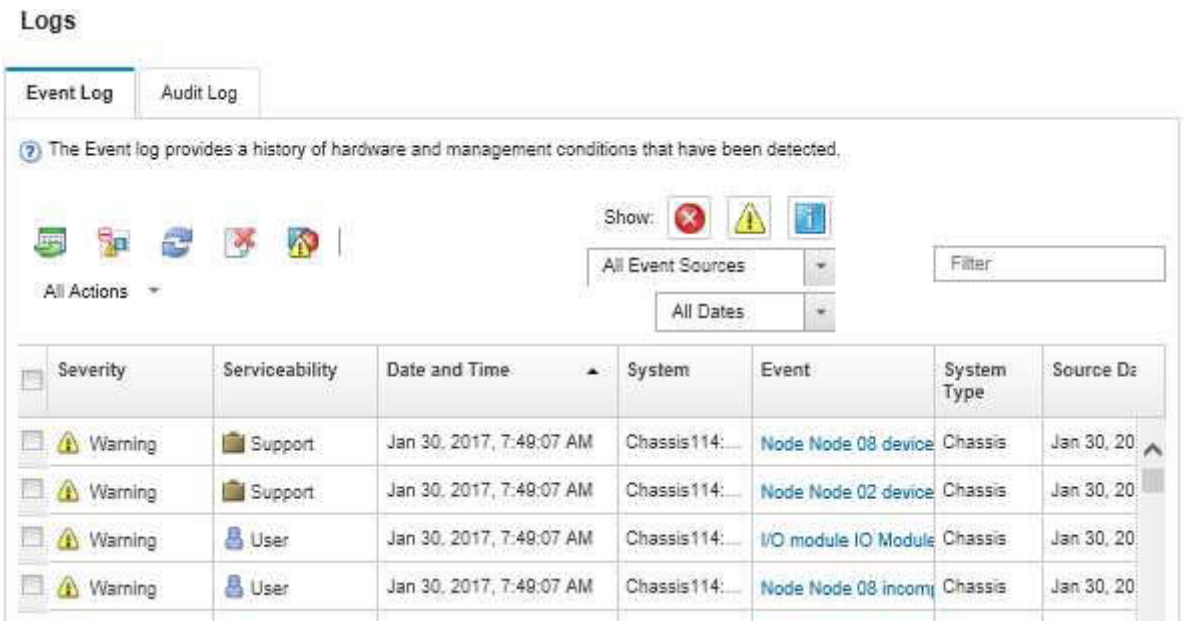


Figure 100. Lenovo XClarity Administrator event log

For more information about working with events from XClarity Administrator, see:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/events_vieweventlog.html

Lenovo XClarity Controller event log

The Lenovo XClarity Controller monitors the physical state of the server and its components using sensors that measure internal physical variables such as temperature, power-supply voltages, fan speeds, and component status. The Lenovo XClarity Controller provides various interfaces to systems management software and to system administrators and users to enable remote management and control of a server.

The Lenovo XClarity Controller monitors all components of the server and posts events in the Lenovo XClarity Controller event log.

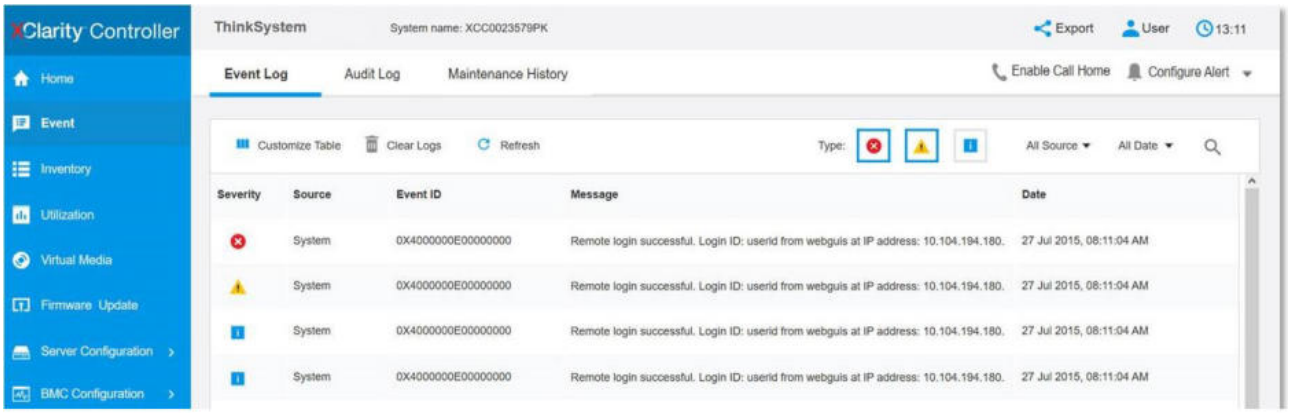


Figure 101. Lenovo XClarity Controller event log

For more information about accessing the Lenovo XClarity Controller event log, see:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/event_log.html

General problem determination procedures

Use the information in this section to resolve problems if the event log does not contain specific errors or the server is inoperative.

If you are not sure about the cause of a problem and the power supplies are working correctly, complete the following steps to attempt to resolve the problem:

1. Turn off the server.
2. Ensure that the server is cabled correctly.
3. Remove or disconnect the following devices, one at a time, until you find the failure. Turn on and configure the server each time you remove or disconnect a device.
   - Any external devices
   - Surge-suppressor device (on the server)
   - Printer, mouse, and non-Lenovo devices
   - Each adapter
   - Storage drives
   - DIMMs until you reach the minimum configuration that is supported for the server

   Note: For minimal configuration for debugging, see “Specifications” on page 2
4. Turn on the server.

If the problem is solved when you remove an adapter from the server, but the problem recurs when you install the same adapter again, suspect the adapter. If the problem recurs when you replace the adapter with a different one, try a different PCIe slot.

If the problem appears to be a networking problem and the server passes all system tests, suspect a network cabling problem that is external to the server.

Resolving suspected power problems

Power problems can be difficult to solve. For example, a short circuit can exist anywhere on any of the power distribution buses. Usually, a short circuit will cause the power subsystem to shut down because of an overcurrent condition.

Complete the following steps to diagnose and resolve a suspected power problem.

Step 1. Check the event log and resolve any errors related to the power.

Note: Start with the event log of the application that is managing the server. For more information about event logs, see “Event logs” on page 145.

Step 2. Check for short circuits, for example, if a loose screw is causing a short circuit on a circuit board.

Step 3. Remove the adapters and disconnect the cables and power cords to all internal and external devices until the server is at the minimum configuration that is required for the server to start. See “Specifications” on page 2 to determine the minimum configuration for your server.

Step 4. Reconnect all ac power cords and turn on the server. If the server starts successfully, reseat the adapters and devices one at a time until the problem is isolated.

If the server does not start from the minimum configuration, replace the components in the minimum configuration one at a time until the problem is isolated.

Resolving suspected Ethernet controller problems

The method that you use to test the Ethernet controller depends on which operating system you are using. See the operating-system documentation for information about Ethernet controllers, and see the Ethernet controller device-driver readme file.

Complete the following steps to attempt to resolve suspected problems with the Ethernet controller.

Step 1. Make sure that the correct device drivers, which come with the server are installed and that they are at the latest level.

Step 2. Make sure that the Ethernet cable is installed correctly.

- The cable must be securely attached at all connections. If the cable is attached but the problem remains, try a different cable.
- If you set the Ethernet controller to operate at 100 Mbps or 1000 Mbps, you must use Category 5 cabling.

Step 3. Determine whether the hub supports auto-negotiation. If it does not, try configuring the integrated Ethernet controller manually to match the speed and duplex mode of the hub.

Step 4. Check the Ethernet controller LEDs on the rear panel of the server. These LEDs indicate whether there is a problem with the connector, cable, or hub.

- The Ethernet link status LED is lit when the Ethernet controller receives a link pulse from the hub. If the LED is off, there might be a defective connector or cable or a problem with the hub.
- The Ethernet transmit/receive activity LED is lit when the Ethernet controller sends or receives data over the Ethernet network. If the Ethernet transmit/receive activity is off, make sure that the hub and network are operating and that the correct device drivers are installed.

Step 5. Check the LAN activity LED on the rear of the server. The LAN activity LED is lit when data is active on the Ethernet network. If the LAN activity LED is off, make sure that the hub and network are operating and that the correct device drivers are installed.

Step 6. Check for operating-system-specific causes of the problem, and also make sure that the operating system drivers are installed correctly.

Step 7. Make sure that the device drivers on the client and server are using the same protocol.

If the Ethernet controller still cannot connect to the network but the hardware appears to be working, the network administrator must investigate other possible causes of the error.

Troubleshooting by symptom

Use this information to find solutions to problems that have identifiable symptoms.

To use the symptom-based troubleshooting information in this section, complete the following steps:

1. Check the event log of the application that is managing the server and follow the suggested actions to resolve any event codes.
   - If you are managing the server from the Lenovo XClarity Administrator, begin with the Lenovo XClarity Administrator event log.
   - If you are using some other management application, begin with the Lenovo XClarity Controller event log.

   For more information about event logs, see “Event logs” on page 145.
2. Review this section to find the symptoms that you are experiencing and follow the suggested actions to resolve the issue.
3. If the problem persists, contact support (see “Contacting Support” on page 165).

Power on and power off problems

Use this information to resolve issues when powering on or powering off the server.

- “Embedded hypervisor is not in the boot list” on page 149
- “The power button does not work (server does not start)” on page 149
- “Server does not power on” on page 150
- “Server does not power off” on page 150

Embedded hypervisor is not in the boot list

Complete the following steps until the problem is solved.

1. If the server has been installed, moved, or serviced recently, or if this is the first time the embedded hypervisor is being used, make sure that the device is connected properly and that there is no physical damage to the connectors.
2. See the documentation that comes with the optional embedded hypervisor flash device for setup and configuration information.
3. Check http://www.lenovo.com/us/en/serverproven/ to validate that the embedded hypervisor device is supported for the server.
4. Make sure that the embedded hypervisor device is listed in the list of available boot options. From the management controller user interface, click **Server Configuration → Boot Options**.

   For information about accessing the management controller user interface, see the XClarity Controller product documentation:

   http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/dw1lm_c_chapter2_openingandusing.html
5. Check http://datacentersupport.lenovo.com for any tech tips (service bulletins) related to the embedded hypervisor and the server.
6. Make sure that other software works on the server to ensure that it is working properly.

The power button does not work (server does not start)

Note: The power button will not function until approximately 1 to 3 minutes after the server has been connected to ac power.

Complete the following steps until the problem is resolved:

1. Make sure that the power button on the server is working correctly:
   a. Disconnect the server power cords.
   b. Reconnect the server power cords.
   c. Reseat the operator information panel cable, and then repeat steps a and b.
      - If the server starts, reseat the operator information panel.
      - If the problem remains, replace the operator information panel.
2. Make sure that:
   - The power cords are correctly connected to the server and to a working electrical outlet.
   - The LEDs on the power supply do not indicate a problem.
3. Reseat the power supplies.
4. Replace each power supply, restarting the server each time:
   - DIMMs

- Power supplies

5. If you just installed an optional device, remove it, and restart the server. If the server starts, you might have installed more devices than the power supply supports.

Server does not power on

Complete the following steps until the problem is resolved:

1. Check the event log for any events related to the server not powering on.
2. Check for any LEDs that are flashing amber.
3. Check the power LED on the system board.
4. Reseat the power supply.
5. Replace the power supply.

Server does not power off

Complete the following steps until the problem is resolved:

1. Determine whether you are using an Advanced Configuration and Power Interface (ACPI) or a non-ACPI operating system. If you are using a non-ACPI operating system, complete the following steps:
   a. Press `Ctrl+Alt+Delete`.
   b. Turn off the server by pressing the power button and holding it down for 5 seconds.
   c. Restart the server.
   d. If the server fails POST and the power button does not work, disconnect the power cord for 20 seconds; then, reconnect the power cord and restart the server.
2. If the problem remains or if you are using an ACPI-aware operating system, suspect the system board.

Memory problems

Use this information to resolve issues related to memory.

- “Displayed system memory less than installed physical memory” on page 150
- “Multiple rows of DIMMs in a branch identified as failing” on page 151

Displayed system memory less than installed physical memory

Complete the following steps until the problem is resolved:

Note: Each time you install or remove a DIMM, you must disconnect the server from the power source; then, wait 10 seconds before restarting the server.

1. Make sure that:
   - No error LEDs are lit on the operator information panel.
   - Memory mirrored channel does not account for the discrepancy.
   - The DIMMs are seated correctly.
   - You have installed the correct type of DIMMs.
   - If you changed the DIMMs, you updated the memory configuration in the Setup utility.
   - All banks of memory are enabled. The server might have automatically disabled a memory bank when it detected a problem, or a memory bank might have been manually disabled.
   - There is no memory mismatch when the server is at the minimum memory configuration.
2. Reseat the DIMMs, and then restart the server.

3. Run memory diagnostics. When you start a server and press F1, the Lenovo XClarity Provisioning Manager interface is displayed by default. You can perform memory diagnostics from this interface. From the Diagnostic page, click **Run Diagnostic → Memory test**.
4. Check the POST error log:
   - If a DIMM was disabled by a systems-management interrupt (SMI), replace the DIMM.
   - If a DIMM was disabled by the user or by POST, reseat the DIMM; then, run the Setup utility and enable the DIMM.
5. Reseat the DIMM.
6. Restart the server.

Multiple rows of DIMMs in a branch identified as failing

1. Reseat the DIMMs; then, restart the server.
2. Remove the lowest-numbered DIMM pair of those that are identified and replace it with an identical known good DIMM; then, restart the server. Repeat as necessary. If the failures continue after all identified DIMMs are replaced, go to step 4.
3. Return the removed DIMMs, one at a time, to their original connectors, restarting the server after each DIMM, until a DIMM fails. Replace each failing DIMM with an identical known good DIMM, restarting the server after each DIMM replacement. Repeat step 3 until you have tested all removed DIMMs.
4. Replace the lowest-numbered DIMM of those identified; then, restart the server. Repeat as necessary.
5. Reverse the DIMMs between the channels (of the same processor), and then restart the server. If the problem is related to a DIMM, replace the failing DIMM.
6. (Trained technician only) Replace the system board.

Hard disk drive problems

Use this information to resolve issues related to the hard disk drives.

- “Server cannot recognize a hard drive” on page 151
- “Multiple hard drives fail” on page 152
- “Multiple hard drives are offline” on page 152
- “A replacement hard disk drive does not rebuild” on page 152
- “Green hard disk drive activity LED does not represent actual state of associated drive” on page 153
- “Yellow hard disk drive status LED does not represent actual state of associated drive” on page 153

Server cannot recognize a hard drive

Complete the following steps until the problem is solved.

1. Observe the associated yellow hard disk drive status LED. If the LED is lit, it indicates a drive fault.
2. If the LED is lit, remove the drive from the bay, wait 45 seconds, and reinsert the drive, making sure that the drive assembly connects to the hard disk drive backplane.
3. Observe the associated green hard disk drive activity LED and the yellow status LED:
   - If the green activity LED is flashing and the yellow status LED is not lit, the drive is recognized by the controller and is working correctly. Run the diagnostics tests for the hard disk drives. When you start a server and press F1, the Lenovo XClarity Provisioning Manager interface is displayed by default. You can perform hard drive diagnostics from this interface. From the Diagnostic page, click **Run Diagnostic → HDD test**.
   - If the green activity LED is flashing and the yellow status LED is flashing slowly, the drive is recognized by the controller and is rebuilding.

- If neither LED is lit or flashing, check the hard disk drive backplane.
- If the green activity LED is flashing and the yellow status LED is lit, replace the drive. If the activity of the LEDs remains the same, go to step Hard disk drive problems. If the activity of the LEDs changes, return to step 1.

4. Make sure that the hard disk drive backplane is correctly seated. When it is correctly seated, the drive assemblies correctly connect to the backplane without bowing or causing movement of the backplane.
5. Reseat the backplane power cable and repeat steps 1 through 3.
6. Reseat the backplane signal cable and repeat steps 1 through 3.
7. Suspect the backplane signal cable or the backplane:
   - Replace the affected backplane signal cable.
   - Replace the affected backplane.
8. Run the diagnostics tests for the hard disk drives. When you start a server and press F1, the Lenovo XClarity Provisioning Manager interface is displayed by default. You can perform hard drive diagnostics from this interface. From the Diagnostic page, click **Run Diagnostic → HDD test**.

   Based on those tests:
   - If the adapter passes the test but the drives are not recognized, replace the backplane signal cable and run the tests again.
   - Replace the backplane.
   - If the adapter fails the test, disconnect the backplane signal cable from the adapter and run the tests again.
   - If the adapter fails the test, replace the adapter.

Multiple hard drives fail

Complete the following steps until the problem is solved:

- View the Lenovo XClarity Controller event log for events related to power supplies or vibration issues and resolve those events.
- Make sure that the device drivers and firmware for the hard disk drive and server are at the latest level

Important: Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.

Multiple hard drives are offline

Complete the following steps until the problem is solved:

- View the Lenovo XClarity Controller event log for events related to power supplies or vibration issues and resolve those events.
- View the storage subsystem log for events related to the storage subsystem and resolve those events.

A replacement hard disk drive does not rebuild

Complete the following steps until the problem is solved:

1. Make sure that the hard disk drive is recognized by the adapter (the green hard disk drive activity LED is flashing).
2. Review the SAS/SATA RAID adapter documentation to determine the correct configuration parameters and settings.

Green hard disk drive activity LED does not represent actual state of associated drive

Complete the following steps until the problem is solved:

1. If the green hard disk drive activity LED does not flash when the drive is in use, run the diagnostics tests for the hard disk drives. When you start a server and press F1, the Lenovo XClarity Provisioning Manager interface is displayed by default. You can perform hard drive diagnostics from this interface. From the Diagnostic page, click **Run Diagnostic → HDD test**.
2. If the drive passes the test, replace the backplane.
3. If the drive fails the test, replace the drive.

Yellow hard disk drive status LED does not represent actual state of associated drive

Complete the following steps until the problem is solved:

1. Turn off the server.
2. Reseat the SAS/SATA adapter.
3. Reseat the backplane signal cable and backplane power cable.
4. Reseat the hard disk drive.
5. Power on the server and observe the activity of the hard disk drive LEDs.

Monitor and video problems

Use this information to solve problems related to a monitor or video.

- “Incorrect characters are displayed” on page 153
- “Screen is blank” on page 153
- “Screen goes blank when you start some application programs” on page 154
- “The monitor has screen jitter, or the screen image is wavy, unreadable, rolling, or distorted.” on page 154
- “The wrong characters appear on the screen” on page 154

Incorrect characters are displayed

Complete the following steps:

1. Verify that the language and locality settings are correct for the keyboard and operating system.
2. If the wrong language is displayed, update the server firmware to the latest level. See “Firmware updates” on page 7.

Screen is blank

1. If the server is attached to a KVM switch, bypass the KVM switch to eliminate it as a possible cause of the problem: connect the monitor cable directly to the correct connector on the rear of the server.
2. The management controller remote presence function is disabled if you install an optional video adapter. To use the management controller remote presence function, remove the optional video adapter.
3. If the server installed with the graphical adapters while turning on the server, the Lenovo logo displays on the screen after approximately 3 minutes. This is normal operation while the system loads.
4. Make sure that:
   - The server is turned on. If there is no power to the server.
   - The monitor cables are connected correctly.
   - The monitor is turned on and the brightness and contrast controls are adjusted correctly.
5. Make sure that the correct server is controlling the monitor, if applicable.
6. Make sure that corrupted server firmware is not affecting the video; see “Firmware updates” on page 7.
7. Observe the LEDs on the system board; if the codes are changing, go to step 6.

8. Replace the following components one at a time, in the order shown, restarting the server each time:
   a. Monitor
   b. Video adapter (if one is installed)
   c. (Trained technician only) System board

Screen goes blank when you start some application programs

1. Make sure that:
   - The application program is not setting a display mode that is higher than the capability of the monitor.
   - You installed the necessary device drivers for the application.

The monitor has screen jitter, or the screen image is wavy, unreadable, rolling, or distorted.

1. If the monitor self-tests show that the monitor is working correctly, consider the location of the monitor. Magnetic fields around other devices (such as transformers, appliances, fluorescents, and other monitors) can cause screen jitter or wavy, unreadable, rolling, or distorted screen images. If this happens, turn off the monitor.

   Attention: Moving a color monitor while it is turned on might cause screen discoloration.

   Move the device and the monitor at least 305 mm (12 in.) apart, and turn on the monitor.

   Notes:
   a. To prevent diskette drive read/write errors, make sure that the distance between the monitor and any external diskette drive is at least 76 mm (3 in.).
   b. Non-Lenovo monitor cables might cause unpredictable problems.
2. Reseat the monitor cable.
3. Replace the components listed in step 2 one at a time, in the order shown, restarting the server each time:
   a. Monitor cable
   b. Video adapter (if one is installed)
   c. Monitor
   d. (Trained technician only) System board

The wrong characters appear on the screen

Complete the following steps until the problem is solved:

1. Verify that the language and locality settings are correct for the keyboard and operating system.
2. If the wrong language is displayed, update the server firmware to the latest level. See “Firmware updates” on page 7.

Keyboard, mouse, or USB-device problems

Use this information to solve problems related to a keyboard, mouse, or USB device.

- “All or some keys on the keyboard do not work.” on page 154
- “Mouse does not work.” on page 155
- “USB-device does not work.” on page 155

All or some keys on the keyboard do not work.

1. Make sure that:

- The keyboard cable is securely connected.
- The server and the monitor are turned on.

2. If you are using a USB keyboard, run the Setup utility and enable keyboardless operation.
3. If you are using a USB keyboard and it is connected to a USB hub, disconnect the keyboard from the hub and connect it directly to the server.
4. Replace the keyboard.

Mouse does not work.

1. Make sure that:
   - The mouse cable is securely connected to the server.
   - The mouse device drivers are installed correctly.
   - The server and the monitor are turned on.
   - The mouse option is enabled in the Setup utility.
2. If you are using a USB mouse and it is connected to a USB hub, disconnect the mouse from the hub and connect it directly to the server.
3. Replace the mouse.

USB-device does not work.

1. Make sure that:
   - The correct USB device driver is installed.
   - The operating system supports USB devices.
2. Make sure that the USB configuration options are set correctly in system setup.

   Restart the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface. Then, click **System Settings → Devices and I/O Ports → USB Configuration**.
3. If you are using a USB hub, disconnect the USB device from the hub and connect it directly to the server.

Optional-device problems

Use this information to solve problems related to optional devices.

- “External USB device not recognized” on page 155
- “PCIe adapter is not recognized or is not functioning” on page 155
- “A Lenovo optional device that worked previously does not work now. ” on page 156
- “A Lenovo optional device that was just installed does not work.” on page 156
- “A Lenovo optional device that worked previously does not work now. ” on page 156

External USB device not recognized

Complete the following steps until the problem is resolved:

1. Make sure that the proper drivers are installed on the compute node. See the product documentation for the USB device for information about device drivers.
2. Use the Setup utility to make sure that the device is configured correctly.
3. If the USB device is plugged into a hub or the console breakout cable, unplug the device and plug it directly into the USB port on the front of the compute node.

PCIe adapter is not recognized or is not functioning

Complete the following steps until the problem is resolved:

1. Check the event log and resolve any issues related to the device.
2. Validate that the device is supported for the server (see http://www.lenovo.com/us/en/serverproven/).
3. Make sure that the adapter is installed in a correct slot.
4. Make sure that the proper device drivers are installed for the device.
5. Resolve any resource conflicts if running legacy mode (UEFI).
6. Check http://datacentersupport.lenovo.com for any tech tips (also known as retain tips or service bulletins) that might be related to the adapter.
7. Ensure any adapter external connections are correct and that the connectors are not physically damaged.

Insufficient PCIe resources are detected.

If you see an error message stating “Insufficient PCI Resources Detected,” complete the following steps until the problem is resolved:

1. Remove one of the PCIe adapters.
2. Restart the system and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface.
3. Click **UEFI Setup → System Settings → Devices and I/O Ports → MM Config Base**; then, modify the setting to the lower memory capacity. For example, modify 3 GB to 2 GB or modify 2 GB to 1 GB.
4. Save the settings and restart the system.
5. The action for this step will differ based on whether or not the reboot is successful.
   - If the reboot is successful, shut down the solution and reinstall the PCIe card you removed.
   - If the reboot failed, repeat step 2 to step 5.

A Lenovo optional device that was just installed does not work.

1. Make sure that:
   - The device is supported for the server (see http://www.lenovo.com/us/en/serverproven/).
   - You followed the installation instructions that came with the device and the device is installed correctly.
   - You have not loosened any other installed devices or cables.
   - You updated the configuration information in system setup. When you start a server and press F1 to display the system setup interface. Whenever memory or any other device is changed, you must update the configuration.
2. Reseat the device that you just installed.
3. Replace the device that you just installed.

A Lenovo optional device that worked previously does not work now.

1. Make sure that all of the cable connections for the device are secure.
2. If the device comes with test instructions, use those instructions to test the device.
3. If the failing device is a SCSI device, make sure that:
   - The cables for all external SCSI devices are connected correctly.
   - The last device in each SCSI chain, or the end of the SCSI cable, is terminated correctly.
   - Any external SCSI device is turned on. You must turn on an external SCSI device before you turn on the server.
4. Reseat the failing device.
5. Replace the failing device.

Serial-device problems

Use this information to solve problems with serial ports or devices.

- “Number of displayed serial ports is less than the number of installed serial ports” on page 157
- “Serial device does not work” on page 157

Number of displayed serial ports is less than the number of installed serial ports

Complete the following steps until the problem is solved.

1. Make sure that:
   - Each port is assigned a unique address in the Setup utility and none of the serial ports is disabled.
   - The serial-port adapter (if one is present) is seated correctly
2. Reseat the serial port adapter.
3. Replace the serial port adapter.

Serial device does not work

1. Make sure that:
   - The device is compatible with the server.
   - The serial port is enabled and is assigned a unique address.
   - The device is connected to the correct connector.
2. Reseat the following components:
   a. Failing serial device.
   b. Serial cable.
3. Replace the following components:
   a. Failing serial device.
   b. Serial cable.
4. (Trained technician only) Replace the system board.

Intermittent problems

Use this information to solve intermittent problems.

- “Intermittent external device problems” on page 157
- “Intermittent KVM problems” on page 158
- “Intermittent unexpected reboots” on page 158

Intermittent external device problems

Complete the following steps until the problem is solved.

1. Make sure that the correct device drivers are installed. See the manufacturer's website for documentation.
2. For a USB device:
   a. Make sure that the device is configured correctly.

      Restart the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface. Then, click **System Settings → Devices and I/O Ports → USB Configuration**.
   b. Connect the device to another port. If using a USB hub, remove the hub and connect the device directly to the compute node. Make sure that the device is configured correctly for the port.

Intermittent KVM problems

Complete the following steps until the problem is solved.

Video problems:

1. Make sure that all cables and the console breakout cable are properly connected and secure.
2. Make sure that the monitor is working properly by testing it on another compute node.
3. Test the console breakout cable on a working compute node to ensure that it is operating properly. Replace the console breakout cable if it is defective.

Keyboard problems:

Make sure that all cables and the console breakout cable are properly connected and secure.

Mouse problems:

Make sure that all cables and the console breakout cable are properly connected and secure.

Intermittent unexpected reboots

Note: Some correctable errors require that the server reboot so that it can disable a device, such as a memory DIMM or a processor to allow the machine to boot up properly.

1. If the reset occurs during POST and the POST watchdog timer is enabled, make sure that sufficient time is allowed in the watchdog timeout value (POST Watchdog Timer).

   To check the POST watchdog time, restart the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface. Then, click **BMC Settings → POST Watchdog Timer**.
2. If the reset occurs after the operating system starts, disable any automatic server restart (ASR) utilities, such as the Automatic Server Restart IPMI Application for Windows, or any ASR devices that are installed.
3. See the management controller event log to check for an event code that indicates a reboot. See “Event logs” on page 145 for information about viewing the event log.

Power problems

Use this information to resolve issues related to power.

System error LED is on and event log "Power supply has lost input" is displayed

To resolve the problem, ensure that:

1. The power supply is properly connected to a power cord.
2. The power cord is connected to a properly grounded electrical outlet for the server.

Network problems

Use this information to resolve issues related to networking.

- “Cannot wake server using Wake on LAN” on page 158
- “Could not log in using LDAP account with SSL enabled” on page 159

Cannot wake server using Wake on LAN

Complete the following steps until the problem is resolved:

1. If you are using the dual-port network adapter and the server is connected to the network using Ethernet 5 connector, check the system-error log or IMM2 system event log (see “Event logs” on page 145), make sure:
   a. The room temperature is not too high (see “Specifications” on page 2).
   b. The air vents are not blocked.
   c. The air baffle is installed securely.
2. Reseat the dual-port network adapter.
3. Turn off the server and disconnect it from the power source; then, wait 10 seconds before restarting the server.
4. If the problem still remains, replace the dual-port network adapter.

Could not log in using LDAP account with SSL enabled

Complete the following steps until the problem is resolved:

1. Make sure that the license key is valid.
2. Generate a new license key and log in again.

Observable problems

Use this information to solve observable problems.

- “The server immediately displays the POST Event Viewer when it is turned on” on page 159
- “Server is unresponsive (POST is complete and operating system is running)” on page 159
- “Server is unresponsive (cannot press F1 to start System Setup)” on page 160
- “Voltage planar fault is displayed in the event log” on page 160
- “Unusual smell” on page 161
- “Server seems to be running hot” on page 161
- “Cracked parts or cracked chassis” on page 161

The server immediately displays the POST Event Viewer when it is turned on

Complete the following steps until the problem is solved.

1. Correct any errors that are indicated by the light path diagnostics LEDs.
2. Make sure that the server supports all the processors and that the processors match in speed and cache size.

   You can view processor details from system setup.

   To determine if the processor is supported for the server, see http://www.lenovo.com/us/en/serverproven/ .
3. (Trained technician only) Make sure that processor 1 is seated correctly.
4. (Trained technician only) Remove processor 2 and restart the server.
5. Replace the following components one at a time, in the order shown, restarting the server each time:
   a. (Trained technician only) Processor
   b. (Trained technician only) System board

Server is unresponsive (POST is complete and operating system is running)

Complete the following steps until the problem is solved.

- If you are in the same location as the compute node, complete the following steps:

1. If you are using a KVM connection, make sure that the connection is operating correctly. Otherwise, make sure that the keyboard and mouse are operating correctly.
2. If possible, log in to the compute node and verify that all applications are running (no applications are hung).
3. Restart the compute node.
4. If the problem remains, make sure that any new software has been installed and configured correctly.
5. Contact your place of purchase of the software or your software provider.

- If you are accessing the compute node from a remote location, complete the following steps:
  1. Make sure that all applications are running (no applications are hung).
  2. Attempt to log out of the system and log back in.
  3. Validate the network access by pinging or running a trace route to the compute node from a command line.
     a. If you are unable to get a response during a ping test, attempt to ping another compute node in the enclosure to determine whether it is a connection problem or compute node problem.
     b. Run a trace route to determine where the connection breaks down. Attempt to resolve a connection issue with either the VPN or the point at which the connection breaks down.
  4. Restart the compute node remotely through the management interface.
  5. If the problem remains, verify that any new software has been installed and configured correctly.
  6. Contact your place of purchase of the software or your software provider.

Server is unresponsive (cannot press F1 to start System Setup)

Configuration changes, such as added devices or adapter firmware updates, and firmware or application code problems can cause the server to fail POST (the power-on self-test).

If this occurs, the server responds in either of the following ways:

- The server restarts automatically and attempts POST again.
- The server hangs, and you must manually restart the server for the server to attempt POST again.

After a specified number of consecutive attempts (automatic or manual), the server to reverts to the default UEFI configuration and starts System Setup so that you can make the necessary corrections to the configuration and restart the server. If the server is unable to successfully complete POST with the default configuration, there might be a problem with the system board.

You can specify the number of consecutive restart attempts in System Setup. Restart the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface. Then, click **System Settings → Recovery and RAS → POST Attempts → POST Attempts Limit**. Available options are 3, 6, 9, and disable.

Voltage planar fault is displayed in the event log

Complete the following steps until the problem is solved.

1. Revert the system to the minimum configuration. See “Specifications” on page 2 for the minimally required number of processors and DIMMs.
2. Restart the system.
   - If the system restarts, add each of the items that you removed one at a time, restarting the system each time, until the error occurs. Replace the item for which the error occurs.
   - If the system does not restart, suspect the system board.

Unusual smell

Complete the following steps until the problem is solved.

1. An unusual smell might be coming from newly installed equipment.
2. If the problem remains, contact Lenovo Support.

Server seems to be running hot

Complete the following steps until the problem is solved.

Multiple compute nodes or chassis:

1. Make sure that the room temperature is within the specified range (see “Specifications” on page 2).
2. Check the management processor event log for rising temperature events. If there are no events, the compute node is running within normal operating temperatures. Note that you can expect some variation in temperature.

Cracked parts or cracked chassis

Contact Lenovo Support.

Software problems

Use this information to solve software problems.

1. To determine whether the problem is caused by the software, make sure that:
   - The server has the minimum memory that is needed to use the software. For memory requirements, see the information that comes with the software.

     Note: If you have just installed an adapter or memory, the server might have a memory-address conflict.
   - The software is designed to operate on the server.
   - Other software works on the server.
   - The software works on another server.
2. If you receive any error messages while you use the software, see the information that comes with the software for a description of the messages and suggested solutions to the problem.
3. Contact your place of purchase of the software.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support are available at:

http://datacentersupport.lenovo.com

Note: IBM is Lenovo's preferred service provider for ThinkSystem.

Before you call

Before you call, there are several steps that you can take to try and solve the problem yourself. If you decide that you do need to call for assistance, gather the information that will be needed by the service technician to more quickly resolve your problem.

Attempt to resolve the problem yourself

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

You can find the product documentation for your ThinkSystem products at the following location:

http://thinksystem.lenovofiles.com/help/index.jsp

You can take these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.lenovo.com/us/en/serverproven/ to make sure that the hardware and software is supported by your product.
- Go to http://datacentersupport.lenovo.com and check for information to help you solve the problem.
  - Check the Lenovo forums at https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg to see if someone else has encountered a similar problem.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

© Copyright Lenovo 2017, 2020

Gathering information needed to call Support

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call. You can also see http://datacentersupport.lenovo.com/warrantylookup for more information about your product warranty.

Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.

- Hardware and Software Maintenance agreement contract numbers, if applicable
- Machine type number (Lenovo 4-digit machine identifier)
- Model number
- Serial number
- Current system UEFI and firmware levels
- Other pertinent information such as error messages and logs

As an alternative to calling Lenovo Support, you can go to https://support.lenovo.com/servicerequest to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The Lenovo service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

Collecting service data

To clearly identify the root cause of a server issue or at the request of Lenovo Support, you might need collect service data that can be used for further analysis. Service data includes information such as event logs and hardware inventory.

Service data can be collected through the following tools:

- **Lenovo XClarity Provisioning Manager**

  Use the Collect Service Data function of Lenovo XClarity Provisioning Manager to collect system service data. You can collect existing system log data or run a new diagnostic to collect new data.

- **Lenovo XClarity Controller**

  You can use the Lenovo XClarity Controller web interface or the CLI to collect service data for the server. The file can be saved and sent to Lenovo Support.

  - For more information about using the web interface to collect service data, see http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_servicesandsupport.html.
  - For more information about using the CLI to collect service data, see http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator can be set up to collect and send diagnostic files automatically to Lenovo Support when certain serviceable events occur in Lenovo XClarity Administrator and the managed endpoints. You can choose to send diagnostic files to Lenovo Support using Call Home or to another service provider using SFTP. You can also manually collect diagnostic files, open a problem record, and send diagnostic files to the Lenovo Support Center.

  You can find more information about setting up automatic problem notification within the Lenovo XClarity Administrator at http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html.

- **Lenovo XClarity Essentials OneCLI**

Lenovo XClarity Essentials OneCLI has inventory application to collect service data. It can run both in-band and out-of-band. When running in-band within the host operating system on the server, OneCLI can collect information about the operating system, such as the operating system event log, in addition to the hardware service data.

To obtain service data, you can run the **getinfor** command. For more information about running the **getinfor**, see http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_getinfor_command.html.

Contacting Support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/supportphonelist for your region support details.

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo s are provided for convenience only and do not in any manner serve as an endorsement of those s. The materials at those s are not part of the materials for this Lenovo product, and use of those s is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2017, 2020

Trademarks

LENOVO, XCLARITY, and THINKSYSTEM are trademarks of Lenovo.

Intel and Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

All other trademarks are the property of their respective owners. © 2020 Lenovo.

Important notes

Processor speed indicates the internal clock speed of the processor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This

specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 20. Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Additional electronic emissions notices are available at:

http://thinksystem.lenovofiles.com/help/index.jsp

Taiwan BSMI RoHS declaration

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (PB)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模組	–	○	○	○	○	○
處理器模組	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源供應器	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電路卡	–	○	○	○	○	○
光碟機	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : "exceeding 0.1wt%" and "exceeding 0.01 wt%" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : "○"indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝-〞係指該項限用物質為排除項目。

Note3 : The "-" indicates that the restricted substance corresponds to the exemption.

Taiwan import and export contact information

Contacts are available for Taiwan import and export information.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Index

A

air baffle
  removing 55
  replacing 55, 57
assert
  physical presence 141

B

backplane for eight 2.5-inch hot-swap drives
  removing 69
  replacing 70
backplane for four 3.5-inch hot-swap drives
  removing 67
  replacing 68
backplanes 33

C

cable routing
  front I/O assembly 31
  RAID super capacitor module 32
  VGA connector 29
cable routing for the server model with eight 2.5-inch hot-swap drives 33
cable routing for the server model with four 3.5-inch hot-swap drives 34
cable routing for the server model with four 3.5-inch simple-swap drives 35
CMOS battery
  install 89
  remove 87
  replacing 87
collecting service data 164
completing
  parts replacement 143
configuring
  LAN over USB manually 10
contamination, particulate and gaseous 168
cover
  installing 54
  removing 52
  replacing 52
CPU
  installing 126
  removing 123
  replacing 123
creating a personalized support web page 163
custom support web page 163

D

devices, static-sensitive
  handling 43
DIMM, install 85

E

enable
  TPM 139
Ethernet
  controller
    troubleshooting 148
Ethernet controller problems
  solving 148
event logs 145

F

firmware updates 7
front I/O assembly
  installing 66
  removing 65
  replacing 65

G

gaseous contamination 168
general problem determination procedures 147
Getting help 163
guidelines
  options installation 41
  system reliability 42

H

handling static-sensitive devices 43
hard disk drive
  installing 74
  replacing 73
hard disk drive problems 151
hard disk drives
  removing 73
hardware service and support telephone numbers 165
heat sink
  installing 126
  removing 123
  replacing 123
help 163
hot-swap drive
  installing 74
  replacing 73
hot-swap drive backplane
  replacing 67
hot-swap drives
  removing 73
hot-swap power supply
  remove 93
  replacing 93
hot-swap power supply, install 99

I

important notices 168
install
  CMOS battery 89
  hot-swap power supply 99
installation
  guidelines 41
installation guidelines 41
installing
  CPU 126
  front I/O assembly 66
  hard disk drive 74
  heat sink 126

© Copyright Lenovo 2017, 2020

hot-swap drive 74
LOM adapter 122
memory module 85
microprocessor 126
microprocessor heat sink module 126
PCIe adapter 106
PHM 126
processor 126
processor-heat-sink module 126
rack latches 46
riser card 109
security bezel 50
serial port module 119
simple-swap drive 78
system board 134
system fan 64
TCM/TPM adapter 91
top cover 54
insufficient PCIe resource
solving 155
intermittent problems 157
internal cable routing 28
introduction 1

K

keyboard problems 154

L

LAN over USB
configuring manually 10
Windows driver installation 10
LOM adapter
installing 122
removing 121
replacing 121

M

M.2 backplane and M.2 drive
installing 114
removing 111
replacing 111
memory
problems 150
memory module
removing 79
replacing 79
Memory module installation order 80
Memory module installation rules 80
memory modules
removal 79
microprocessor
installing 126
removing 123
replacing 123
microprocessor heat sink module
installing 126
removing 123
replacing 123
monitor problems 153
mouse problems 154

N

network
problems 158
notes, important 168
notices 167

O

observable problems 159
operator information panel 15
optional-device problems 155

P

particulate contamination 168
parts list 36
parts replacement, completing 143
PCIe
troubleshooting 155
PCIe adapter
installing 106
removing 105
replacing 105
PHM
installing 126
removing 123
replacing 123
physical presence 141
power
problems 158
power cords 39
power off the server 11
power on the server 11
power problems 147
problem determination 145
problems
Ethernet controller 148
hard disk drive 151
intermittent 157
keyboard 154
memory 150
monitor 153
mouse 154
network 158
observable 159
optional devices 155
PCIe 155
power 147, 158
power on and power off 149
serial-device 157
software 161
USB device 154
video 153
processor
installing 126
removing 123
replacing 123
processor heat sink module
replacing 123
processor-heat-sink module
installing 126
removing 123

R

rack latches
installing 46
removing 44
replacing 44
RAID super capacitor module
removing 58
replacing 58, 60
rear view 17
remove

CMOS battery 87
hot-swap power supply 93
removing
air baffle 55
backplane for eight 2.5-inch hot-swap drives 69
backplane for four 3.5-inch hot-swap drives 67
CPU 123
front I/O assembly 65
hard disk drive 73
heat sink 123
hot-swap drive 73
LOM adapter 121
memory modules 79
microprocessor 123
microprocessor heat sink module 123
PCIe adapter 105
PHM 123
processor 123
processor-heat-sink module 123
rack latches 44
RAID super capacitor module 58
riser card 107
security bezel 48
serial port module 117
simple-swap drive 76
simple-swap drive backplate assembly 71
system board 131
system fan 62
TCM/TPM adapter 90
top cover 52
removing, memory modules 79
replacing
air baffle 55, 57
backplane for eight 2.5-inch hot-swap drives 70
backplane for four 3.5-inch hot-swap drives 68
CMOS battery 87
CPU 123
front I/O assembly 65
hard disk drive 73
heat sink 123
hot-swap drive 73
hot-swap drive backplane 67
hot-swap power supply 93
LOM adapter 121
M.2 module 111
memory module 79
microprocessor 123
microprocessor heat sink module 123
PCIe adapter 105
PHM 123
processor 123
processor heat sink module 123
rack latches 44
RAID super capacitor module 58, 60
riser card 107
security bezel 48
serial port module 117
simple-swap drive 76
simple-swap drive backplate assembly 71–72
system board 131
system fan 62
TCM/TPM adapter 90
top cover 52
retainer on M.2 backplane
adjustment 113
riser card
installing 109
removing 107
replacing 107

S

safety iii
safety inspection checklist iv
Secure Boot 142
security advisories 11
security bezel
installing 50
removing 48
replacing 48
serial port module
installing 119
removing 117
replacing 117
serial-device problems 157
server components 13
server power on or power off problems 149
service and support
before you call 163
hardware 165
software 165
service data 164
simple-swap drive
installing 78
replacing 76
simple-swap drive backplate assembly
removing 71
replacing 71–72
simple-swap drives
removing 76
software problems 161
software service and support telephone numbers 165
solving
Ethernet controller problems 148
insufficient PCIe resource 155
solving power problems 147
specifications 2
static-sensitive devices
handling 43
support web page, custom 163
system board
installing 134
removing 131
replacing 131
system board components 23
system board LEDs 27
system board switches and jumpers 25
system fan
installing 64
removing 62
replacing 62
system reliability guidelines 42

T

Taiwan BSMI RoHS declaration 170
Taiwan import and export contact information 170
TCM 139
TCM policy 139
TCM/TPM adapter
installing 91
removing 90
replacing 90
Tech Tips 11
telecommunication regulatory statement 169
telephone numbers 165
top cover
installing 54
removing 52
replacing 52
TPM 139
TPM 1.2 141
TPM 2.0 141
TPM policy 139
TPM version 141
trademarks 168

© Copyright Lenovo 2017, 2020

troubleshooting 153, 155, 161
by symptom 148
hard disk drive problems 151
intermittent problems 157
keyboard problems 154
memory problems 150
mouse problems 154
network problems 158
observable problems 159
power on and power off problems 149
power problems 158
serial-device problems 157
symptoms-based troubleshooting 148
USB-device problems 154
video 153
Trusted Cryptographic Module 139
Trusted Platform Module 139

U

UEFI Secure Boot 142
update firmware 7
updating
DMI/SMBIOS 137
Universal Unique Identifier (UUID) 135
USB-device problems 154

V

video problems 153

W

Windows driver, LAN over USB 10
working inside the server
power on 43

Processador Intel® Xeon® Gold 5215

cache de 13,75 M, 2,50 GHz

Especificações

Especificações de exportação

Essenciais

Coleção de produtos	Processadores escaláveis Intel® Xeon® da 2ª Geração
Codinome	Produtos com denominação anterior Cascade Lake
Segmento vertical	Server
Número do processador	5215
Status	Launched
Data de introdução	Q2'19
Litografia	14 nm
Condições de uso	Server/Enterprise
Preço recomendado para o cliente	$1221.00

Especificações da CPU

Número de núcleos	10
Nº de threads	20
Frequência baseada em processador	2.50 GHz
Frequência turbo max	3.40 GHz
Cache	13.75 MB
Nº de links de UPI	2
TDP	85 W

Informações complementares

Opções integradas disponíveis	Sim
Descrição resumida do produto	Ver agora

Especificações de memória

Tamanho máximo de memória (de acordo com o tipo de memória)	1 TB
Tipos de memória	DDR4-2667
Velocidade máxima de memória	2667 MHz
Nº máximo de canais de memória	6
Compatibilidade com memória ECC ‡	Sim
Memória persistente Intel® Optane™ DC com suporte	Sim

Opções de expansão

Escalabilidade	4S
Revisão de PCI Express	3.0
Nº máximo de linhas PCI Express	48

Especificações de encapsulamento

Soquetes suportados	FCLGA3647
T_{CASE}	77°C
Tamanho do pacote	76.0mm x 56.5mm

Tecnologias avançadas

Intel® Deep Learning Boost (Intel® DL Boost)	Sim
Intel® Speed Select Technology – Perfil de desempenho	Não
Intel® Speed Select Technology – Frequência básica	Não
Intel® Resource Director Technology (Intel® RDT)	Sim
Tecnologia Intel® Speed Shift	Sim
Tecnologia Intel® Turbo Boost Max 3.0 ‡	Não
Tecnologia Intel® Turbo Boost ‡	2.0
Elegibilidade da plataforma Intel® vPro™ ‡	Sim
Tecnologia Hyper-Threading Intel® ‡	Sim
Tecnologia de virtualização Intel® (VT-x) ‡	Sim
Tecnologia de virtualização Intel® para E/S dirigida (VT-d) ‡	Sim
Intel® VT-x com Tabelas de páginas estendidas (EPT) ‡	Sim
Intel® TSX-NI	Sim
Intel® 64 ‡	Sim
Extensões do conjunto de instruções	Intel® SSE4.2, Intel® AVX, Intel® AVX2, Intel® AVX-512
Nº de unidades de FMA de AVX-512	1

Tecnologia Enhanced Intel SpeedStep®	Sim
Intel® Volume Management Device (VMD - Dispositivo de Gerenciamento de Volume)	Sim

Segurança e confiabilidade

Novas instruções Intel® AES	Sim
Intel® Trusted Execution Technology ‡	Sim
Bit de desativação de execução ‡	Sim
Tecnologia Intel® Run Sure	Sim
Controle de Execução baseado em Modo (MBE — Mode-based Execute Control)	Sim

Pedidos e conformidade

Imagens do produto

Produtos compatíveis

Drivers e software

Documentação técnica

Todas as informações fornecidas estão sujeitas a alterações a qualquer momento, sem aviso prévio. A Intel pode alterar o ciclo de vida da fabricação, as especificações e as descrições dos produtos a qualquer momento, sem aviso prévio. As informações aqui contidas são fornecidas "no estado em que se encontram" e a Intel não atribui qualquer declaração ou garantias relacionadas à precisão das informações, nem sobre os recursos dos produtos, disponibilidade, funcionalidade ou compatibilidade dos produtos listados. Para obter mais informações sobre os produtos ou sistemas, entre em contato com o fornecedor do sistema.

As classificações da Intel são apenas para fins informativos e consistem em Export Control Classification Numbers (ECCN — Número de Classificação de Controle de Exportações) e Harmonized Tariff Schedule (HTS — Programa de Tarifas Harmonizadas). Quaisquer usos das classificações da Intel são sem os recursos da Intel e não devem ser interpretados como uma representação ou garantia relacionada ao ECCN ou HTS apropriado. Como exportadora e/ou importadora, sua empresa é responsável por determinar a classificação correta de sua transação

Consulte a Ficha técnica para obter definições formais de propriedades e recursos de produtos.

‡ Este recurso pode não estar disponível em todos os sistemas de computação. Verifique com o fornecedor do sistema para determinar se seu sistema oferece este recurso ou consulte as especificações de seu sistema (motherboard, processador, chipset, alimentação, HDD, controle gráfico, memória, BIOS, drivers, monitor de máquina virtual [VMM], software de plataforma e/ou sistema operacional) para saber sobre a compatibilidade do recurso. A funcionalidade, o desempenho e outros benefícios deste recurso podem variar, dependendo das configurações do sistema.

Alguns produtos suportam as novas instruções AES com uma atualização da Configuração do processador, em particular, i7-2630QM/i7-2635QM, i7-2670QM/i7-2675QM, i5-2430M/i5-2435M, i5-2410M/i5-2415M. Favor entrar em contato com o OEM para o BIOS que inclui a mais recente atualização da Configuração do processador.

O TDP máximo e do sistema se baseiam nos piores casos. O TDP real pode ser inferior, se nem todas as E/Ss para chipsets forem utilizadas.

Frequência máxima de turbo refere-se à frequência máxima do processador de núcleo único que pode ser atingida com a Tecnologia Intel® Turbo Boost. Mais informações estão disponíveis no site https://www.intel.com/content/www/br/pt/architecture-and-technology/turbo-boost/turbo-boost-technology.html

.

Os processadores compatíveis com a computação de 64 bits na arquitetura Intel® requerem BIOS habilitados para arquitetura Intel 64.

SKUs "anunciados" ainda não estão disponíveis. Favor consultar a data de lançamento para a disponibilidade no mercado.

Consulte https://www.intel.com.br/content/www/br/pt/architecture-and-technology/hyper-threading/hyper-threading-technology.html?wapkw=hyper+threading

para obter mais informações, incluindo detalhes sobre quais

processadores são compatíveis com a Tecnologia Hyper-Threading Intel®.

Os números dos processadores Intel não são indicação de desempenho. Os números dos processadores diferenciam recursos dentro de cada família de processador, e não entre famílias diferentes de processadores. Consulte https://www.intel.com.br/content/www/br/pt/processors/processor-numbers.html para obter mais detalhes.

Informações sobre a empresa

Nosso compromisso

Diversidade e inclusão

Relações com investidores

Fale conosco

Sala de imprensa

Mapa do site

Empregos

© Intel Corporation

Termos de uso

*Marcas comerciais

Privacidade

Cookies

Transparência da cadeira de fornecimento

As tecnologias Intel podem exigir ativação de hardware, software específico ou de serviços. // Nenhum produto ou componente pode ser totalmente seguro. // Os seus custos e resultados podem variar. // O desempenho varia de acordo com o uso, a configuração e outros fatores. // Veja nossos avisos legais completos e isenção de responsabilidades. // A Intel está comprometida em respeitar os direitos humanos e evitar cumplicidade com abusos de direitos humanos. Consulte Princípios Globais de Direitos Humanos da Intel. Os produtos e software da Intel são destinados a serem utilizados apenas em aplicações que não causem ou contribuam com a violação de um direito humano reconhecido internacionalmente.

THINK BIOS CONFIGURATOR V1

Revision 19

Copyright Lenovo 2020

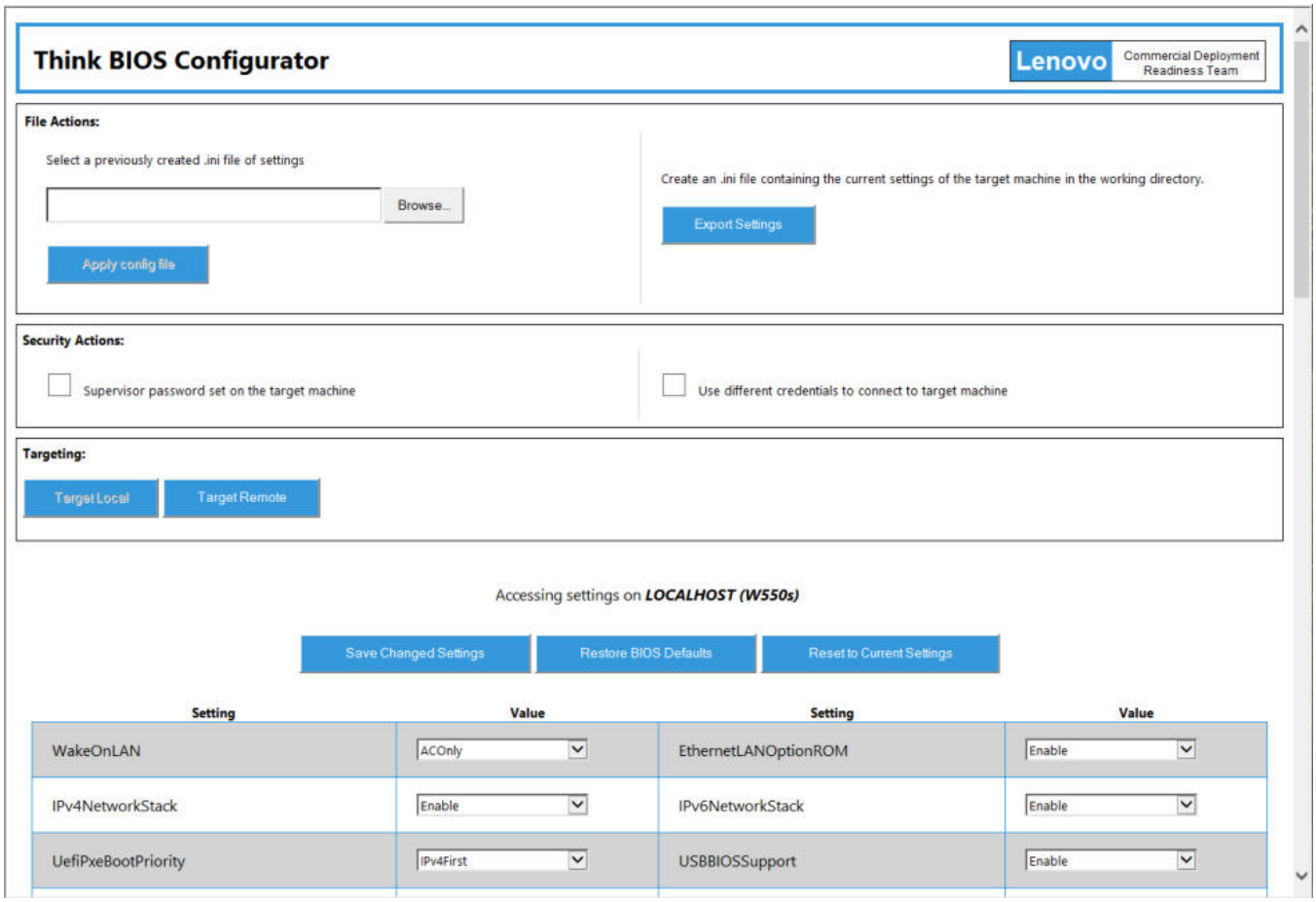
INTRODUCTION

The Think BIOS Configurator tool was developed using the WMI BIOS interface methods and the scripts located at this website to create a user friendly way of applying changes to the BIOS from within the Windows environment. This document will describe the ways the tool can be used and the various options it supports. The application needs no other files for execution. The application will read from WMI to provide the proper options for each of the available settings.

NOTE: Not all BIOS settings are exposed through the WMI interface. This tool will list only the settings that are configurable through WMI.

Standard execution of the application

This tool is in the HTML application format (hta) so it can be portable and be used in lightweight versions of Windows like WinPE without needing additional libraries to run. When launched by a user in Windows, the application will attempt to relaunch itself with administrative privileges which causes a User Account Control dialog to be displayed with the Program Name of "Microsoft (R) HTML application host" and the Verified Publisher as "Microsoft Windows". This occurs because access to the WMI BIOS Settings interface requires administrative privileges on the system and there is no "Run as Administrator" option for .HTA files. After approving the UAC prompt, the application window will appear. Below is an example of what a standard execution of the application will look like:



Copyright Lenovo 2020

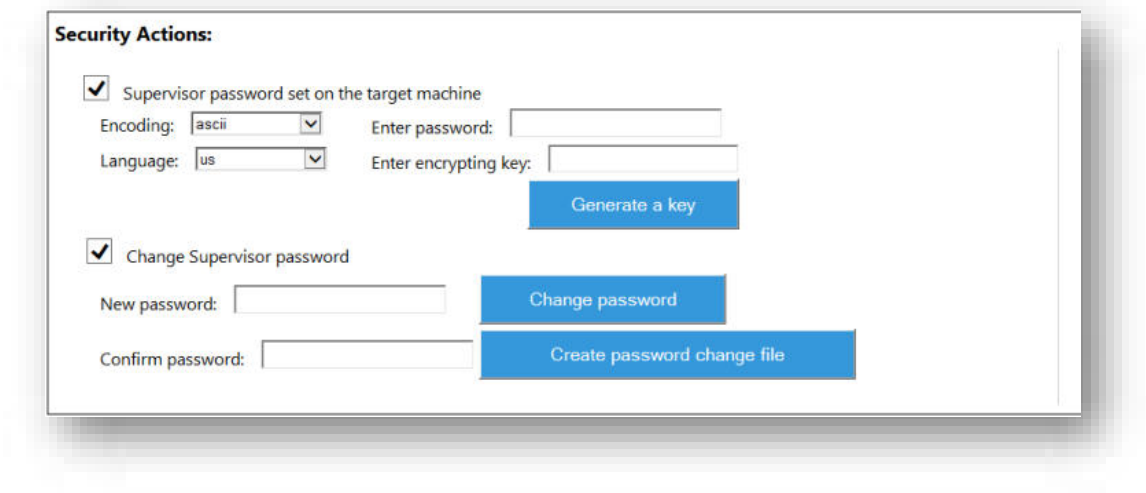
File Actions

At the top of the application screen is the File Actions section. On the left it is possible to browse to and select an .INI file that was previously generated by this program. Once selected, click **Apply Settings File** to make any changes detected in the .INI file. All the settings are read into the potential changes and then compared to the current settings of the machine. Only those that are different will be applied. A dialog box is displayed once the import is completed showing the settings that were successfully changed. This feature is also available via command line which is discussed in the Execution via Command Line section.

On the right, an .INI file of the current settings can be generated simply by clicking **Export Settings**. The file will be generated in the working directory the application is launched from. The file will be named <***model***>**Config.ini** where <***model***> is the text inside the parenthesis above the Settings Table. The settings that are exported are the current settings of the machine AND the pending changes to the machine. This is done to allow the user to create these files without actually having to commit changes to the machine. The created file has an optional first line if there is a supervisor password and the remaining lines are of the form ***key,value***. If there is a supervisor password on the machine the application will include it based on the details provided in the Security Actions sections below.

Security Actions

If settings are being changed on a system where a BIOS Supervisor Password has been set, the Security Actions section provides the ability to provide the necessary password details. Select the check box next to **Supervisor password set on the target machine** to expand the user interface to show input fields for the password details as shown below. If a password is detected on the machine, the first checkbox will automatically be checked.

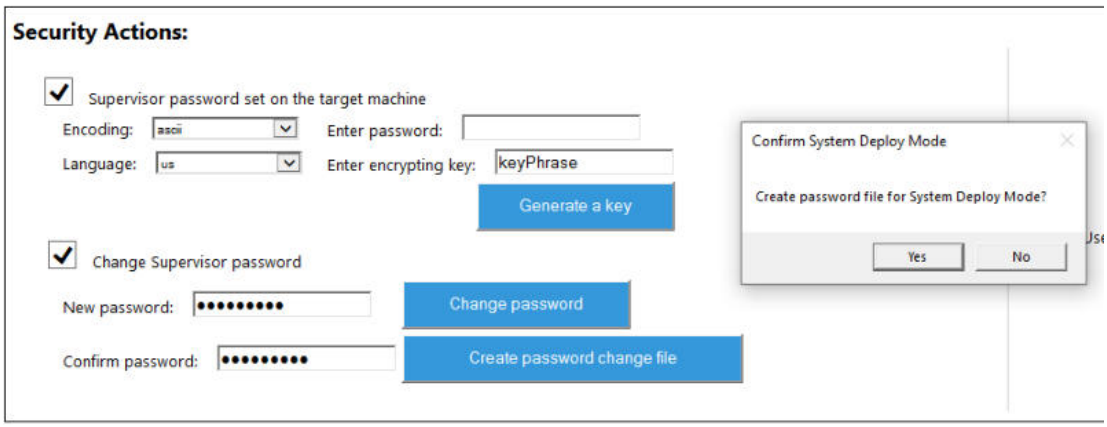


Encoding can be either "ascii" or "scancode" and language is either "us", "fr", "gr". In most cases, the user should only have to supply the password and leave the other fields as they are. The password box is for the Supervisor password on the targeted machine. The encrypting key box is only used if the Export Settings function will be used to capture the settings of this targeted machine into an .INI file. A random 16 character string can be generated or the user can create their own personal encryption key using characters from this set: a-z, A-Z, 0-9. Do not use any punctuation or special characters. This will allow the Supervisor password to be encrypted using xxTEA in the .INI file, which is simply plain text. The encrypting key would be used later when the tool is used to apply the settings in the .INI file.

Copyright Lenovo 2020

Under the first security action section is the area to change the current supervisor password. By providing the new password, the user can click the **Change password** button to change the current machine's password or click the **Create password change file** button to generate a file to change the password on multiple machines. If you want to clear the password from the machine just leave the new password fields blank. The generated password file will contain the previous password and the new password encrypted with the encrypting key that is provided above. Note: the user CANNOT set a supervisor password.

Now on updated Whiskey Lake ThinkPads, administrators can set a supervisor password using System Deployment Boot Mode (boot to device list and press 'delete'). In this one-time boot environment, a password change file can be used to set the supervisor password for the machine. To create a specialized System Deployment Boot Mode password file, leave the current supervisor password field blank and fill in the other information for a password change file.



On the right side of the Security Actions section the user can select the check box next to **Use different credentials to connect to target machine** to expand the user interface to show additional input fields. When connecting to a remote machine over the network, a username and password for a local administrator account of the targeted machine must be supplied. On a domain network, the username may need to be in the format of "<domain>\<username".

Note: the user CANNOT use different credentials when targeting the local machine.

Logging

A text file will be created using the machine type and serial number to uniquely identify the machine the tool is running on. A list of transactions and results of applying settings will be written to the file.

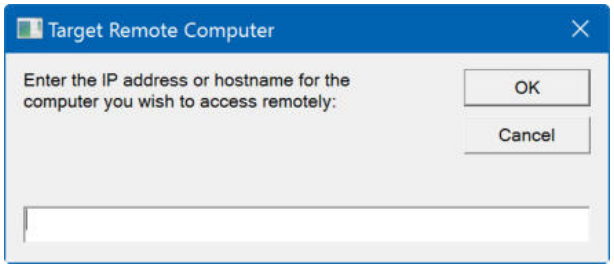
Targeting

By default the application will attempt to load the settings of the local machine when it launches. The address and model of the machine whose settings are being displayed will be displayed above the Settings table, such as:

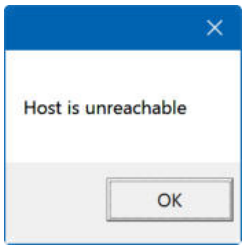
Accessing settings on ***LOCALHOST (W550s)***

If you would like to target another remote machine on the network, click **Target Remote** and the dialog below will be displayed

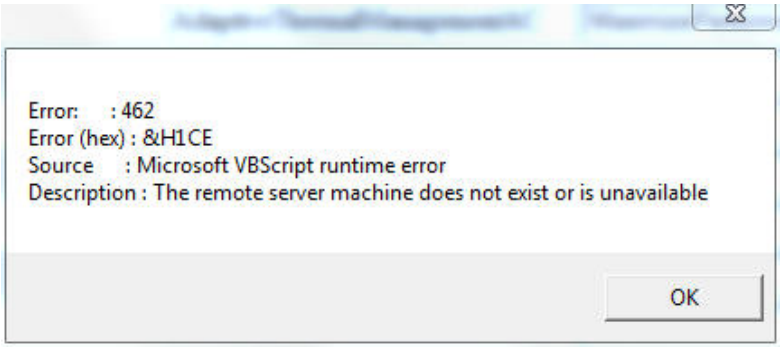
Copyright Lenovo 2020



If the host is unreachable, the application will gracefully display that information.

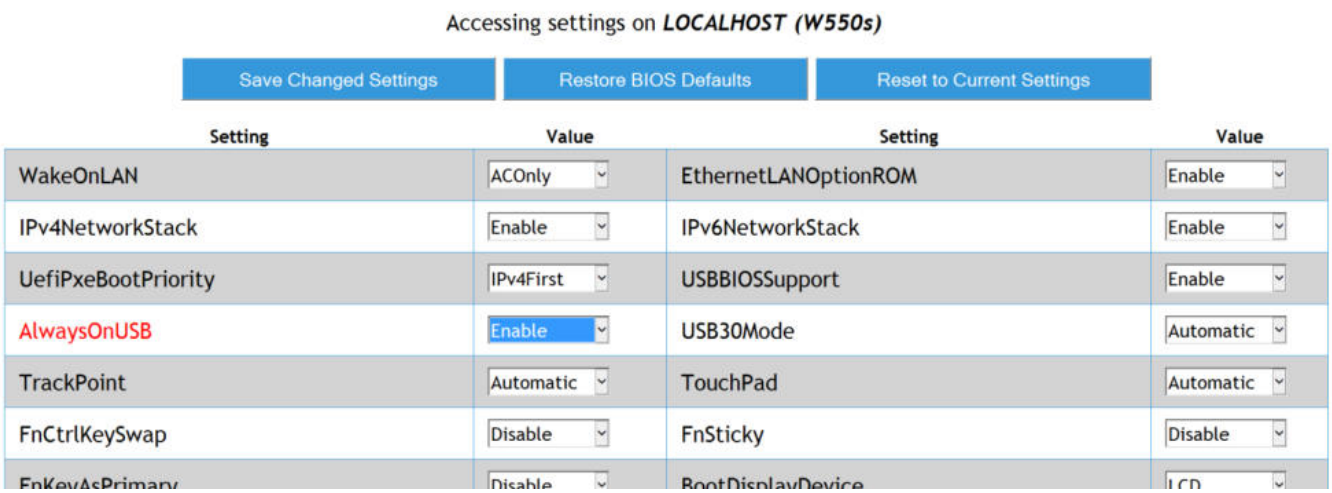


If the WMI service is unavailable on the target machine or the application is denied access another message box will come up and provide an error message similar to below. Once this dialog is acknowledged, the application will refresh with the information on the local machine.



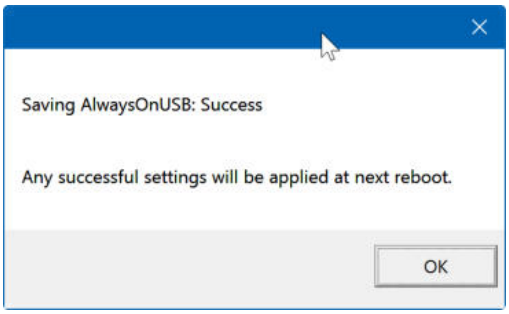
Once connected to the remote computer, the screen will refresh with the data that is on that machine. To switch back to the local machine, just click the 'Target Local' button, which is only enabled if the application is accessing a remote machine.

Settings Table



The Settings Table displays the current settings of the target machine. As seen above, each setting has an associated value column which can be changed easily. Most settings are in the form of dropdown boxes but options like 'BootOrder' have more complex options to select the new value of the setting. If the user makes any changes, the text of the setting name will be changed to red (as seen above with the AlwaysOnUSB setting) to signify that it is a value different than what is currently set on the computer.

Once all the required changes have been set, click **Save Changed Settings** and the application attempts to commit the changes to the machine. Only the settings that are pending change are attempted to be saved to save time and eliminate any issues with trying to commit a setting will the same value. This is what will be displayed after the button is clicked:

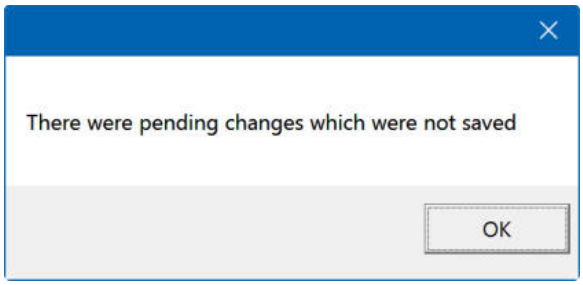


As seen above, the application was successful in setting one setting. Error messages are provided in the case of a failure. More than likely, the error users will see will be 'Access Denied'. **NOTE: All settings will only take affect once the computer is restarted.**

If settings have been changed in the application but not applied to the machine and the user wants to revert back to the original settings, click **Reset to Current Settings**. The user will see the items that were previously marked in red text will be reverted back to black text and the values reset to their original settings. This is a quick way for the user to create multiple configuration files and revert back to the settings they had already saved.

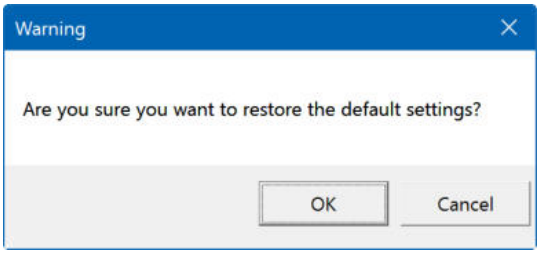
If a user closes the application with changes pending, a message will be displayed that there were pending changes. Unfortunately, there is a bug in Microsoft's code that makes it so the closing of the application cannot be stopped once it is started.

Copyright Lenovo 2020



As seen above, the application was successful in setting one setting. Error messages are provided in the case of a failure. More than likely, the error users will see will be 'Access Denied'. **All settings will only take affect once the computer is restarted.**

The **Restore BIOS Defaults** button applies factory default values to the settings. NOTE: Not all BIOS settings are affected by the BIOS defaults change and varies by product. If the button is clicked, a warning prompt will be shown to confirm the user wishes to do that.



Copyright Lenovo 2020

Execution via Command Line

This was a very important feature when developing this application. By having command line execution of the application, the user can use this in deployment situations. When used in this fashion, the application will flash briefly and suppress all notifications. All command line parameters must be enclosed in quotation marks and have the following format: "***switch=key,value***". There are no spaces around the equals sign. There are several switches that are supported. Order does not matter but parameters are processed from left to right. Therefore if for some reason the user provides any switch more than once the last one will be the one the application uses. If the user passes both the 'config' and 'file' switch in one command, the 'file' switch will take precedence over the 'config'.

File switch

To apply a configuration or password file via the command line, the user would want to use the 'file' switch. The configuration file can be described either by a full path or just the name if it is located in the same folder as the application itself. Just like the 'Apply config file', all the settings will be processed and applied if they are different than the current settings on the machine.

Eg. `ThinkBiosConfig.hta "file=C:\W550sConfig.ini"`

Config switch

To apply a single configuration change, the user would want to use the "config" switch. This switch is mainly used for when the user wants to change just one setting and using a configuration file would be too much overhead.

Eg. `ThinkBiosConfig.hta "config=USB30Mode,Disable"`

Pass switch

This switch is used in conjunction with both 'file' and 'config'. If there is a supervisor password on the target machine, the application needs this information to apply the settings.

In the case of the 'file' switch, the application will be expecting the encryption key that was used when creating the configuration file if the password was encrypted and stored in the file or the supervisor password itself. If there is an encrypted string at the beginning of the file, the application will attempt to decrypt the first line of the configuration file to retrieve the supervisor password that is stored in the file. Note – This option must be used with a password file.

Eg. `ThinkBiosConfig.hta "file=C:\W550sConfig.ini" "pass=myEncryptionKey"`

In the case of the 'config' switch, the application will be expecting the supervisor password itself. This will be passed to the application to save the setting properly.

Eg. `ThinkBiosConfig.hta "config=USB30Mode,Disable" "pass=mySupervisorPassword"`

Also if working with a different language than 'US' the user can enter their language along with the password in the following format (example demonstrates French password):

Eg. `ThinkBiosConfig.hta "config=USB30Mode,Disable" "pass=mySupervisorPassword,ascii,fr"`

Remote switch

The remote feature allows the user to set the target computer before the application displays the first settings. This can be used in two ways: set the target computer and open the GUI or set the target computer and apply a command line switch to it. To set the target computer for the GUI, only include the 'remote' switch.

Copyright Lenovo 2020

Eg. `ThinkBiosConfig.hta "remote=<IP_or_Hostname>"`

To apply a command line switch to the remote machine, just use the previously described switches. Remember order of the switches does not matter.

Eg. `ThinkBiosConfig.hta "remote=<IP_or_Hostname>" "file=C:\W550sConfig.ini"`

Log switch

Use this switch to control where the log file should be written to. By default, a log file with the name of *machineType_serialNumber.txt* will be created in the current directory with the tool.

Eg. `ThinkBiosConfig.hta "log=C:\path\to\log\"`

NoLog switch

Use this switch to prevent the log file from being created or written to. The switch is case insensitive.

Eg. `ThinkBiosConfig.hta "NoLog"`

Default switch

Use this switch to apply the default settings to a computer quickly. The only parameter for this setting is a case insensitive "true". Only when it is provided will the settings be reset. No actions will be taken if any other string is provided.

Eg. `ThinkBiosConfig.hta "default=true"`

Help switch

Shows a list of the most recent changes to the tool.

Eg. `ThinkBiosConfig.hta "help"`

Deployment Situations

This application can be used in a deployment environment like MDT or SCCM provided support for HTA/HTML is enabled (MDT boot images provide this by default, SCCM needs to have the feature enabled). The application must be called after the disk has been partitioned. In testing, placing the command during the Post-Install step seems like a good place. Also remember that a restart is required to apply the settings. Example code for a task sequence step:

cmd.exe /c *PathToApp*\ThinkBiosConfig.hta "config=BootOrder,HDD0:PCILAN"

Note: The ‘cmd.exe /c’ is needed 9 out of 10 times when running as a Local System account. In some cases it isn’t necessary but for consistency it is recommended.

Troubleshooting

If a supervisor password exists and you know you are typing in the correct password but are receiving ‘Access Denied’ errors, restart the machine. You may have exceeded the allowed attempts. The tool will validate the password to prevent exceeding the number of allowed attempts.

Copyright Lenovo 2020

M910x has a slightly different ‘Load Defaults’ functionality. Once it is completed, you will no longer be able to see the settings until after a reboot.

Powershell execution with command line parameters – To pass the desired switches, Powershell needs them inside single quotes.

Eg. `ThinkBiosConfig.hta '"help"'`

```
ThinkBiosConfig.hta '"file=C:\W550sConfig.ini"' '"pass=myEncryptionKey"'
```


Copyright Lenovo 2020

Red Hat
Customer Portal

Products & Services › Ecosystem › Certified Hardware › ThinkSystem SR530 (Xeon SP Gen 2)

This solution matches your environment.

ThinkSystem SR530 (Xeon SP Gen 2)

by Lenovo

LEARN MORE FROM LENOVO

Certifications

Support

Select a certification to see details:

Products	Version	Arch	Level	Notes	Additional Information
Red Hat Enterprise Linux	8.0 - 8.x	x86_64	Certified		Details

Products	Version	Arch	Level	Notes	Additional Information
Red Hat Enterprise Linux	7.6 - 7.x	x86_64	Certified		
Red Hat OpenStack Platform for Compute	16.1 - 16.x	x86_64	Certified		Details
Red Hat OpenStack Platform for Compute	16.0 - 16.x	x86_64	Certified		Details
Red Hat OpenStack Platform for Compute	13.0 - 13.x	x86_64	Certified		
Red Hat Gluster Storage	3.4 - 3.x	x86_64	Certified		
Red Hat Virtualization	4.2 - 4.3	x86_64	Certified	▸ Notes	

Copyright © 2021 Red Hat, Inc.

ThinkSystem Server with Intel Xeon SP (1st, 2nd Gen) UEFI Manual



Server Models: SD530, SD650, SN550, SN850, SR530, SR550, SR570, SR590, SR630, SR650, SR670, SR850, SR860, SR950, ST550, and ST558

Second Edition (December 2020)

© Copyright Lenovo 2020.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Chapter 1. ThinkSystem server with Intel Xeon SP (1st, 2nd Gen). 1

Chapter 2. Get started. 3

Chapter 3. System configuration and boot management 5

System information 5
System setting 7
- Device and I/O ports 8
- Driver health 16
- Legacy BIOS 18
- Memory 19
- Network 22
- Operating modes 24
- Power 28
- Processors 30
- Recovery and RAS 34
- Security 36
- Storage 40

Date and time 40
Start options 41
Boot manager 42
BMC settings 45
System event logs 48
User security 49

Appendix A. Notices. 55

Trademarks 56

© Copyright Lenovo 2020

Chapter 1. ThinkSystem server with Intel Xeon SP (1st, 2nd Gen)

This topic provides general introduction to the Unified Extensible Firmware Interface (UEFI).

UEFI is an interface packed with various features, including system information and settings, boot and runtime services, BMC settings, system event logs, and user security. This guide applies to the following server models:

• SR530 • SR550 • SR570 • SR590 • SR630 • SR650 • SR670 • SR850 • SR860 • SR950	• SD530 • SD650 • SN550 • SN850 • ST550 • ST558

Below table details the main menu:

Table 1. Main menu details

Item	Options	Description
System Configuration and Boot Management	N/A	Main menu
Select Language		Change the language for the current system.
Launch Graphical System Setup	N/A	Enter the graphical user interface for system setup, provisioning manager, and RAID configuration. When in Graphical System Setup, there will be no screen output to console, use VGA monitor for setup. **Note:** For more information, see Lenovo XClarity Provisioning Manager.
System Information	N/A	Display the basic details of the system.

© Copyright Lenovo 2020

Table 1. Main menu details (continued)

System Settings	N/A	Display or modify system settings. Changes may not take effect immediately. Save any changed settings and reboot the system.
Date and Time	N/A	Set the local Date and Time of the system.
Start Options	N/A	Boot a desired selection from the primary boot sequence as specified under **Boot Manager**.
Boot Manager	N/A	Change boot order, boot parameters, and boot from a file.
BMC Settings	N/A	Configure the management controller.
System Event Logs	N/A	Clear or view the System Event Log.
User Security	N/A	Set or change Power-On and Administrator passwords.
Save Settings	N/A	Save the changes and commit them to BMC.
Discard Settings	N/A	Discard any changes.
Load Default Settings	N/A	Load the default values for system settings.
Exit Setup Utility	N/A	Exit Setup.

Note: Depending on model and configuration, your server might look slightly different from the images and item descriptions in this guide.

Chapter 2. Get started

First launch

Perform the following steps to first launch the UEFI setup utilities.

1. (Optional)Connect the local keyboard, video, and mouse (KVM) to the server using a cable, or open the **Remote Console** page on the Lenovo XClarity Controller web user interface (XCC WebUI).
2. Power on the system and press F1.
3. If you have set the power on password, enter the correct password.
4. Wait for about 90 seconds, the setup utilities window is displayed.

© Copyright Lenovo 2020

Switch between graphic/text modes

The setup utilities are launched in graphic mode by default, the utilities can also be launched in text mode. You can switch between the two modes by referring to sections below.

Graphic mode to text mode

If you have entered graphic mode and need to switch to text mode, perform the following steps.

1. On the main interface, choose **UEFI Setup** > **System Settings** > **<F1> Start Control**.
2. Select **Text Setup** for **<F1> Start Control**.
3. Restart the server and press F1.
4. Wait for about 90 seconds, the setup utilities window is displayed in text mode.

Text mode to graphic mode

If you have entered text mode and need to switch to graphic mode, perform the following steps.

1. On the main interface, choose **System Settings** > **<F1> Start Control**.
2. Select **Tool Suite** or **Auto** for **<F1> Start Control**.
3. Restart the server and press F1.
4. Wait for about 90 seconds, the setup utilities window is displayed in graphic mode.

Chapter 3. System configuration and boot management

This chapter details system setup utility.

System information

Select **System Information**, and then the following window is displayed:



Table 2. System information details

Item	Description
System Summary	Display the basic details of the system.
Product Data	Display system firmware information.

System Summary

Item	Description
System Identification Data	
Machine Type/Model	Specify the system machine type and model.
Serial Number	Specify the tag for the serial number.
UUID Number	Specify the tag for the UUID.

© Copyright Lenovo 2020

Asset Tag Number	Specify a customer assigned system asset tag number.
Processor	
Installed CPU packages	Specify the number of installed CPU packages.
Processor Speed	Specify the processor speed.
UPI Link Speed	Specify the UPI link speed.
Memory	
Memory Mode	Specify the memory mode.
Memory Speed	Specify the installed memory speed.
Total Memory Detected	Specify the total amount of the memory from the sum of all DIMM installed.
Total Usable Memory Capacity	Specify the amount of usable memory after deducting the overhead caused by mirroring mode, reserved or bad blocks, etc.
Volatile Memory Capacity*	Usable volatile memory capacity, seen by the OS as standard RAM.
Non-volatile Memory Capacity*	Usable non-volatile memory capacity, could be partitioned and used by the OS as persistent RAM or as persistent storage.

Notes: Settings marked with asterisk (*) are available on the following models only: .

- SD530
- SD650
- SN550
- SN850
- SR570
- SR590
- SR630
- SR650
- SR850
- SR860
- SR950

Product Data

Item	Description
Host Firmware	
Build ID	Specify the build ID of the host firmware.
Version	Specify the version of the host firmware.
Build Date	Specify the build date of the host firmware.
BMC Firmware	
Build ID	Specify the build ID of the BMC firmware.

Version	Specify the version of the BMC firmware.
Build Date	Specify the build date of the BMC firmware.

System setting

Select **System Settings** and press Enter. Then the following window is displayed:



Table 3. System setting details

Item	Options	Description
Start Control	• **Auto** • Tool Suite • Text Setup	Press F1 to start control. **Auto** is the default setting.
Devices and I/O Ports	N/A	Display onboard devices and I/O port options.
Driver Health	N/A	View the health of the controllers in the system as reported by their corresponding drivers.
Intel Optane DCPMMs*	N/A	View and configure Intel Optane DCPMMs.
Legacy BIOS	N/A	Configure system UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.
Memory	N/A	Display and provide options to change the memory settings.

Table 3. System setting details (continued)

Network	N/A	Display network devices and network related settings.
Operating Modes	N/A	Select the operating mode based on your preference. **Note:** Power savings and performance are also highly dependent on hardware configuration and the software running on the system.
Power	N/A	Configure power scheme options.
Processors	N/A	Display and provide options to change the processor settings.
Recovery and RAS	N/A	Configure recovery policies and advanced reliability, availability, and serviceability settings.
Security	N/A	Configure system security settings.
Storage	N/A	Manage storage adapter options. Some systems may use planar devices and can be configured under “Devices and I/O Ports”.

Notes: Setting marked with asterisk (*) is available on the following models only: .

- SD530
- SD650
- SN550
- SN850
- SR570
- SR590
- SR630
- SR650
- SR850
- SR860
- SR950

Device and I/O ports

This menu displays onboard devices and I/O port options.

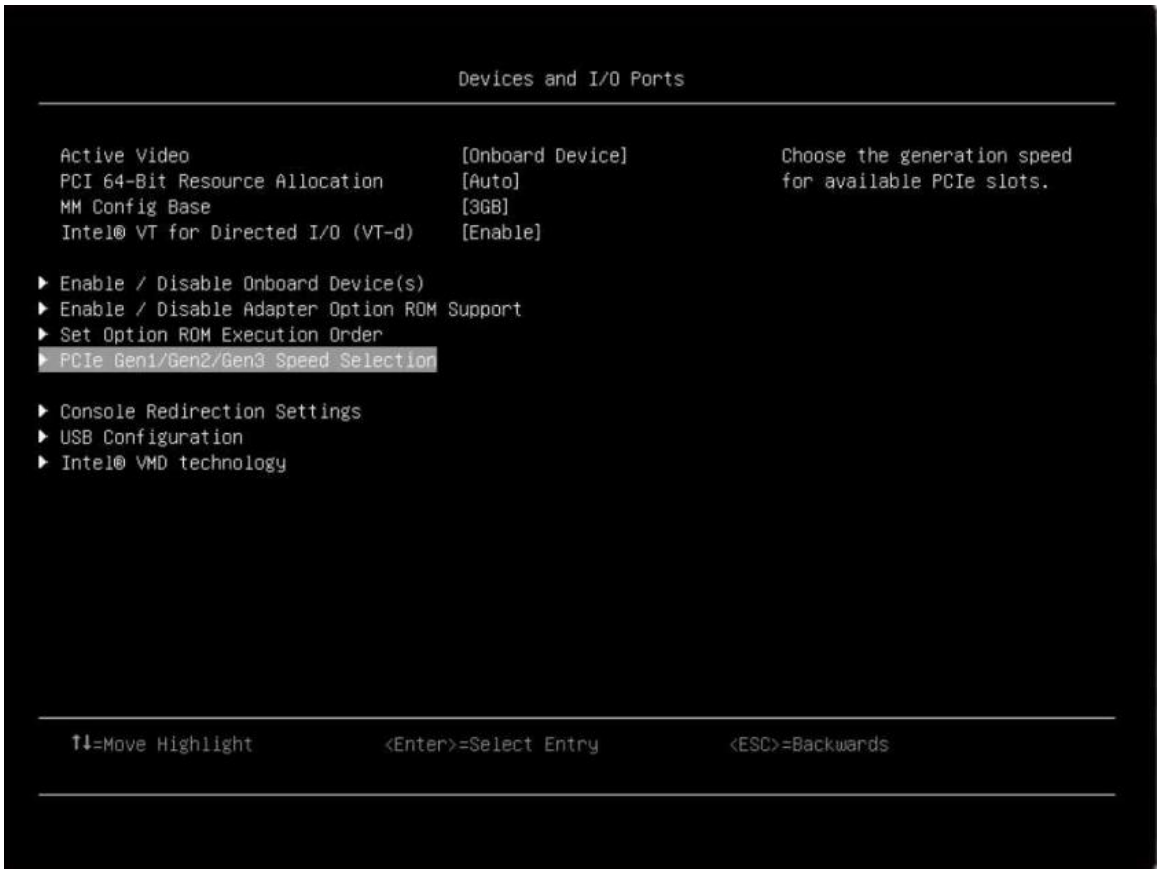


Table 4. Device and I/O ports details

Item	Options	Description
Active Video	• **Onboard Device** • Add-in Device	This setting only applies when the server has an add-in video adapter. When the option ROM is set to Legacy for both onboard and add-in video adapters, the Active Video setting controls which single adapter will display the System Setup utility. **Onboard Device** is the default setting. Regardless of this setting, the system boot early video is displayed at the onboard video only, and the management controller remote console shows the onboard video only. This setting does not affect how the OS chooses to display its graphical desktop.
PCI 64-Bit Resource Allocation	• Enable • Disable • **Auto**	[Enable] or [Disable] the allocation of 64-bit resources for PCI. **Auto** is the default setting, would allocate some resources below 4GB for legacy compatibility.
MM Config Base	• **3GB** • 2GB • 1GB	Recommend default setting of **3GB**. A higher value will increase memory available to the OS below 4G but reduce memory mapped I/O (MMIO) resource available to PCI adapters. A lower than 3GB value will increase MMIO resources but decrease memory available to OS below 4GB. Revert to your previous selection if you see new issues with changed setting.

Table 4. Device and I/O ports details (continued)

Intel® VT for Direct I/O (VT-d)	• **Enable** • Disable	Enable/Disable Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables. **Enable** is the default setting.
Enable/Disable Onboard Device(s)	N/A	Enable or disable onboard devices or slots.
Enable/Disable Adapter Option ROM Support	N/A	Control Legacy and UEFI-compliant adapter support. Disabling UEFI/Legacy support may adversely affect pre-boot/boot functions.
Set Option ROM Execution Order	N/A	Control legacy ROM load order.
PCIe Gen1/Gen2/Gen3 Speed Selection	N/A	Choose the generation speed for available PCIe slots.
Console Redirection Settings	N/A	Settings for console redirection and COM port settings.
USB Configuration	N/A	Disable USB storage devices or individual ports.
Intel® VMD technology	N/A	Press Enter to bring up the Intel® VMD for Volume Management Device Configuration menu.

Note: Settings in this menu vary with models and configurations.

Enable/Disable Onboard Device(s)

Item	Options	Description
Onboard Video	• **Enable** • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting.
Onboard SATA	• **Enable** • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Onboard sSATA (for M.2 SATA mode)	• **Enable** • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Slot 1 (Display depending on which riser card is installed)	• **Auto** • Enable • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Auto** is the default setting. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Slot 2 (Display depending on which riser card is installed)	• **Auto** • Enable • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Auto** is the default setting. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.

Slot (n...) (Display depending on which riser card is installed)	• **Auto** • Enable • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Auto** is the default setting. [Auto] is removing the port if there is no device or errors on that device. **Note:** [Auto] is the setting for PCIe devices by CPU only.
Onboard LAN (Display when PHY card installed)	• **Enable** • Disable	Disabling an entry will prevent the associated device from being enumerated during subsequent boots. **Enable** is the default setting.
Onboard LAN Port 1 (The number of “Onboard LAN Port x” varies with the PHY card.)	• **Enable** • Disable	Disabling an entry will prevent the associated device from being enumerated during boot. greyout when “Onboard LAN” is [Disable]; Hidden when this port is not present. **Enable** is the default setting.
Onboard LAN Port 2 (The number of “Onboard LAN Port x” varies with the PHY card.)	• **Enable** • Disable	Disabling an entry will prevent the associated device from being enumerated during boot. greyout when “Onboard LAN” is [Disable]; Hidden when this port is not present. **Enable** is the default setting.

Enable/Disable Adapter Option ROM Support

Item	Options	Description
Onboard SATA	• **Auto** • Disable • UEFI • Legacy	Select whether UEFI or legacy option ROM of this device will be executed. [Disable] means both UEFI and legacy option ROM will not be executed. [UEFI] means only UEFI option ROM will be executed. [Legacy] means only legacy option ROM will be executed. [Auto] means option ROMs will be executed based on “System Boot Mode”, UEFI or legacy. When [Legacy] is selected, "Onboard Video" will also be changed to [Legacy] automatically and cannot be changed to other options. **Auto** is the default setting.
Onboard sSATA (for M.2 SATA mode)	• **Auto** • Disable • UEFI • Legacy	Select whether UEFI or legacy option ROM of this device will be executed. [Disable] means both UEFI and legacy option ROM will not be executed. [UEFI] means only UEFI option ROM will be executed. [Legacy] means only legacy option ROM will be executed. [Auto] means option ROMs will be executed based on “System Boot Mode”, UEFI or legacy. When [Legacy] is selected, "Onboard Video" will also be changed to [Legacy] automatically and cannot be changed to other options. **Auto** is the default setting.
Onboard Video	• Auto • Disable • UEFI • **Legacy**	Select whether UEFI or legacy option ROM of this device will be executed. [Disable] means both UEFI and legacy option ROM will not be executed. [UEFI] means only UEFI option ROM will be executed. [Legacy] means only legacy option ROM will be executed. [Auto] means option ROMs will be executed based on “System Boot Mode”, UEFI or legacy. **Legacy** is the default setting.

Onboard LAN Port 1 (The number of “Onboard LAN Port x” varies with PHY card.)	• **Auto** • Disable • UEFI • Legacy	Select whether UEFI or legacy option ROM of this device will be executed. [Disable] means both UEFI and legacy option ROM will not be executed. [UEFI] means only UEFI option ROM will be executed. [Legacy] means only legacy option ROM will be executed. [Auto] means option ROMs will be executed based on “System Boot Mode”, UEFI or legacy. When [Legacy] is selected, "Onboard Video" will also be changed to [Legacy] automatically and cannot be changed to other options. **Auto** is the default setting.
Slot 1 (Display depending on which riser card is installed.)	• **Auto** • Disable • UEFI • Legacy	When card installed: Select whether UEFI or legacy option ROM of this device will be executed. [Disable] means both UEFI and legacy option ROM will not be executed. [UEFI] means only UEFI option ROM will be executed. [Legacy] means only legacy option ROM will be executed. [Auto] means option ROMs will be executed based on “System Boot Mode”, UEFI or legacy. When [Legacy] is selected, "Onboard Video" will also be changed to [Legacy] automatically and cannot be changed to other options. When there is NO card installed: Slot is empty **Auto** is the default setting.

Set Option ROM Execution Order

Item	Options	Description
Set Option ROM Execution Order **Notes:** • 1. “Onboard LAN Port x” depends on whether PHY card is installed or not. • 2. Slot 1~3 and Slot 5~6 will display depending on which riser card is installed.	• Onboard Video • Onboard SATA • Onboard sSATA • Onboard LAN • Slot 1 • Slot 2 • Slot 3 • Slot 4 • Slot 5 • Slot 6 • Slot 7 • Slot 8	Select the load order for legacy PCI option ROM(s). Use the + key to execute the selected devices ROM sooner or – key to execute later.

PCIe Gen1/Gen2/Gen3 Speed Selection

Item	Options	Description
Slot 1 (Display depending on which riser card is installed.)	• Gen1 • Gen2 • **Gen3**	Set the PCIe slot as Generation 1 or Generation 2 or Generation 3. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power off and power on the system for these settings to take effect.

Slot 2 (Display depending on which riser card is installed.)	• Gen1 • Gen2 • **Gen3**	Set the PCIe slot as Generation 1 or Generation 2 or Generation 3. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power off and power on the system for these settings to take effect.
Slot 7 (for RAID slot)	• Gen1 • Gen2 • **Gen3**	Set the PCIe slot as Generation 1 or Generation 2 or Generation 3. **Note:** Some adapters may not operate correctly in Gen2 or Gen3. Make sure to power OFF and power ON the system for these settings to take effect.

Console Redirection Settings

Item	Options	Description
COM Port 1	• **Enable** • Disable	Enable or disable COM 1 device. If [Disable] is selected, the associated COM1 terminal settings will be hidden. **Enable** is the default setting.
COM Port 2	• **Enable** • Disable	Enable or disable COM 2 device. If [Disable] is selected, the associated COM 2 terminal settings will be hidden. **Enable** is the default setting.
Console Redirection	• Enable • Disable • **Auto**	Set remote console redirection preference to enable or disable console redirection. While [Auto] is selected, console redirection will be enabled automatically if IPMI Serial over LAN status is active. **Auto** is the default setting.
Serial Port Sharing	• Enable • **Disable**	Enable the system Baseboard Management Controller to allow access to the system serial port. If this option is set to [Enable], the BMC will be allowed to control the serial communication port as requested by remote control commands. If sharing is [Disable], the serial port will be assigned to the BMC unless the “Serial Port Access Mode” is set to [Disable]. **Disable** is the default setting.
Serial Port Access Mode	• Shared • Dedicated • **Disable**	This option allows you to control the access the system Baseboard Management Controller has over the system serial port. 1. Shared mode: By selecting [Shared], the serial port will be available for POST and operating system use; however the BMC will/can monitor the serial data for a takeover control sequence. 2. Dedicated mode: By selecting [Dedicated], the BMC will have complete control of the serial port and POST and/or the operating system will not be able to use the serial port. 3. Disable mode: By selecting [Disable], the BMC will not have any access to the serial port. **Disable** is the default setting.

SP Redirection	• Enable • **Disable**	This option is only displayed while “Console Redirection”, “COM Port 1” and “COM Port 2” set to [Enable]. It allows you to choose which COM port to have the redirection. **Note:** Only show when set Console Redirection to Enable. **Disable** is the default setting.
Legacy OS/Option ROM Display	• COM Port 2 • **COM Port 1**	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages. **COM Port 1** is the default setting.
COM1 Settings	N/A	Settings required for serial connections used for asynchronous start-stop communication.
COM1 Baud Rate	• **115200** • 57600 • 38400 • 19200 • 9600	Control the connection speed between the host and remote system. **115200** is the default setting.
COM1 Data Bits	• **8** • 7	Set the number of Data bits in each character.
COM1 Parity	• **None** • Odd • Even	Select parity bit in each character to be [None], [Odd], or [Even]. [None] means that no parity bit is sent at all. **None** is the default setting.
COM1 Stop Bits	• 2 • **1**	Set Stop Bits. Stop Bits sent at the end of every character allow the signal receiver to detect the end of a character and to resynchronize with the character stream.
COM1 Terminal Emulation	• VT100 • VT-UTF8 • **ANSI**	Select [VT100] only if the remote emulator does not support ANSI text graphics. Consult the emulator documentation for more information. **ANSI** is the default setting.
COM1 Active After Boot	• Enable • **Disable**	When [Disable] is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When [Enable] is selected, then Legacy Console Redirection is enabled for legacy OS. "COM1 Active after Boot" and "COM2 Active after Boot" settings go together, and if you change one setting, it automatically changes the other. Disable is the default setting.
COM1 Flow Control	• **Disable** • Hardware	Select [Hardware] only if the remote emulator support and is using hardware flow control. Consult the emulator documentation for more information. **Disable** is the default setting.
COM2 Settings	N/A	Settings required for serial connections used for asynchronous start-stop communication.

COM2 Baud Rate	• **115200** • 57600 • 38400 • 19200 • 9600	Control the connection speed between the host and remote system. **115200** is the default setting.
COM2 Data Bits	• **8** • 7	Set the number of Data bits in each character.
COM2 Parity	• **None** • Odd • Even	Select parity bit in each character to be [None], [Odd], or [Even]. [None] means that no parity bit is sent at all. **None** is the default setting.
COM2 Stop Bits	• 2 • **1**	Set Stop Bits. Stop Bits sent at the end of every character allow the signal receiver to detect the end of a character and to resynchronize with the character stream.
COM2 Terminal Emulation	• VT100 • VT-UTF8 • **ANSI**	Select [VT100] only if the remote emulator does not support ANSI text graphics. Consult the emulator documentation for more information. **ANSI** is the default setting.
COM2 Active After Boot	• Enable • **Disable**	When [Disable] is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When [Enable] is selected, then Legacy Console Redirection is enabled for legacy OS. "COM1 Active after Boot" and "COM2 Active after Boot" settings go together, and if you change one setting, it automatically changes the other. **Disable** is the default setting.
COM2 Flow Control	• **Disable** • Hardware	Select [Hardware] only if the remote emulator support and is using hardware flow control. Please consult the emulator documentation for more information. **Disable** is the default setting.

USB Configuration

Item	Options	Description
USB Mass Storage Driver Support	• **Enable** • Disable	Enable/Disable USB Mass Storage Driver Support. This setting only takes effect in post time. **Enable** is the default setting. **Notes:** If the USB Mass Storage Driver Support is disabled, • The GUI tool for UEFI Setup utilities is disabled, in this case, the UEFI Setup utilities can only be launched in text mode. • Some other features relying on the USB Mass Storage Driver Support might be disabled as well.
USB Front Port 1	• **Enable** • Disable	Enable/Disabe USB individual ports. **Enable** is the default setting.
USB Front Port 2	• **Enable** • Disable	Enable/Disabe USB individual ports. **Enable** is the default setting.

USB Rear Port 1	• **Enable** • Disable	Enable/Disabe USB individual ports. **Enable** is the default setting.
USB Rear Port 2	• **Enable** • Disable	Enable/Disabe USB individual ports. **Enable** is the default setting.

Intel® VMD technology

Item	Options	Description
Intel® VMDTechnology	N/A	Press Enter to bring up the Intel® VMD for Volume Management Device Configuration menu.
Enable/Disable Intel® VMD	• Enable • **Disable**	Enable/Disable Intel® Volume Management Device Technology. **Disable** is the default setting.

Driver health

This menu displays the health of the controllers in the system as reported by their corresponding drivers.



Table 5. Driver health details

Item	Options	Description
The platform is:	The platform is: • **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Select this option to view the health of the controllers in the system as reported by their corresponding drivers.
Driver/Controller Status		
Controller Name - Status	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Select this option to view the health of controller.

Table 5. Driver health details (continued)

POST Attempts Driver	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Select this option to view the health of post attempts driver.
Partition Driver (MBR/GPT/El Torito)	• **Healthy** • Repair Required • Configuration Required • Operation Failed • Reconnect Required • Reboot Required • Shutdown Required • No Operation Required	Select this option to view the health of partition driver.

Legacy BIOS

This menu configures system UEFI firmware execution environment preferences for supporting legacy OS and legacy Option ROM.



Table 6. Legacy BIOS details

Item	Options	Description
Legacy BIOS	• **Enable** • Disable	Enable/Disable the system UEFI firmware execution environment for supporting legacy OS and legacy Option ROM. **Enable** is the default setting.
Rehook INT 19h	• Enable • **Disable**	[Enable] prevents devices from taking control of the boot process. **Disable** is the default setting.
Non-Onboard PXE	• **Enable** • Disable	Enable/Disable legacy PXE boot for installed network adapters. **Enable** is the default setting.

Memory

This menu displays and provides options to change the memory setting.

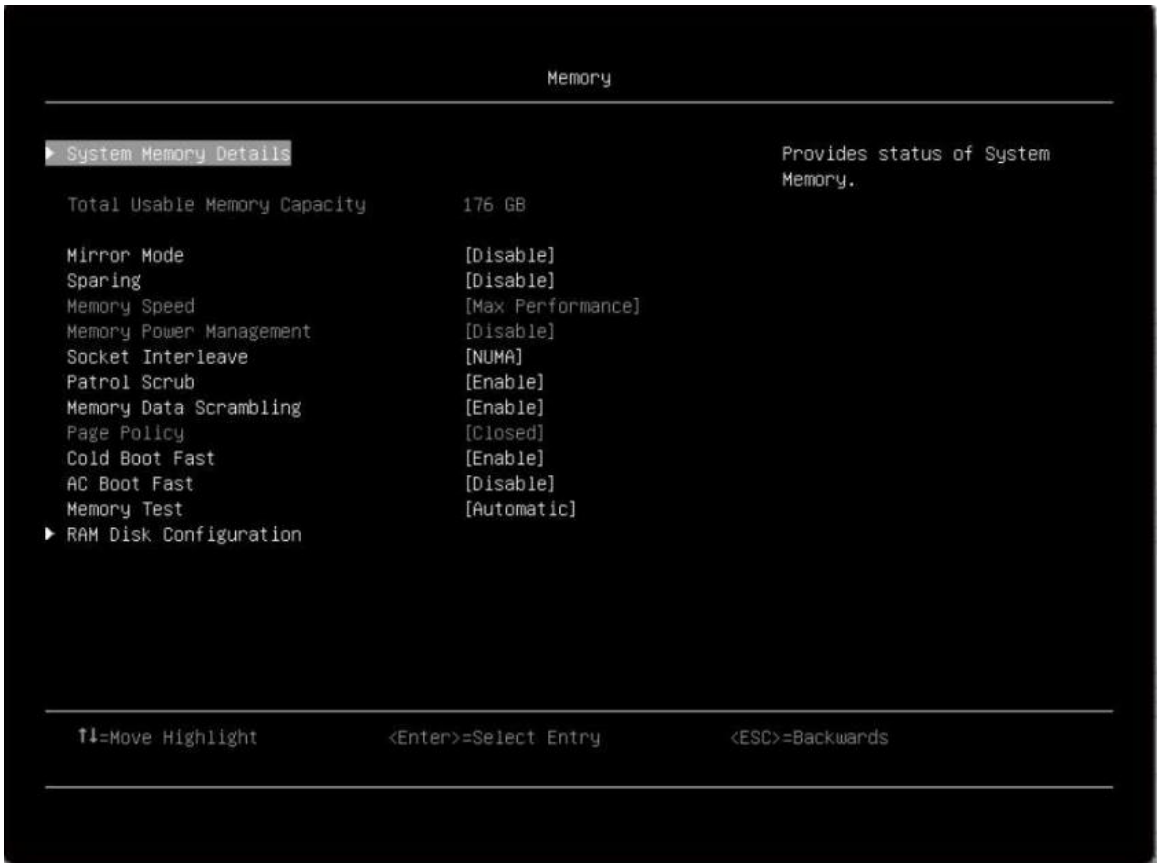


Table 7. Memory details

Item	Options	Description
System Memory Details	N/A	Provides status of System Memory.
Total Usable Memory Capacity	yyyy GB	Display the total usable memory capacity.
Mirror Mode	• **Disable** • Full • Partial **Note:** Partial is only available on Intel Xeon Gold, Platinum processors.	**For Intel Xeon Bronze, Silver processors** Mirror Type configures the system hardware to shadow all memory writes to secondary memory. Full mirroring reduces the available system memory by half of the total installed memory. **For Intel Xeon Gold, Platinum processors** Mirror Type configures the system hardware to shadow all memory writes to secondary memory. Full mirroring reduces the available system memorprocessoty by half of the total installed memory. Partial mirroring reduces the available system memory by a maximum of 36 GB per **Disable** is the default setting.
Sparing	• **Disable** • Enable	Rank Sparing is supported but default mode of leaving it disabled as ADDDC gives a similar protection without losing capacity. **Disable** is the default setting.

Table 7. Memory details (continued)

Memory Speed	• Minimal Power • Balanced • **Max Performance**	Select the desired memory speed. [Maximum Performance] mode maximizes performance. [Balanced] mode offers a balance between performance and power. [Minimal power] mode maximizes power savings. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, choose [Custom Mode] in "Operating Mode" located under "System Setting" submenu. **Max Performance** is the default setting.
Memory Power Management	• Automatic • **Disable**	[Disable] provides maximum performance but minimum power savings. [Automatic] is suitable for most applications. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in "Operating Mode" located under "System Setting" submenu. Disable is the default setting.
Socket Interleave	• **NUMA** • Non-NUMA	Sets Socket Interleave to NUMA(Non Unified Memory Architecture) or Non-NUMA. [NUMA]: Memory is not interleaved across processors. [Non-NUMA]: Memory is interleaved across processors. **Note:** Changing this setting will require a Power Good reset to take effect.
Patrol Scrub	• **Enable** • Disable	Enable/Disable "Patrol Scrub" which proactively searches the system memory to repair correctable errors. **Enable** is the default setting.
Memory Data Scrambling	• **Enable** • Disable	Memory Data Scrambling Disable/Enable. **Enable** is the default setting.
ADDDC Sparing	• **Disable** • Enable	Enable/Disable ADDDC Sparing. This setting is [Disable] and grayed out when **Page Policy** is [Adaptive]. Enabling ADDDC may cause reduced reliability of memory error correction in virtual lockstep under rare conditions. **Disable** is the default setting.
Page Policy	• **Adaptive** • Closed	Adaptive Page Policy can improve performance for applications with a highly localized memory access pattern; Closed Page Policy can benefit applications that access memory more randomly. This setting is [Closed] and grayed out when **ADDDC Sparing** is [Enable]. **Adaptive** is the default setting.
Cold Boot Fast	• **Enable** • Disable	Enable/Disable "Cold Boot Fast". **Enable** is the default setting.
Memory Test	• **Automatic** • Disable • Enable	[Enable] Enables memory test during normal boot. [Disable] - Disables this feature. [Automatic] - Skip memory test by default unless memory configuration changed or greater than 90 days since last time test ran. **Automatic** is the default setting.
RAM Disk Configuration	N/A	Press Enter to create/remove RAM disks.

Table 7. Memory details (continued)

System Memory Details	N/A	Display system memory details.
DIMM Details For Processor X	N/A	Display DIMM status.

RAM Disk Configuration

Item	Options	Description
Disk Memory Type	• **Boot Service Data** • Reserved	Specify type of memory to use from available memory pool in system to create a disk. **Boot Service Data** is the default setting.
Create raw	N/A	Create a raw RAM disk.
Create from file	N/A	Create a RAM disk from a given file.
Create RAM disk list	N/A	Specify RAM disk list.
Remove selected RAM disk(s)	N/A	Remove selected RAM disk(s)

Network

This menu displays network devices and network related setting.

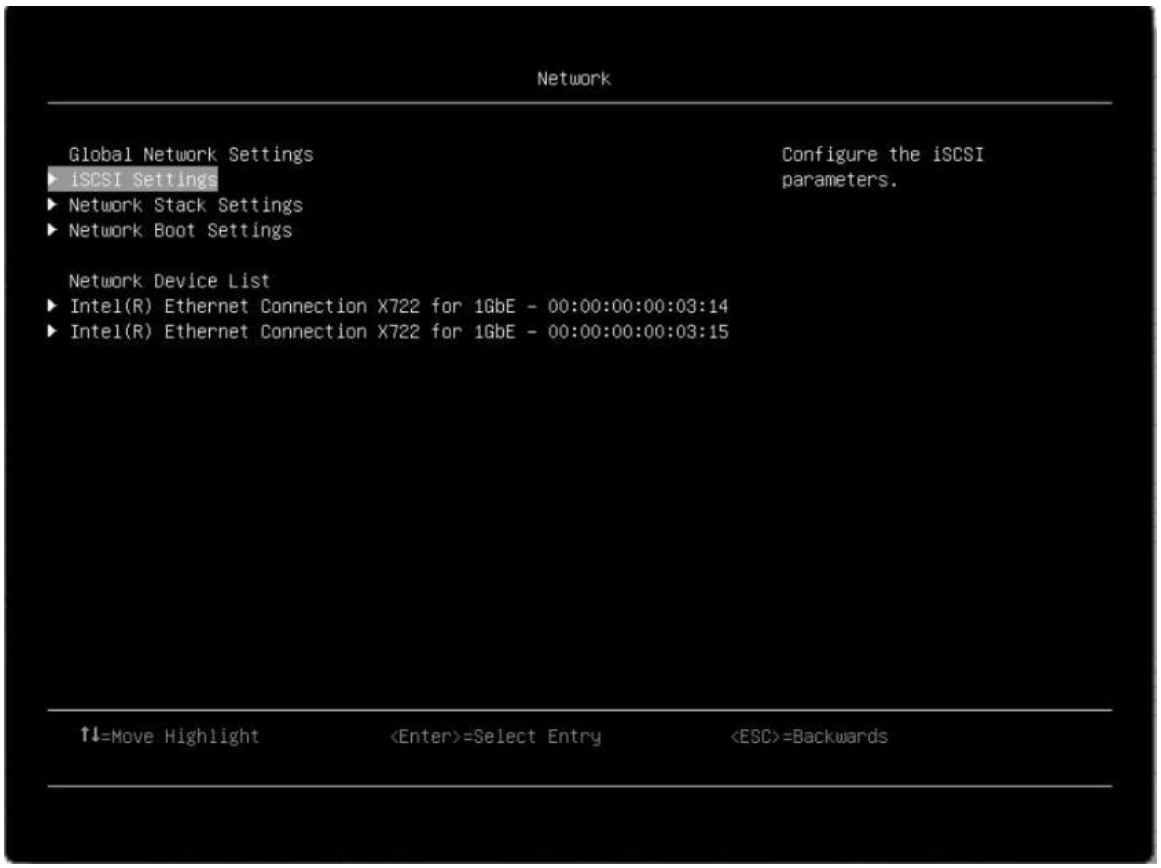


Table 8. Network details

Item	Options	Description
Global Network Settings	N/A	Specify global network settings.
iSCSI Settings	N/A	Configure the iSCSI parameters.
Network Stack Settings	N/A	Specify Network Stack Settings.
Network Boot Settings	N/A	Configure the network boot parameters
Network Device List	N/A	Specify network device list.

iSCSI Settings

Item	Options	Description
iSCSI Initiator Name	Iqn.1986-03.com.example	The worldwide unique name of iSCSI Initiator. Only IQN format is accepted. Range is from 4 to 233.
Add an Attempt	N/A	Add an Attempt
List of Attempts. **Note:** Only appears when attempts exist. Selecting an item will lead to Attempt Configuration page in 2.1.10.1.1.1.	N/A	MAC: XX:XX:XX:XX:XX:XX, PFA: Bus XX | Dev XX | Func XX, “iSCSI Mode”: [%s1], “Internet Protocol”: [%s2] Exact value will be different depends on the attempt settings. %s1 will be option name for iSCSI Mode. %s2 will be the setting name for Internet Protocol.
Delete Attempts	N/A	Delete one or more attempts
Change Attempt Order	N/A	Change the order of Attempts using +/- keys. Use arrow keys to select the attempt then press +/- to move the attempt up/down in the attempt order list.

Network Stack Settings

Item	Options	Description
Network Stack	• **Enable** • Disable	Enable/Disable UEFI Network Stack. **Enable** is the default setting.
IPv4 PXE Support	• **Enable** • Disable	Enable IPv4 PXE Boot Support. If disabled IPv4 PXE boot option will not be created. **Enable** is the default setting.
IPv4 HTTP Support	• Enable • **Disable**	Enable IPv4 HTTP Boot Support. If disabled IPv4 HTTP boot option will not be created. **Enable** is the default setting.
IPv6 PXE Support	• **Enable** • Disable	Enable IPv6 PXE Boot Support. If disabled IPv6 PXE boot option will not be created. **Enable** is the default setting.
IPv6 HTTP Support	• Enable • **Disable**	Enable IPv6 HTTP Boot Support. If disabled IPv6 HTTP boot option will not be created. **Disable** is the default setting.

PXE boot wait time	0	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value. **Notes:** When inputting an invalid value, the following popup message box will show up: • ERROR • Invalid Input Range • Ok
Media detect count	1	Number of times presence of media will be checked. Use either +/- or numeric keys to set the value. **Notes:** When inputting an invalid value, the following popup message box will show up: • ERROR • Invalid Input Range • Ok

Network Boot Settings

Item	Options	Description
List of NICs in the system e.g. MAC:XX:XX:XX:XX:XX:XX Onboard PFA XX:XX:XX	N/A	Set the boot configuration parameters on MAC XX:XX:XX:XX:XX:XX PCI Function Address: Bus XX:Dev XX:Func: XX

Operating modes

Select the operating mode bases on your preference.



Table 9. Operating modes details

Item	Options	Description
Choose Operating Mode	• Minimal Power • Efficiency – Favor Power • **Efficiency – Favor Performance** • Custom Mode • Maximum Performance	Select the operating mode based on your preference. Power savings and performance are also highly dependent on hardware and software running on the system. **Efficiency – Favor Performance** is the default setting.
Memory Speed	• Minimal Power • Balanced • **Max Performance**	Select the desired memory speed. [Maximum performance] mode maximizes performance. [Balanced] mode offers a balance between performance and power. [Minimal power] mode maximizes power savings. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, choose [Custom Mode] in “Operating Mode located under “System Setting” submenu. **Max Performance** is the default setting.

Table 9. Operating modes details (continued)

Memory Power Management	• Automatic • **Disabled**	[Disabled] provides maximum performance but minimum power savings. [Automatic] is suitable for most applications. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, choose [Custom Mode] in "Operating Mode" located under "System Setting" submenu. **Disabled** is the default setting.
CPU P-state Control	• None • Legacy • **Autonomous** • Cooperative	Select the method to control CPU P-states (performance states). [None] disables all P-states and the CPUs run at either their rated frequency or in turbo mode (if turbo is enabled). When [Legacy] is selected, the CPU P-states will be presented to the operating system (OS) and the OS power management (OSPM) will directly control which P-state is selected. With [Autonomous], the P-states are controlled fully by system hardware. No P-state support is required in the OS or VM. [Cooperative] is a combination of Legacy and Autonomous. The P-states are still controlled in hardware but the OS can provide hints to the hardware for P-state limits and the desired setting. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Autonomous** is the default setting.
C1 Enhanced Mode	• **Enable** • Disable	Enabling C1E (C1 enhanced) state can save power by halting CPU cores that are idle. An operating system that supports C1E state must be installed to take advantage of this feature. Changing this setting takes effect after the next reboot. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” and [Legacy]/[Disable] in “C-States” located under “System Setting” submenu. C1E is changeable only when C-state is not **Autonomous**. **Enable** is the default setting.
UPI Link Frequency	• Minimal Power • Balanced • **Max Performance**	Select the desired CPU UPI link frequency. [Maximum Performance] mode maximizes performance. [Balanced] mode offers a balance between performance and power. [Minimal Power] maximizes power savings. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Max Performance** is the default setting.

Table 9. Operating modes details (continued)

UPI Link Disable	• **Enable All Links** • Disable 1 Link	Disabling one of the CPU UPI links can save power. If maximum performance is desired, all UPI links should be left enabled. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Enable All Links** is the default setting.
Turbo Mode	• **Enable** • Disable	Enabling turbo mode can boost the overall CPU performance when all CPU cores are not being fully utilized. A CPU core can run above its rated frequency for a short period of time when it is in turbo mode. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Enable** is the default setting.
Energy Efficient Turbo	• **Enable** • Disable	When energy efficient turbo is enabled, the CPU’s optimal turbo frequency will be tuned dynamically based on CPU utilization. The power/performance bias setting also influences energy efficient turbo. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” and [Enable] in "Turbo Mode" located under “System Setting” submenu. **Enable** is the default setting.
C-States	• Legacy • **Autonomous** • Disable	C-states reduce CPU idle power. When [Legacy] is selected, the operating system initiates the C-state transitions. For E5/E7 CPUs, ACPI C1/C2/C3 map to Intel C1/C3/C6. For 6500/7500 CPUs, ACPI C1/C3 map to Intel C1/C3 (ACPI C2 is not available). Some OS SW may defeat the ACPI mapping (e.g. intel_idle driver). When [Autonomous] is selected, HALT and C1 request get converted to C6 requests in hardware. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Autonomous** is the default setting.

Table 9. Operating modes details (continued)

Power/Performance Bias	• **Platform Controlled** • OS Controlled	Power/Performance bias determines how aggressively the CPU will be power managed and placed into turbo. With [Platform Controlled], the system controls the setting. Selecting [OS Controlled] allows the operating system to control it. Not all OSes support this feature. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Platform Controlled** is the default setting.
Platform Controlled Type	• Maximum Performance • **Efficiency - Favor Performance** • Minimal Power	[Maximum Performance] allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption. [Minimal Power] disables turbo and maximizes the use of power management features. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Efficiency - Favor Performance** is the default setting.
Page Policy	• Adaptive • **Closed**	Adaptive Open Page Policy can improve performance for applications with a highly localized memory access pattern; Closed Page Policy can benefit applications that access memory more randomly. **Closed** is the default setting.
MONITOR/MWAIT	• **Enable** • Disable	MONITOR/MWAIT instructions are used to engage C-states. Some operating systems will re-enable C-states even when they are disabled in setup. To prevent this, disable MONNITOR/MWAIT, choose [Custom Mode] in “Operating Mode” and [Disable] in "C-States" located under “System Setting” submenu. This item can be changed after the steps as below. • 1. Operating Modes -> Custom • 2. C-states -> Disable **Enable** is the default setting.
UPI Power Management	N/A	Select the desired power management level for the CPU UPI interface. L1 saves the most power but has longer latency compared to L0p or Disabled. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu.

Power

Use this menu to configure power scheme options.



Table 10. Power details

Item	Options	Description
Power/Performance Bias	• **Platform Controlled** • OS Controlled	Power/Performance bias determines how aggressively the CPU will be power managed and placed into turbo. With [Platform Controlled], the system controls the setting. Selecting [OS Controlled] allows the operating system to control it. Not all OSes support this feature. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Platform Controlled** is the default setting.
Platform Controlled Type	• Maximum Performance • **Efficiency - Favor Performance** • Efficiency - Favor Power • Minimal Power	[Maximum Performance] allows the most aggressive use of turbo and power management functions are disabled, thereby increasing power consumption. [Minimal Power] disables turbo and maximizes the use of power management features. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Efficiency - Favor Performance** is the default setting.

Table 10. Power details (continued)

Workload Configuration	• **Balanced** • I/O sensitive	I/O sensitive should be used with expansion cards that require high I/O bandwidth when the CPU cores are idle to allow enough frequency for the workload. **Balanced** is the default setting.
ACPI Fixed Power Button	• **Enable** • Disable	Enable/Disable ACPI Fixed Power Button. When setting as disabled, physically pressing the power button on front of the system won't execute the Operating System's Power Button Policy such as shutdown, turn off monitor, etc. Also, when disabled the 'Shut down OS and ..." options under the iMM Server Power Actions feature will be disabled. **Enable** is the default setting.
Zero Output	• **Disable** • Advance Mode	When zero output is enabled and multiple power supplies are installed in the server, some of the PSUs will be automatically placed into a low power state under light load conditions. This helps to save power. **Disable** is the default setting.

Processors

This menu displays and provides options to change the processor settings.



Table 11. Processors details

Item	Options	Description
Processor Details	N/A	Displays summary of the installed processors.
Turbo Mode	• **Enable** • Disable	Enabling turbo mode can boost the overall CPU performance when all CPU cores are not being fully utilized. A CPU core can run above its rated frequency for a short period of time when it is in turbo mode. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Enable** is the default setting. **Note:** If CPU doesn’t support the feature, it won’t show.
CPU P-state Control	• None • Legacy • **Autonomous** • Cooperative	Select to control CPU P-states (performance states). [None] disables all P-states and the CPUs run at either their rated frequency or in turbo mode (if turbo is enabled). When [Legacy] is selected, the CPU P-states will be presented to the operating system (OS) and the OS power management (OSPM) will directly control which P-state is selected. With [Autonomous], the P-states are controlled fully by system hardware. No P-state support is required in the OS or VM. [Cooperative] is a combination of Legacy and Autonomous. The P-states are still controlled in hardware but the OS can provide hints to the hardware for P-state limits and the desired setting. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Autonomous** is the default setting.
C-States	• Legacy • **Autonomous** • Disable	C-states reduce CPU idle power. When [Legacy] is selected, the operating system initiates the C-state transitions. For E5/E7 CPUs, ACPI C1/C2/C3 map to Intel C1/C3/C6. For 6500/7500 CPUs, ACPI C1/C3 map to Intel C1/C3 (ACPI C2 is not available). Some OS SW may defeat the ACPI mapping (e.g. intel_idle driver). When [Autonomous] is selected, HALT and C1 request get converted to C6 requests in hardware. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in "Operating Mode" located under "System Setting" submenu. **Autonomous** is the default setting.

Table 11. Processors details (continued)

C1 Enhanced Mode	• **Enable** • Disable	Enabling C1E (C1 enhanced) state can save power by halting CPU cores that are idle. An operating system that supports C1E state must be installed to take advantage of this feature. Changing this setting takes effect after the next reboot. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” and [Legacy]/ [Disable] in “C-States” located under “System Setting” submenu. **Enable** is the default setting. **Note:** C1E can only be changeable when C-state is not “Autonomous”
Hyper-Threading	• **Enable** • Disable	Enable Hyper Threading (Software Method to Enable/ Disable Logical Processor threads). **Enable** is the default setting. **Notes:** • Changing this setting will require a Power Good reset to take effect. • If CPU doesn’t support the feature, it won’t show.
Execute Disable Bit	• **Enable** • Disable	The execute disable bit allows memory to be marked as executable or non-executable when used with a supporting operating system. This can improve system security by configuring the processor to raise an error to the operating system when code attempts to run in non-executable memory. **Enable** is the default setting.
Trusted Execution Technology	• Enable • **Disable**	Enable Intel Trusted Execution Technology (Intel TXT). **Disable** is the default setting.
Intel Virtualization Technology	• **Enable** • Disable	Enable the Virtualization Technology. **Enable** is the default setting.
Hardware Prefetcher	• **Enable** • Disable	Lightly threaded applications and some benchmarks can benefit from having the hardware prefetcher enabled. **Enable** is the default setting.
Adjacent Cache Prefetch	• **Enable** • Disable	Lightly threaded applications and some benchmarks can benefit from having the adjacent cache line prefetch enabled. **Enable** is the default setting.
DCU Streamer Prefetcher	• **Enable** • Disable	Lightly threaded applications and some benchmarks can benefit from having the DCU streamer prefetcher enabled. **Enable** is the default setting.
DCU IP Prefetcher	• **Enable** • Disable	DCU IP prefetcher is typically best left enabled for most environments. **Enable** is the default setting.
DCA	• **Enable** • Disable	DCA capable I/O devices such as network controllers can place data directly into the CPU cache, which improves response times. **Enable** is the default setting.

Table 11. Processors details (continued)

Energy Efficient Turbo	• **Enable** • Disable	When energy efficient turbo is enabled, the CPU's optimal turbo frequency will be tuned dynamically based on CPU utilization. The power/performance bias setting also influences energy efficient turbo. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in "Operating Mode" and [Enable] in "Turbo Mode" located under "System Setting" submenu. **Enable** is the default setting.
Uncore Frequency Scaling	• **Enable** • Disable	When enabled, the CPU uncore will dynamically change speed based on the workload. All miscellaneous logic inside the CPU package is considered to be the uncore. **Enable** is the default setting.
MONITOR/MWAIT	• **Enable** • Disable	MONITOR/MWAIT instructions are used to engage C-states. Some operating systems will re-enable C-states even when they are disabled in setup. To prevent this, disable MONNITOR/MWAIT. Please choose [Custom Mode] in "Operating Mode" and [Disable] in "C-States" located under "System Setting" submenu. **Enable** is the default setting. This item can be changed after the steps as below. • 1. Operating Modes -> Custom • 2. C-states -> Disable
UPI Link Disable	• **Enable All Links** • Disable 1 Link	Disabling one of the CPU UPI links can save power. If maximum performance is desired, all UPI links should be left enabled. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in "Operating Mode" located under "System Setting" submenu. **Enable All Links** is the default setting.
SNC	• Enable • **Disable**	SNC (sub NUMA cluster) partitions the cores and last level cache into clusters with each cluster bound to a set of memory controllers in the system. SNC improves average latency to the last level cache. **Disable** is the default setting.
Snoop Preference	• **Home Snoop Plus** • Home Snoop	Select the appropriate snoop mode based on the workload. Setting the snoop mode preference does not always guarantee that it will be selected. The mode will be changed if the current hardware configuration does not support the desired mode. Also not that SNC has priority over the snoop mode. **Home Snoop Plus** is the default setting.

Table 11. Processors details (continued)

XPT Prefetcher	• **Enable** • Disable	XPT prefetch is a mechanism that enables a read request that is being sent to the last level cache to speculatively issue a copy of that read to the memory controller prefetching. **Enable** is the default setting.
UPI Prefetcher	• **Enable** • Disable	UPI prefetch is a mechanism to get the memory read started early on DDR bus. The UPI receive path will spawn a memory read to the memory controller prefetcher. **Enable** is the default setting.
Cores in CPU Package	• **All** • 1 • . • . • . • n-1	Select the amount of cores enabled within each CPU Package. **All** is the default setting. n is the maximum number of cores that installed processor support. For example, if the installed processor support 6 cores, it will show All, 1, 2, 3 4, and 5.
UPI Link Frequency	• Minimal Power • Balanced • **Maximum Performance**	Select the desired CPU UPI link frequency. [Maximum Performance] mode maximizes performance. [Balanced] mode offers a balance between performance and power. [Minimal Power] maximizes power savings. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu. **Maximum Performance** is the default setting.
UPI Power Management	N/A	Select the desired power management level for the CPU UPI interface. L1 saves the most power but has longer latency compared to L0p or Disabled. When a preset mode is selected, the low-level settings are not changeable and will be grayed out. If user would like to change the settings, please choose [Custom Mode] in “Operating Mode” located under “System Setting” submenu.
CPU Frequency Limits	N/A	The maximum frequency (turbo, AVX, and non turbo) can be restricted to a frequency that is between the maximum turbo frequency for the CPU installed and 1.2GHz. This can be useful for synchronizing CPU tasks. Note that the max frequency for N+1 cores cannot be higher than N cores. If an illegal frequency is entered, it will automatically be limited to a legal value. If the CPU frequency limits are being controlled through application software, leave this menu item at the default ([Full turbo uplift]),please choose [Custom Mode] in "Operating Mode" and [Enable] in "Turbo Mode" located under "System Setting" submenu.

Recovery and RAS

Use this menu to configure recovery policies and advanced reliability, availability, and serviceability settings.



POST Attempts

Item	Options	Description
Post Attempt Limit	• Disable • 9 • 6 • **3**	Configure the number of attempts to POST before the recovery mechanism is invoked. When the number of consecutive failed POST attempts reaches the limit, the system will reboot with the factory default settings. **3** is the default setting.

Note: You may encounter some message boxes when post attempts. Follow the message for setup.

Advanced RAS

Item	Options	Description
Machine Check Recovery	• **Enable** • Disable	Enable software layers (OS, VMM, DBMS, Application) to assist in system recovery from hardware uncorrectable error. **Enable** is the default setting.
PCI Error Recovery	• Enable • **Disable**	Allow the system to recover from an uncorrectable PCIe fault when enabled. The faulting PCIe device will be disabled for error containment and the OS will be notified to rescan the PCIe buses. **Disable** is the default setting. An uncorrectable PCIe fault will result in an NMI when disabled.
PCIe Endpoint Reset on Fatal Error	• Enable • **Disable**	PCIe Endpoint Reset On Fatal Error. **Disable** is the default setting.

Disk GPT Recovery

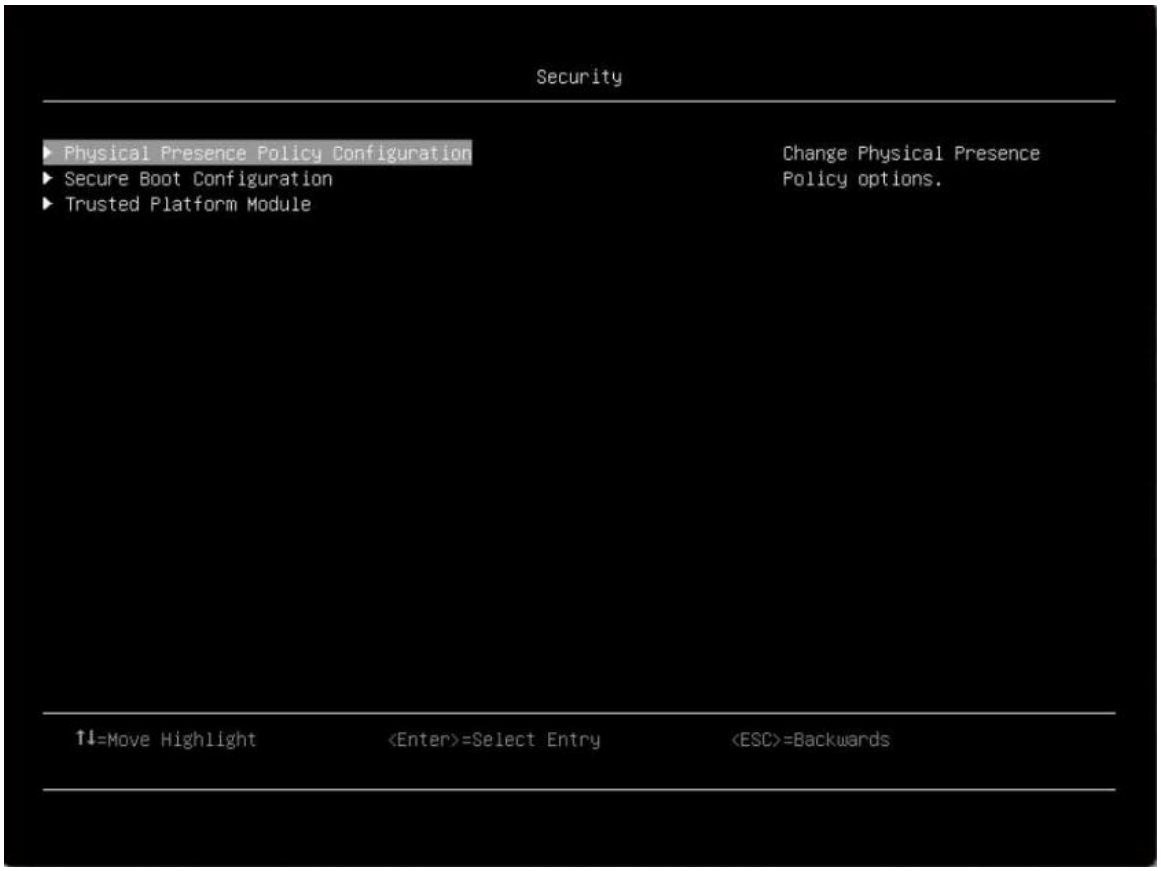
Item	Options	Description
Disk GPT Recovery	• Automatic • Manual • **None**	[Automatic] means that system UEFI will automatically repair the corrupt GUID Partition Table (GPT). [Manual] means that system UEFI will only repair the corrupt GPT based on user input to a message box. [None] means the system UEFI will not repair the corrupted GPT. Recovery result can be retrieved from the system event log. **None** is the default setting.

System Recovery

Item	Options	Description
POST Watchdog Timer	• Enable • **Disable**	Enable/Disable POST Watchdog Timer. **Disable** is the default setting.
POST Watchdog Timer Value	[5]	Enter POST loader Watchdog timer value in minutes from the specified range (5-20).
Reboot System On NMI	• **Enable** • Disable	Enable/Disable reboot of the system during non-maskable interrupt. **Enable** is the default setting.

Security

Use this menu to configure system security settings.



Physical Presence Policy Configuration

Item	Options	Description
Physical Presence Policy	• **Enabled** • Disabled	Enable/Disable "Remote Physical Presence Policy". **Enabled** is the default setting. The option is modifiable when "Physical Presence State" is asserted. Enabled allows Remote Physical Presence to be asserted without the need for Hardware Physical Presence. Once enabled, a time-out value is used to assert the policy for a specified number of minutes. **Note:** If moved to the Disabled state, it will require Hardware Physical Presence to re-enable this policy.
Minutes To Assert	30	Number of minutes (range 1-100) to have Remote Physical Presence asserted. Physical Presence Policy must be Enabled and a value set to have remote physical Presence asserted. NOTE: This is not a count down value.

Physical Presence State	• Hardware Physical Presence Asserted • Remote Physical Presence Asserted • Hardware and Remote Physical Presence are Asserted • **De-asserted**	If Hardware Physical Presence Jumper is Asserted, the only way to de-assert Physical Presence is to change the jumper on the planar. Asserting allows Physical Presence to be set for a duration listed in minutes even if Hardware Physical Presence Jumper is not asserted. Asserting does not require a reboot. Both the Hardware Physical Presence Jumper on the planar and the Remote Physical Presence are Asserted. De-asserting turns off Physical Presence (unless the HW Physical Presence Jumper is asserted). De-asserting does not require a reboot. **De-asserted** is the default setting
Toggle Remote Physical Presence Assert	N/A	Switch the Remote Physical Presence between Assert and De-assert when "Physical Presence Policy" is enabled. The option is NOT modifiable when "Physical Presence Policy" is disabled.

Secure Boot Configuration

Item	Options	Description
Physical Presence	• Asserted • **De-asserted**	Display the current Physical Presence status. Physical Presence is a form of authorization to perform certain security functions. [Asserted] means being authorized. ”Secure Boot Setting” and “Secure Boot Policy” is modifiable when “Physical Presence” is asserted. **De-asserted** is the default setting **Note:** When the setting is De-asserted, the whole page is grayed.
Secure Boot Status	• **Disabled** • Enabled	Display the current secure boot status. **Disabled** is the default setting.
Secure Boot Mode	• Setup Mode • **User Mode**	System will do secure boot authentication when “Secure Boot Mode” is [User Mode] and secure boot is enabled. **User Mode** is the default setting.

Secure Boot Setting	• Enable • **Disable**	Enable/Disable secure boot. This setting is modifiable when “Physical Presence” is asserted and cannot be loaded to default in Setup Utility. **User Mode** is the default setting. **Notes:** • When you attempt to enable secure boot while CSM is enabled, there is a prompt to tell you. • Legacy BIOS will be disabled when secure boot is enabled. • When you fail to change secure boot settings, verify physical presence and retry.
Secure Boot Policy	• **Factory Policy** • Custom Policy • Delete All Keys • Delete PK • Reset All Keys to Default	This setting is modifiable when "Physical Presence" is asserted and cannot be loaded to default in Setup Utility. [Factory Policy]: Factory default keys will be used after reboot. **Factory Policy** is the default setting. [Custom Policy]: Customized keys will be used after reboot. [Delete All Keys]: PK, KEK, DB and DBX will be deleted after reboot. [Delete PK]: PK will be deleted after reboot. "Secure Boot Mode" is [Setup Mode] and "Secure Boot Policy" is [Custom Policy] after PK is deleted. [Reset All Keys to Default]: All the keys will be set to factory defaults and "Secure Boot Policy" is [Factory Policy] after reboot.
View Secure Boot Keys	N/A	View the details of PK(Platform Key) , KEK (Key Exchange Key) , DB (Authorized Signature Database) and DBX (Forbidden Signature Database).
Secure Boot Custom Policy	N/A	Customize PK (Platform Key), KEK (Key Exchange Key), DB (Authorized Signature Database) and DBX (Forbidden Signature Database). User could enter this page when “Secure Boot Policy” is [Custom Policy].

Trusted Platform Module (TPM 1.2)

Item	Options	Description
TPM Version	N/A	Specify the version infromation.
Update to TPM2.0 compliant	N/A	Update to TPM2.0. **Notes:** • When update TPM version to TPM2.0 compliant, do not boot a legacy OS due to security consideration. Change is effective after system reboot and physical presence confirmed. You can only switch TPM firmware 128 times. • Click this button, a pop-up warning message will show up to confirm the action. Update is a significant change. Once completed, all keys and encrypted data will be lost.

Storage

Use this menu to manage storage adapter options. Some systems may use planar devices and can be configured under **Devices and I/O ports**.

Item	Description
Intel(R) Virtual RAID on CPU	This formset allows the user to manage Intel(R) Virtual RAID on CPU.

Note: The device list is based on your system configuration and system setting. The contents in this page are dynamically generated by installed storage vendor's HII utilities.

Date and time

Use this menu to set the local Date and Time of the system.



Table 12. Date and time details

Item	Format	Description
System Date	MM/DD/YYYY	Use the +/- to set the month, day and year (2000 – 2099). The date is saved as it is set.
System Time	HH:MM:SS	Use the +/- to set the hour, minutes, and seconds. Use a 24 hour format. Example: 15:00 for 3pm.

Start options

Use this menu to boot a desired selection from the primary boot sequence from the primary boot sequence as specified under **Boot Manager**.

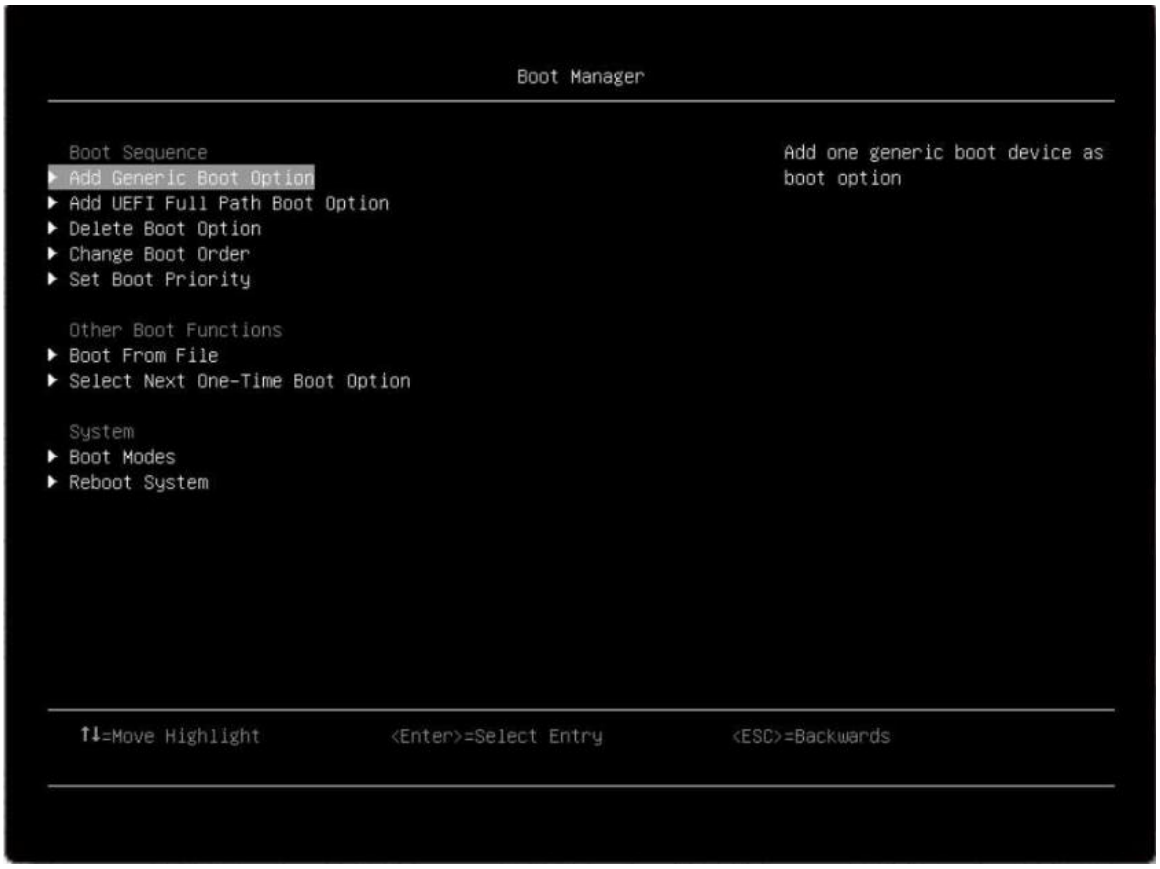


Table 13. Start options details

Item	Operation	Function
CD/DVD Rom		Executable item Select the hexadecimal device address and the server will be boot from this device next time.
Hard Disk		Executable item Select the hexadecimal device address and the server will be boot from this device next time.
Network		Executable item Select the hexadecimal device address and the server will be boot from this device next time.

Boot manager

Use this menu to choose boot order, boot parameters, and boot from a file.



Add Generic Boot Option

Add one generic boot device as boot option:

Item	Options	Description
USB Storage	N/A	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,04000000)

Add UEFI Full Path Boot Option

Add one UEFI application or one removable file systems as boot option.

Item	Options	Description
Boot option File Path	N/A	File path for newly created boot option
Input the Description	N/A	Specify name for the new boot option
Select Device Path Option	Xxxx {xxxx-xxx-xxx…}	Select device path option.
Commit Changes and Exit	N/A	Save changes and exit.

Delete Boot Option

Remove boot option(s) from “Boot Order”.

Item	Options	Description
CD/DVD Rom	• [] • [X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,02000000)
Hard Disk	• [] • [X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,01000000)
Network	• [] • [X]	VenHw(B2AD3248-4F72-4950-A966-CFE5062DB83A,05000000)
Commit Changes and Exit	N/A	Save changes and exit.

Change Boot Order

Modify the ordering of selections within “Boot Order”.

Item	Options	Description
Change the Order	• CD/DVD Rom • Hard Disk • Network	Change the order. It would display the boot options in [Start Options]
Commit Changes and Exit	N/A	Save changes and exit.

Set Boot Priority

Set boot priority of the devices in a device group.

Item	Options	Description
CD/DVD Priority	N/A	Set boot priority in the CD/DVD group if multiple devices exist in the system.
Hard Disk Priority	N/A	Set boot priority in the Hard Disk group if multiple devices exist in the system.
Network Priority	N/A	Set boot priority in the Network group if multiple devices exist in the system.
USB Priority	N/A	Set boot priority in the USB group if multiple devices exist in the system.

Boot From File

Boot the system from a specific file or device.

Select Next One-Time Boot Option

Select the one-time boot option for the next boot.

Item	Options	Description
Boot Option	• CD/DVD Rom • Hard Disk • Network • System Setup • **NONE**	Select the one-time boot option for next boot. **NONE** is the default setting.

Boot Modes

Change between UEFI boot mode and legacy boot mode.

Item	Options	Description
System Boot Mode	• **UEFI Mode** • Legacy Mode	Drivers, option ROMs and OS loaders the “Boot Manager” attempt to boot. [UEFI Mode]: Run UEFI drivers and boot a UEFI OS loader. **UEFI Mode** is the default setting. [Legacy Mode]: Run option ROMs and boot a legacy OS. **Note:** This setting will be forced to [UEFI Mode] when Legacy BIOS is disabled in System Settings->Legacy BIOS->Legacy BIOS.
Infinite Boot Retry	• Enable • **Disable**	Continuously retry the Boot Order. Ensure a bootable device is specified in “Boot Order”. **Disable** is the default setting.

Reboot Systems

Prompt to reboot the system. If Y is pressed, any setup changes will be lost and the system will reboot.

BMC settings

Use this menu to configure the management controller.



Table 14. BMC settings settings

Item	Options	Description
Power Restore Policy	• **Always Off** • Restore • Always On	Determine the mode of operation after loss of power. [Always Off]: System remains off upon power restore. [Restore]: System restores to the state it was before power failed. [Always On]: System turns on upon power restore. Allow a few minutes for the changes to take effect. **Always Off** is the default setting. **Note:** This option is configuration dependent, and this item could not use Setup load default to back to default value.
Ethernet over USB interface	• **Enable** • Disable	[Enable] for using the xClarity Essentials in-band update utility. [Disable] will prevent xClarity Essentials and other applications that are running on the server from requesting the BMC to perform tasks. **Enable** is the default setting.
Network Settings	N/A	Configure the network of the management controller.
Reset Factory Defaults Setting	N/A	Restore all management controller settings to factory defaults, including network configuration and credentials, the management controller will be restarted automatically.
Restart BMC	N/A	Restart the BMC.

Network settings

Item	Options	Description
Network Interface Port	• **Dedicated** • Shared	Select the System Management Network Interface Port. **Dedicated** is the default setting. **Note:** This option is configuration dependent.
Shared NIC on	1. ML2 Card 2. PHY Card 3. Onboard Port 1	Select the shared NIC port. **Note:** This item is only on when network interface port is on Shared, and this option is configuration dependent.
Fail-Over Rule	• **None** • Failover to shared (Optional Card ML2) • Failover to shared (Optional Card PHY) • Failover to shared (Onboard Port)	Setting to control Fail-Over types allowed. **None** is the default setting. **Note:** This item is only on when network interface port is on Shared, and this option is configuration dependent.
Burned-in MAC Address	N/A	
Hostname	N/A	Change the host name. The new name should be within 1 to 63 characters.
DHCP Control	• Static IP • DHCP Enabled • **DHCP with Fallback**	Configure DHCP Control or manually configure a static IP address. Fallback will use static IP address if DHCP fails. Select Static to enter IPV4 address manually. **DHCP with Fallback** is the default setting.
IP Address	**x.x.x.x**	Enter IP address in dotted-decimal notation. When entering an invalid IP address: • ERROR • Invalid Input Range • Ok
Subnet Mask	**x.x.x.x**	Enter Subnet Mask in dotted-decimal notation. When entering an invalid IP address: • ERROR • Invalid Input Range • Ok
Default Gateway	**x.x.x.x**	Enter Default Gateway in dotted-decimal notation. When entering an invalid IP address: • ERROR • Invalid Input Range • Ok
IP6	• **Enable** • Disable	Enable/Disable IPv6 support on management port. **Enable** is the default setting.

Local Link Address	N/A	
VLAN Support	• Enable • **Disable**	Enable VLAN Support to specify the 802.1q VLAN ID on the management port network device. **Disable** is the default setting.
Advanced Setting for BMC Ethernet	N/A	Advanced Setting for BMC Ethernet.

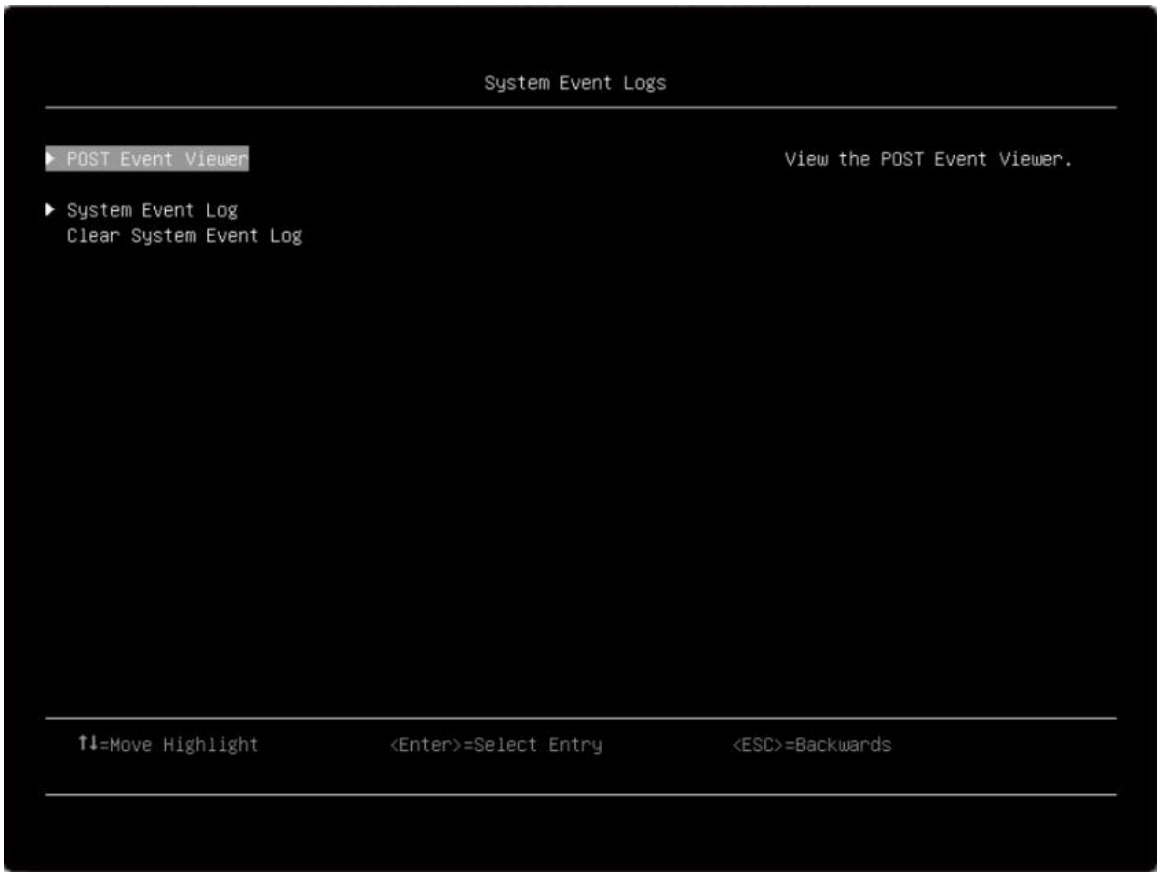
Advanced Settings for BMC Ethernet

Item	Options	Description
Autonegotiation	• No • **Yes**	Choose whether the Data rate and Duplex network settings are configurable or not. **Yes** is the default setting.
Data rate	Autonegotiation is 'Yes': Auto Autonegotiation is 'No': 100 Mb (Ethernet) 10 Mb (Ethernet)	Amount of data to be transferred per second over LAN connection.
Duplex	Autonegotiation is 'Yes': Auto Autonegotiation is 'No': Half Full	Type of communication channel used in your network. [Full]: Allow data to be transferred in both directions at once. [Half]: Allow data to be transferred in either one direction or the other, but not both at the same time.
Maximum Transmission Unit	**1500**	Specify the maximum size of a packet (in bytes) for the network interface. The valid range is 68 – 1500. **1500** is the default setting.

Note: Changes will be valid after saving network settings in previous page.

System event logs

Use this menu to clear or view the System Event Log.



Post Event Viewer

View the Post Event Viewer.

System Event Log

View the System Event Log.

Item	Options	Description
Total SEL entries	N/A	Total number of System Event Logs retrieved from the BMC. This does not include any associated extended logs.

User security

Use this menu to set or change Power-On and Administrator passwords.



Table 15. User security details

Item	Options	Description
Password Rule and Policy	**N/A**	Set rule and policy.

Table 15. User security details (continued)

Set Power-On Password	N/A	Set the power-On password. The password can only contain the following characters (no white-space characters allowed): A-Z, a-z, 0-9, ~`!@#$ %^&*()-+={}[]|:;"'<>,?/._ Must contain at least one letter Must contain at least one number Must contain at least 2 of the following combinations: • At least one upper-case letter • At least one lower-case letter • At least one special character No more than 2 consecutive occurrences of the same character Must be at least 8 characters if doesn't select other value in "Minimum password length" option. **Notes:** Click the button, pop-up message box will show up. • Please type in your password • Please type in your new password • Please confirm your new password • Power-On Password has been set successfully • The password failed to meet the "Minimum password reuse cycle" requirements. • Please enter enough characters Press Enter to Continue • The password can't be changed because the "Minimum password change interval" time is not exceeded. • The password does not meet the minimum password complexity requirements. Please check the help for "Set Power-On Password" or "Set Administrator Password" settings. • Passwords are not the same Press Enter to Continue • Incorrect Password Press Enter to Continue • Passwords operation have unknown problem. Press Enter to Continue When IPMI command has no response, then pop out this message.

Table 15. User security details (continued)

Clear Power-On Password	N/A	Clear the Power-On password. **Note:** Click the button, pop-up message box will show up. • Power-On Password is not set Press Enter to Continue • An existing Power-On Password will be deleted. <ENTER> Continue. <ESC> Return to Setup Utility • Power-On Password has been cleared successfully Press Enter to Continue
Set Administrator Password	N/A	Set the Administrator password. The password can only contain the following characters (no white-space characters allowed): A-Z, a-z, 0-9, ~`!@#$ %^&*()-+={}[]|:;"'<>,?/._ Must contain at least one letter Must contain at least one number Must contain at least 2 of the following combinations: • At least one upper-case letter • At least one lower-case letter • At least one special character No more than 2 consecutive occurrences of the same character Must be at least 8 characters if doesn't select other value in "Minimum password length" option. **Notes:** Clicking the button, pop-up message box will show up. • Please type in your password • Please type in your new password • Please confirm your new password • Administrative Password has been set successfully • The password failed to meet the "Minimum password reuse cycle" requirements. • The password can't be changed because the "Minimum password change interval" time is not exceeded. • The password does not meet the minimum password complexity requirements. Please check the help for "Set Power-On Password" or "Set Administrator Password" settings. • Please enter enough characters Press Enter to Continue

Table 15. User security details (continued)

		• Passwords are not the same Press Enter to Continue • Incorrect Password Press Enter to Continue • Passwords operation have unknown problem. Press Enter to Continue When IPMI command has no response then pop out this message.
Clear Administrator Password	N/A	Clear the Administrator password. Clicking the button, pop-up message box will show up. • An existing Administrative Password will be deleted <ENTER> Continue. <ESC> Return to Setup Utility • Administrative Password has been cleared successfully Press Enter to Continue • Administrative Password is not set Press Enter to Continue

Password Rule and Policy

Item	Options	Function
Minimum password length	8~20	Input a value from 8 to 20. The minimum number of characters that can be used to specify a valid password.
Password expiration period	0~365	Input a value from 0 to 365. The number of days a password may be used before it must be changed. If set to 0 the passwords never expire.
Password expiration warning period	0~365	Input a value from 0 to 365. The number of days before receiving a warning about the expiration of the password. If set to 0 the passwords never warned.
Minimum password change interval	0~240	Input a value from 0 to 240. The number of hours that must elapse before changing a password. The value specified for this setting cannot exceed the value specified for the “Password expiration period”. If set to 0 the passwords may be changed immediately.
Minimum password reuse cycle	0~10	Input a value from 0 to 10. The minimum number of times a unique password must be set before reusing a previous password. If set to 0 the passwords may be reused immediately.

Maximum number of login failures	0~100	Input a value from 0 to 100. The number of login attempts that can be made with an incorrect password before the user account is locked out. The account is locked out for the time specified in “Lockout period after maximum login failures”. If set to 0 accounts are never locked. The failed login counter is reset to zero after a successful login.
Lockout period after maximum login failures	0~2880	Input a value from 0 to 2880. The number of minutes that must pass before a locked out user can attempt to login. Entering a valid password does not unlock the account during the lockout period. If set to 0 the accounts will not be locked out even if the “Maximum number of login failures” is exceeded.

Appendix A. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2020

Trademarks

LENOVO and LENOVO logo are trademarks of Lenovo.

All other trademarks are the property of their respective owners. © 2020 Lenovo

VMware Compatibility Guide

Back to Search Results Print

Model Details

Model :	ThinkSystem SR530	Notes:
Partner :	Lenovo	For further details about BIOS, server product configurations and best practices, please contact the server vendor
CPU Series:	Intel Xeon Gold 6200/5200 (Cascade-Lake-SP/Refresh) Series	
System Type:	Rackmount	
Number of Sockets:	2	
Max Cores per Socket:	28	rss feed

Model Release Details

VMware Product Name : ESXi 7.0 U2

BIOS	Feature Category	Features	Feature Value	Hardware Health
Lenovo -[TEE168I-2.90]- UEFI Mode (Boot Mode:UEFI)	Server	Fault Tolerant(FT) UEFI Secure Boot		
Lenovo -[TEE164L-2.80]- UEFI Mode (Boot Mode:UEFI)	Server	Fault Tolerant(FT) UEFI Secure Boot		
Lenovo -[TEE160M-2.70]- UEFI Mode (Boot Mode:UEFI)	Server	Fault Tolerant(FT) UEFI Secure Boot		
Lenovo -[TEE156K-2.60]- UEFI Mode (Boot Mode:UEFI)	Server	Fault Tolerant(FT) UEFI Secure Boot		
Lenovo -[TEE152L-2.51]- UEFI Mode (Boot Mode:UEFI)	Server	Fault Tolerant(FT)		
Lenovo -[TEE152L-2.51]- UEFI Mode (Boot Mode:UEFI)	Server	Fault Tolerant(FT) UEFI Secure Boot		
Lenovo -[TEE152L-2.51]- UEFI Mode (Boot Mode:UEFI)	Server	Trusted Platform Module (TPM) UEFI Secure Boot	TPM 1.2 with TXT	
Lenovo -[TEE152L-2.51]- UEFI Mode (Boot Mode:UEFI)	Server	Trusted Platform Module (TPM) UEFI Secure Boot	TPM 2.0 with TXT	
Lenovo -[TEE148M-2.41]- UEFI Mode (Boot Mode:UEFI)	Server	Fault Tolerant(FT) UEFI Secure Boot		
Lenovo -[TEE148L-2.40]- UEFI Mode (Boot Mode:UEFI)	Server	Fault Tolerant(FT) UEFI Secure Boot		

Back to Search Results Print

CONTACT US

vmware
Contact Sales
Get Support
About VMware
Careers
Thought Leadership
© 2021 VMware, Inc
Terms of Use
Your California Privacy Rights
Privacy
Accessibility
Site Map
Trademarks
Glossary
Help
Feedback

Configurações de cookies

Menu

CONTACT US

Configurações de cookies

Lenovo

XClarity Controller User's Guide



Note: Before using this information, read the general information in Appendix B “Notices” on page 205.

Fifteenth Edition (August 2020)

© Copyright Lenovo 2017, 2020.
LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Chapter 1. Introduction 1

XClarity Controller Standard, Advanced, and Enterprise Level features 2
- XClarity Controller Standard Level features . . . 2
- XClarity Controller Advanced Level features . . . 5
- XClarity Controller Enterprise Level features . . . 5
- Upgrading XClarity Controller 6

Web browser and operating-system requirements 6

Multiple language support 7

MIBs Introduction 7

Notices used in this document 8

Chapter 2. Opening and Using the XClarity Controller Web Interface 9

Accessing the XClarity Controller web interface . . . 9
- Setting up the XClarity Controller network connection through the XClarity Provisioning Manager 10
- Logging in to the XClarity Controller 12

Description of XClarity Controller functions on web interface. 13

Chapter 3. Configuring the XClarity Controller 17

Configuring user accounts/LDAP 17
- User authentication method 17
- Creating a new user account 17
- Deleting a user account 20
- Using hashed passwords for authentication . . 20
- Configuring global login settings 22
- Configuring LDAP 24

Configuring network protocols 29
- Configuring the Ethernet settings 29
- Configuring DNS 31
- Configuring DDNS 31
- Configuring Ethernet over USB 32
- Configuring SNMPv3 32
- Enabling or Disabling IPMI Network Access . . 33
- Configuring Network Settings with IPMI commands 33
- Service Enablement and Port Assignment . . . 33
- Configuring Access Restriction 34
- Configuring Front Panel USB Port to Management 35

Configuring security settings. 36
- SSL overview 36
- SSL certificate handling 37
- SSL certificate management 37
- Configuring the Secure Shell server 38
- IPMI over Keyboard Controller Style (KCS) Access 38
- Prevent System Firmware Down-Level 38
- Assert Physical Presence 39
- Configuring the Security Key Lifecycle Manager (SKLM) 39
- Extended Audit Log 43

Configuring Call Home 43

Backing up and Restoring the BMC configuration 45

Backing up the BMC configuration 45

Restoring the BMC configuration 46

Resetting the BMC to Factory Default 46

Restarting the XClarity Controller 46

Chapter 4. Monitoring the server status. 47

Viewing the Health Summary/Active System Events 47

Viewing the System Information 48

Viewing the System Utilization 50

Viewing Event Logs 50

Viewing Audit Logs 51

Viewing the Maintenance History 51

Configuring Alert Recipients 52

Capturing the latest OS failure screen data 54

Chapter 5. Configuring the Server . . 55

Viewing the adapter information and configuration settings 55

Configuring system boot mode and order. 55

Configuring one-time boot 56

Managing the server power 56
- Configuring the power redundancy 57
- Configuring the power capping policy 57
- Configuring the power restore policy 58
- Power actions. 58
- Managing and monitoring power consumption with IPMI commands 59

Remote Console Functionality 61
- Enabling the remote console functionality . . . 62
- Remote power control 62
- Remote console capture screen 63
- Remote console keyboard support 63
- Remote console mouse support 63
- Screen Video Record/Replay 64

© Copyright Lenovo 2017, 2020

Remote console screen modes 64
Media mount methods 65
Remote disk using Java client 69
Media mount error issues 73
Exiting the remote console session 75
Downloading service data 75
Server Properties 75
Setting Location and Contact 75
Setting server timeouts 76
Trespass message 76
Setting the XClarity Controller date and time . . . 77

Chapter 6. Configuring the Storage 79
RAID Detail 79
RAID Setup 79
Viewing and configuring the virtual drives . . . 79
Viewing and configuring the storage inventory 80

Chapter 7. Updating Server Firmware 83
Overview 83
System, Adapter and PSU Firmware Update . . . 83
Update From Remote Repository 84

Chapter 8. License Management . . . 85
Installing an activation key. 85
Removing an activation key 86
Exporting an activation key 86

Chapter 9. Lenovo XClarity Controller Redfish REST API 87

Chapter 10. Command-line interface 89
Accessing the command-line interface 89
Logging in to the command-line session 89
Configuring serial-to-SSH redirection 89
Command syntax 90
Features and limitations 90
Alphabetical command listing 91
Utility commands 93
exit command. 93
help command 93
history command 93
Monitor commands 94
clearlog command 94
fans command 95
ffdc command 95
hreport command 96
mhlog command 97
led command 97
readlog command 99
syshealth command 100
temps command 101
volts command 101
vpd command 102
Server power and restart control commands . . . 103
power command 103
reset command 105
fuelg command 105
pxeboot command 106
Serial redirect command 107
console command 107
Configuration commands 107
accseccfg command 107
alertcfg command 109
asu command. 109
backup command 112
dhcpinfo command 113
dns command 114
encaps command 116
ethtousb command 116
firewall command 117
gprofile command 118
hashpw command 119
ifconfig command 120
keycfg command 122
ldap command 124
ntp command 125
portcfg command 126
portcontrol command. 127
ports command 128
rdmount command. 129
restore command 130
restoredefaults command 131
roles command 131
seccfg command 133
set command 133
smtp command 133
snmp command 134
snmpalerts command 136
srcfg command 137
sshcfg command 138
ssl command 139
sslcfg command. 140
storekeycfg command 143
syncrep command 144
thermal command 145
timeouts command 146

tls command 146
trespass command. 147
uefipw command 148
usbeth command 148
usbfp command 148
users command 149
IMM control commands 152
alertentries command 153
batch command 155
clearcfg command 156
clock command 156
identify command 156
info command 157
spreset command 158
Service advisor commands 158
chconfig command 158
chmanual command 160
chlog command 160
Agent-less commands 161
storage command 161
adapter command 170
mvstor command 172
Support commands 173
dbgshimm command 173

Chapter 11. IPMI interface 175
Managing the XClarity Controller with IPMI 175
Using IPMItool 175
IPMI Commands with OEM Parameters 176
Get / Set LAN Configuration Parameters . . . 176
OEM IPMI Commands 187

Chapter 12. Edge servers 197
System Lockdown Mode 197
SED Authentication Key (AK) Manager 198
Edge Networking 198

Appendix A. Getting help and technical assistance 201
Before you call 201
Collecting service data 202
Contacting Support 203

Appendix B. Notices. 205
Trademarks 206
Important notes. 206
Particulate contamination 206
Telecommunication regulatory statement. 207
Electronic emission notices 207
Taiwan BSMI RoHS declaration. 208
Taiwan import and export contact information . . . 208

Index 211

© Copyright Lenovo 2017, 2020

Chapter 1. Introduction

The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers.

It is the follow-on to the Integrated Management Module II (IMM2) service processor that consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities into a single chip on the server system board. It provides features such as the following:

- Choice of a dedicated or shared Ethernet connection for systems management
- Support for HTML5
- Support for access via XClarity Mobile
- XClarity Provisioning Manager
- Remote configuration using XClarity Essentials or XClarity Controller CLI.
- Capability for applications and tools to access the XClarity Controller either locally or remotely
- Enhanced remote-presence capabilities.
- REST API (Redfish schema) support for additional web-related services and software applications.

  Note: The XClarity Controller currently supports Redfish Scalable Platforms Management API Specification 1.0.2 and schema 2016.2

Notes:

- In the XClarity Controller web interface, BMC is used in referring to the XCC.
- A dedicated systems-management network port may not be available on some ThinkSystem servers; for these servers access to the XClarity Controller is only available through a network port that is shared with the server operating system.
- For Flex servers, the Chassis Management Module (CMM) is the primary management module for systems-management functions. Access to the XClarity Controller is available through the network port on the CMM.

This document explains how to use the functions of the XClarity Controller in a ThinkSystem server. The XClarity Controller works with the XClarity Provisioning Manager and UEFI to provide systems-management capability for ThinkSystem servers.

To check for firmware updates, complete the following steps.

Note: The first time you access the Support Portal, you must choose the product category, product family, and model numbers for your server. The next time you access the Support Portal, the products you selected initially are preloaded by the website, and only the links for your products are displayed. To change or add to your product list, click the **Manage my product lists** link. Changes are made periodically to the website. Procedures for locating firmware and documentation might vary slightly from what is described in this document.

1. Go to http://datacentersupport.lenovo.com.
2. Under **Support**, select **Data Center**.
3. When the content is loaded, select **Servers**.
4. Under **Select Series**, first select the particular server hardware series, then under **Select SubSeries**, select the particular server product subseries, and finally, under **Select Machine Type** select the particular machine type.

© Copyright Lenovo 2017, 2020

XClarity Controller Standard, Advanced, and Enterprise Level features

With the XClarity Controller, Standard, Advanced, and Enterprise levels of XClarity Controller functionality are offered. See the documentation for your server for more information about the level of XClarity Controller installed in your server. All levels provide the following:

- Around-the-clock remote access and management of your server
- Remote management independent of the status of the managed server
- Remote control of hardware and operating systems

Note: Some features might not apply to Flex system servers.

The following is a list of XClarity Controller standard level features:

XClarity Controller Standard Level features

The following is a list of XClarity Controller Standard Level features:

Industry Standard Management Interfaces

- IPMI 2.0 Interface
- Redfish
- CIM-XML
- DCMI 1.5
- SNMPv3
- SNMPv1 (Traps Only) requires minimum v2.10 or v2.12 XCC Firmware updates depending on server type. See XCC Firmware update Change file for details.

Other Management Interfaces

- Web
- Legacy CLI
- Front Panel USB - virtual operator panel via mobile device

Power / Reset Control

- Power On
- Hard/Soft Shutdown
- Scheduled Power Control
- System Reset
- Boot Order Control

Event Logs

- IPMI SEL
- Human Readable Log
- Audit Log

Environmental Monitoring

- Agent Free Monitoring
- Sensor Monitoring

- Fan Control
- LED Control
- Chipset Errors (Caterr, IERR, etc...)
- System Health Indication
- OOB Performance Monitoring for I/O adapters
- Inventory Display and Export

RAS

- Virtual NMI
- Automatic Firmware Recovery
- Automated promotion of backup firmware
- POST Watchdog
- OS Loader Watchdog
- Blue Screen Capture (OS Failure)
- Embedded Diagnostic Tools

Network Configuration

- IPv4
- IPv6
- IP Address, Subnet Mask, Gateway
- IP Address Assignment Modes
- Host name
- Programmable MAC address
- Dual MAC Selection (if supported by server hardware)
- Network Port Reassignments
- VLAN Tagging

Network Protocols

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SNMPv1 (Traps only)
- SSL
- SSH
- SMTP
- LDAP client
- NTP
- SLP
- SSDP

Alerts

- PET Traps
- CIM Indication
- SNMP TRAPs
- E-mail
- Redfish events

Serial Redirection

- IPMI SOL
- Serial port configuration

Security

- XClarity Controller Core Root of Trust for Measurement (CRTM)
- Digitally signed firmware updates
- Role Based Access Control (RBAC)
- Local User Accounts
- LDAP/AD User Accounts
- Secure Rollback of Firmware
- Chassis intrusion detection (only available on some server models)
- XCC remote assertion of UEFI TPM Physical Presence
- Audit logging of configuration changes and server actions
- Public-key (PK) Authentication
- System Retire/Repurpose

Remote Presence

- Remote Disk on Card (RDOC): Virtual Media mounting of remote ISO/IMG files via CIFS, NFS, HTTP, HTTPS, FTP, SFTP, and LOCAL

Power Management

- Real time Power Meter

License Management

- Activation Key Validation and Repository

Deployment & Configuration

- Remote Configuration
- Deployment & Configuration Tools and Driver Packs using the embedded XClarity Provisioning Manager
- Configuration Backup and Restore

Firmware Updates

- Agent Free Update
- Remote Update

XClarity Controller Advanced Level features

The following is a list of XClarity Controller Advanced Level features:

All of the XClarity Controller Standard Level features plus:

Alerts

- Syslog

Remote Presence

- Remote KVM

Serial Redirection

- Serial Redirection via SSH

Security

- Security Key Lifecycle Manager (SKLM)
- IP address blocking

Power Management

- Real time Power Graphics
- Historical Power Counters
- Temperature Graphics

Deployment & Configuration

- Remote OS Deployment using the embedded XClarity Provisioning Manager with the XClarity Controller Remote KVM feature

XClarity Controller Enterprise Level features

The following is a list of XClarity Controller Enterprise Level features:

All of the XClarity Controller Standard and Advanced Level features plus:

RAS

- Boot Capture

Remote Presence

- Quality/Bandwidth Control
- Virtual Console Collaboration (six users)
- Virtual Console Chat
- Virtual Media
  - Mounting of remote ISO/IMG files via remote console
  - Mounting file from Network: - Mount an ISO or IMG image file from a file server (HTTPS, CIFS, NFS) to the host as a DVD or USB drive

Power Management

- Power Capping

- OOB Performance Monitoring - System Performance metrics

Deployment & Configuration

- Remote Deployment using Lenovo XClarity Administrator. When using the Lenovo XClarity Administrator for operating system deployment, see http://sysmgt.lenovofiles.com/help/index.jsp?topic=%2Fcom.lenovo.lxca.doc%2Fsupported_operating_system_images.html for details on the supported operating systems.

Upgrading XClarity Controller

If your server came with the Standard or Advanced level of the XClarity Controller firmware functionality, you might be able to upgrade the XClarity Controller functionality in your server. For more information about available upgrade levels and how to order, see Chapter 8 “License Management” on page 85.

Web browser and operating-system requirements

Use the information in this topic to view the list of supported browsers, cipher suites and operating systems for your server.

The XClarity Controller web interface requires one of the following web browsers:

- Chrome 48.0 or above (55.0 or above for remote console)
- Firefox ESR 38.6.0 or above
- Microsoft Internet Explorer 11 (above 11.0.9600.16384 for remote console)
- Microsoft Edge
- Safari 9.0.2 or above (iOS 7 or later and OS X)

Note: Support for the remote console feature is not available through the browser on mobile device operating systems.

The browsers listed above match those currently supported by the XClarity Controller firmware. The XClarity Controller firmware may be enhanced periodically to include support for other browsers.

Depending upon the version of the firmware in the XClarity Controller, web browser support can vary from the browsers listed in this section. To see the list of supported browsers for the firmware that is currently on the XClarity Controller, click the **Supported Browsers** menu list from the XClarity Controller login page.

For increased security, only high strength ciphers are now supported when using HTTPS. When using HTTPS, the combination of your client operating system and browser must support one of the following cipher suites:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Your internet browser's cache stores information about web pages that you visit so that they will load more quickly in the future. After a flash update of the XClarity Controller firmware, your browser may continue to use information from its cache instead of retrieving it from the XClarity Controller. After updating the XClarity Controller firmware, it is recommended that you clear the browser cache to ensure that web pages served by the XClarity Controller are displayed correctly.

Multiple language support

Use the information in this topic to view the list of languages supported by the XClarity Controller.

By default, the chosen language for the XClarity Controller web interface is English. The interface is capable of displaying multiple languages. These include the following:

- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazil)
- Russian
- Simplified Chinese
- Spanish (international)
- Traditional Chinese

To choose the language of your preference, click the arrow beside the currently selected language. A drop-down menu will appear to let you choose your preferred language.

Text strings that are generated by the XClarity Controller firmware are displayed in the language dictated by the browser. If the browser specifies a language other than one of the translated languages listed above, the text is displayed in English. In addition, any text string that is displayed by the XClarity Controller firmware, but is not generated by the XClarity Controller (for example messages generated by UEFI, PCIe adapters, etc…) are displayed in English.

The input of language-specific text other than English, such as the *Trespass message* is currently not supported. Only text typed in English is supported.

MIBs Introduction

Use the information in this topic to access Management Information Base.

The SNMP MIBs can be downloaded from the https://support.lenovo.com/ (Search by machine type on the portal). It includes the following four MIBs.

- The **SMI MIB** describes the Structure of Management Information for the Lenovo Data Center Group.
- The **Product MIB** describes the object identifier for Lenovo Products.
- The **XCC MIB** provides the inventory and monitoring information for Lenovo XClarity Controller.
- The **XCC Alert MIB** defines traps for alert conditions detected by Lenovo XClarity Controller.

Note: The import order for the four MIBs is **SMI MIB** → **Product MIB** → **XCC MIB** → **XCC Alert MIB**.

Notices used in this document

Use this information to understand the notices that are used in this document.

The following notices are used in the documentation:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate potential damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.

Chapter 2. Opening and Using the XClarity Controller Web Interface

This topic describes the login procedures and the actions that you can perform from the XClarity Controller web interface.

The XClarity Controller combines service processor functions, a video controller, and remote presence function in a single chip. To access the XClarity Controller remotely by using the XClarity Controller web interface, you must first log in. This chapter describes the login procedures and the actions that you can perform from the XClarity Controller web interface.

Accessing the XClarity Controller web interface

The information in this topic explains how to access the XClarity Controller web interface.

The XClarity Controller supports static and Dynamic Host Configuration Protocol (DHCP) IPv4 addressing. The default static IPv4 address assigned to the XClarity Controller is 192.168.70.125. The XClarity Controller is initially configured to attempt to obtain an address from a DHCP server, and if it cannot, it uses the static IPv4 address.

The XClarity Controller also supports IPv6, but it does not have a fixed static IPv6 IP address by default. For initial access to the XClarity Controller in an IPv6 environment, you can either use the IPv4 IP address or the IPv6 link-local address. The XClarity Controller generates a unique link-local IPv6 address, using the IEEE 802 MAC address by inserting two octets, with hexadecimal values of 0xFF and 0xFE in the middle of the 48-bit MAC as described in RFC4291 and flipping the 2nd bit from the right in the first octet of the MAC address. For example if the MAC address is 08-94-ef-2f-28-af, the link-local address would be as follows:
`fe80::0a94:efff:fe2f:28af`

When you access the XClarity Controller, the following IPv6 conditions are set as default:

- Automatic IPv6 address configuration is enabled.
- IPv6 static IP address configuration is disabled.
- DHCPv6 is enabled.
- Stateless auto-configuration is enabled.

The XClarity Controller provides the choice of using a *dedicated* systems-management network connection (if applicable) or one that is *shared* with the server. The default connection for rack-mounted and tower servers is to use the *dedicated* systems-management network connector.

The dedicated systems-management network connection on most servers is provided using a separate 1Gbit network interface controller. However, on some systems the dedicated systems-management network connection may be provided using the Network Controller Sideband Interface (NCSI) to one of the network ports of a multi-port network interface controller. In this case, the dedicated systems-management network connection is limited to the 10/100 speed of the sideband interface. For information and any limitations on the implementation of the management port on your system, see your system documentation.

Note: A *dedicated* systems-management network port might not be available on your server. If your hardware does not have a *dedicated* network port, the *shared* setting is the only XClarity Controller setting available.

© Copyright Lenovo 2017, 2020

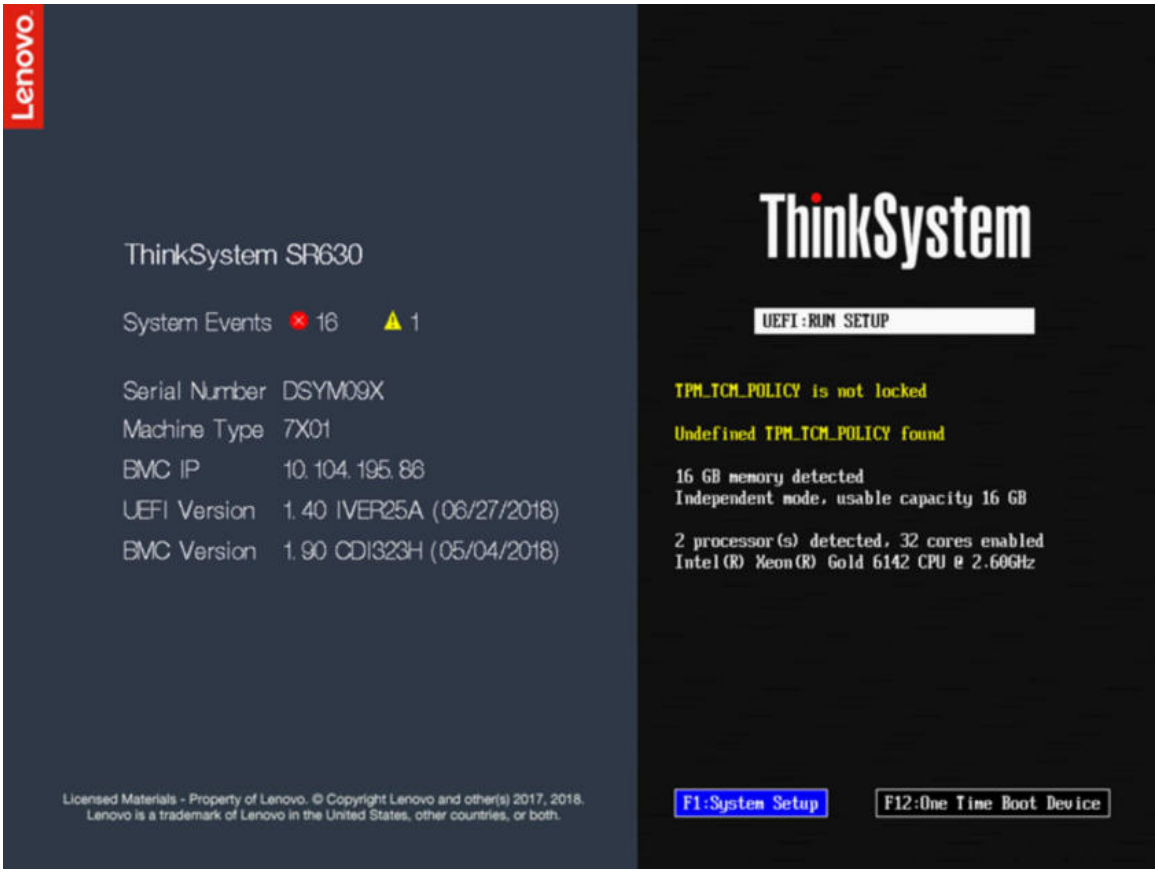
Setting up the XClarity Controller network connection through the XClarity Provisioning Manager

Use the information in this topic to set up an XClarity Controller network connection through the XClarity Provisioning Manager.

After you start the server, you can use the XClarity Provisioning Manager to configure the XClarity Controller network connection. The server with the XClarity Controller must be connected to a DHCP server, or the server network must be configured to use the XClarity Controller static IP address. To set up the XClarity Controller network connection through the Setup utility, complete the following steps:

Step 1. Turn on the server. The ThinkSystem welcome screen is displayed.

Note: It may take up to 40 seconds after the server is connected to AC power for the power-control button to become active.



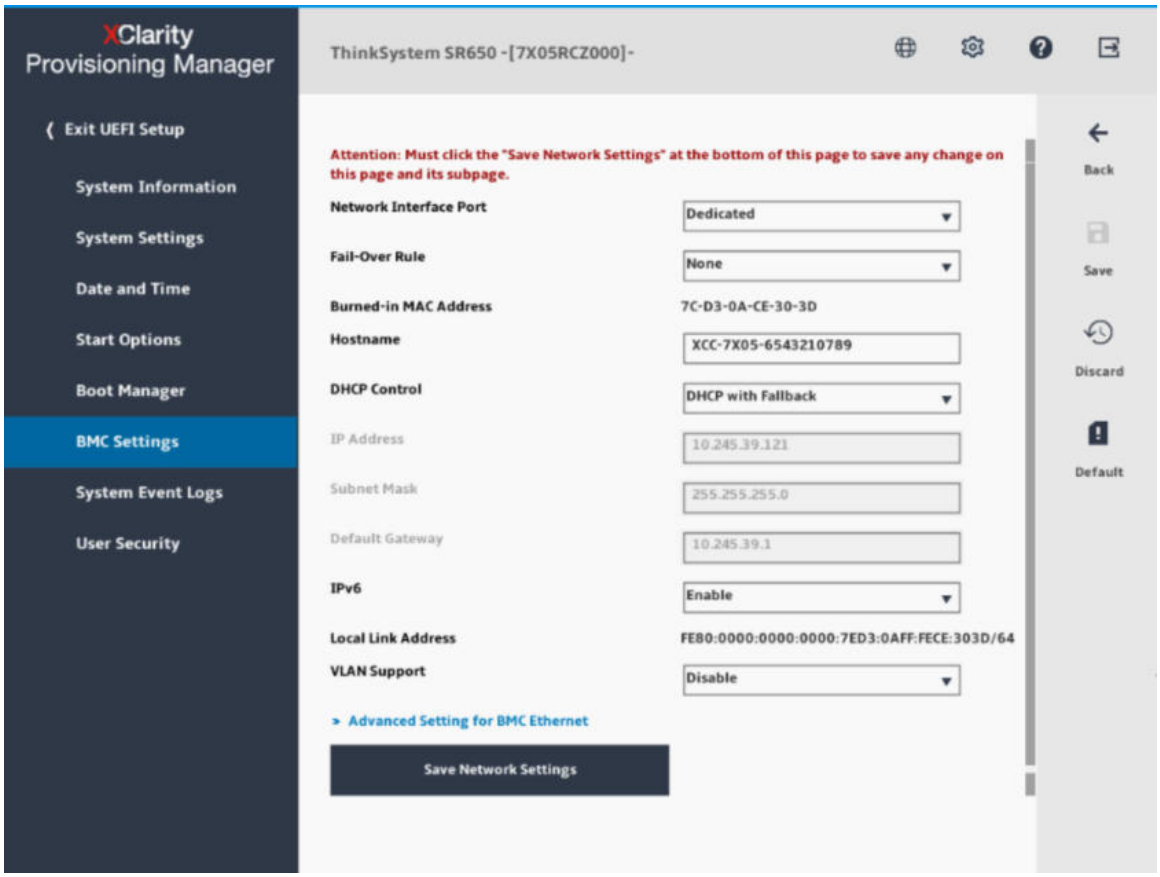
Step 2. When the prompt `<F1> System Setup` is displayed, press F1. If you have set both a power-on password and an administrator password, you must type the administrator password to access the XClarity Provisioning Manager.

Step 3. From the XClarity Provisioning Manager main menu, select **UEFI Setup**.

Step 4. On the next screen, select **BMC Settings**; then, click **Network Settings**.

Step 5. There are three XClarity Controller network connection choices in the **DHCP Control** field:

- Static IP
- DHCP Enabled
- DHCP with Fallback



Step 6. Select one of the network connection choices.

Step 7. If you choose to use a static IP address, you must specify the IP address, the subnet mask, and the default gateway.

Step 8. You can also use the Lenovo XClarity Controller Manager to select a dedicated network connection (if your server has a dedicated network port) or a shared XClarity Controller network connection.

Notes:

- A dedicated systems-management network port might not be available on your server. If your hardware does not have a dedicated network port, the *shared* setting is the only XClarity Controller setting available. On the **Network Configuration** screen, select **Dedicated** (if applicable) or **Shared** in the **Network Interface Port** field.
- To find the locations of the Ethernet connectors on your server that are used by the XClarity Controller, see the documentation that came with your server.

Step 9. Click **Save**.

Step 10. Exit from the XClarity Provisioning Manager.

Notes:

- You must wait approximately 1 minute for changes to take effect before the server firmware is functional again.
- You can also configure the XClarity Controller network connection through the XClarity Controller web interface or command-line interface (CLI). In the XClarity Controller web interface, network connections can be configured by clicking **BMC Configuration** from the left navigation panel , and then selecting **Network**. In the XClarity Controller CLI, network connections are configured using several commands that depend on the configuration of your installation.

Logging in to the XClarity Controller

Use the information in this topic to access the XClarity Controller through the XClarity Controller web interface.

Important: The XClarity Controller is set initially with a user name of `USERID` and password of `PASSWORD` (with a zero, not the letter O). This default user setting has Supervisor access. Change this user name and password during your initial configuration for enhanced security. After making the change, you are unable to set `PASSWORD` as the login password again.

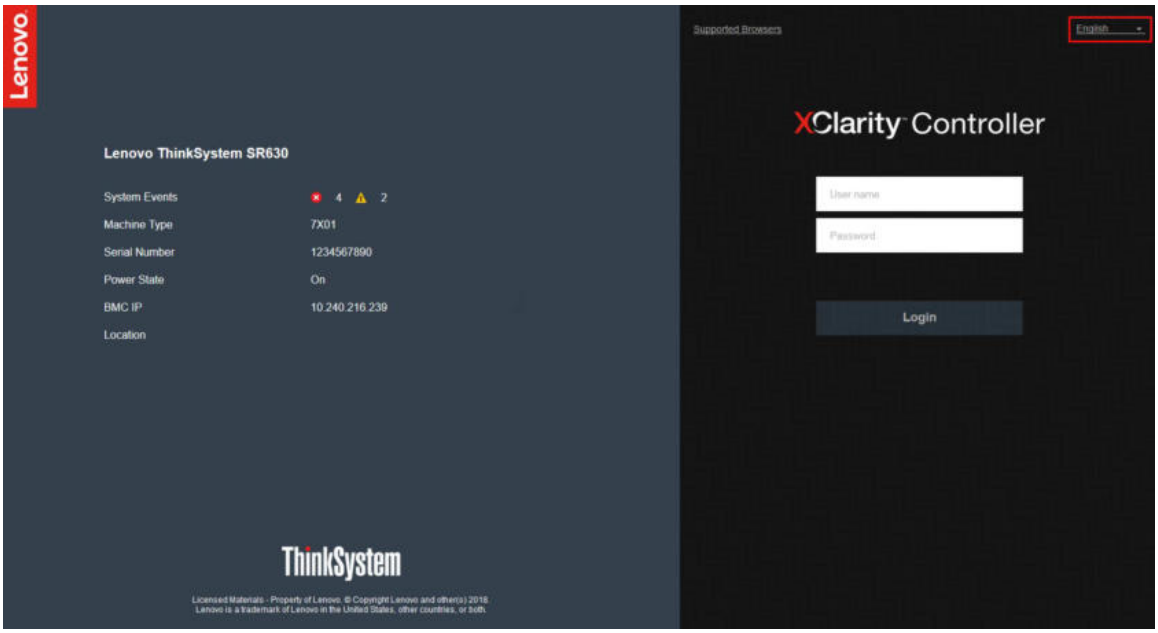
Note: In a Flex System, the XClarity Controller user accounts can be managed by a Flex System Chassis Management Module (CMM) and might be different than the USERID/PASSW0RD combination described above.

To access the XClarity Controller through the XClarity Controller web interface, complete the following steps:

Step 1. Open a web browser. In the address or URL field, type the IP address or host name of the XClarity Controller to which you want to connect.

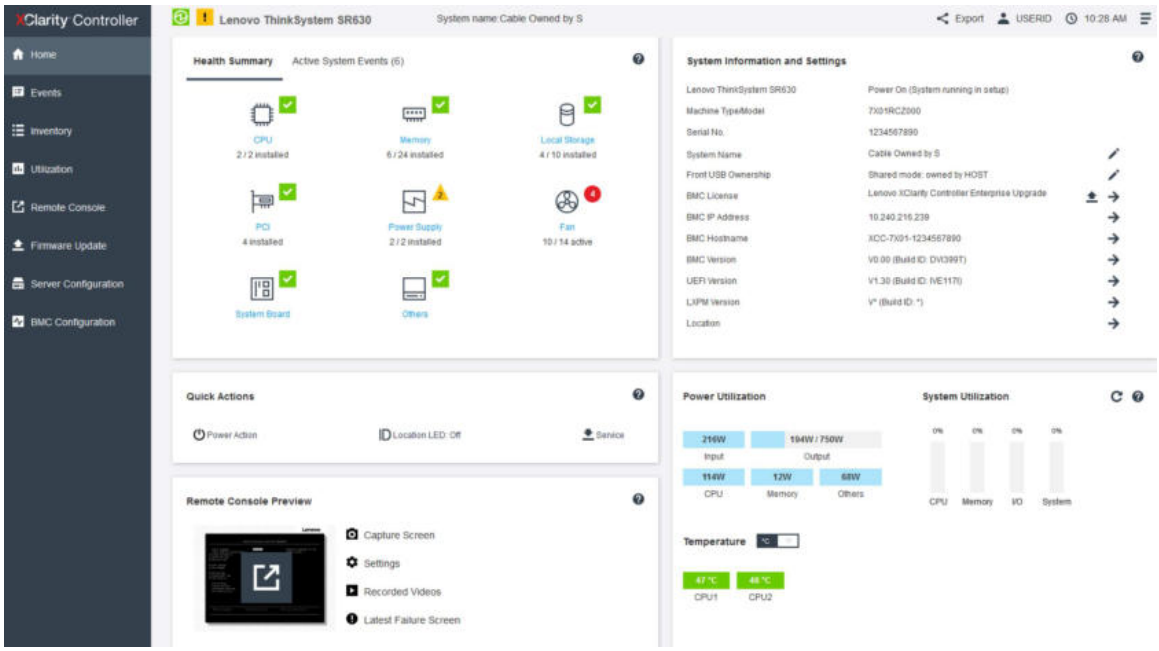
Step 2. Select the desired language from the language drop-down list.

The Login window is shown in the following illustration.



Step 3. Type your user name and password in the XClarity Controller Login window. If you are using the XClarity Controller for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. Depending on how your system administrator configured the user ID, you might need to enter a new password after logging in.

Step 4. Click **Log In** to start the session. The browser opens the XClarity Controller home page, as shown in the following illustration. The home page displays information about the system that the XClarity Controller manages plus icons indicating how many critical errors and how many warnings are currently present in the system.



The home page is essentially divided into two sections. The first section is the left navigation panel, which is a set of topics that allow you to perform the following actions:

- Monitor the server status
- Configure the server
- Configure the XClarity Controller or BMC
- Update the firmware

The second section is the graphical information provided to the right of the navigation panel. The modular format gives you a quick view of the server status and some quick actions that can be performed.

Description of XClarity Controller functions on web interface

The following is a table that describes the XClarity Controller functions in the left navigation panel.

Note: When navigating the web interface, you can also click the question mark icon for online help.

Table 1. XClarity Controller functions

Three column table containing descriptions of the actions that you can perform from the XClarity Controller web interface.

Tab	Selection	Description
Home	Health Summary/Active System Events	Shows the current status of the major hardware components in the system.
	System Information and Settings	Provides a summary of common system information.
	Quick Actions	Provides a quick link to control the server power and location LED, and a button to download the service data.
	Power Utilization/System Utilization/Temperature	Provides a quick overview of the current power utilization, system utilization and overall server temperature.

Table 1. XClarity Controller functions (continued)

Tab	Selection	Description
	Remote Console Preview	Control the server at the operating system level. You can view and operate the server console from your computer. The remote console section in the XClarity Controller home page displays a screen image with a Launch button. The right tool bar includes the following quick actions: • Capture Screen • Settings • Recorded Videos • Latest Failure Screen
Events	Event Log	Provides a historical list of all hardware and management events.
	Audit Log	Provides a historical record of user actions, such as logging in to the Lenovo XClarity Controller, creating a new user, and changing a user password. You can use the audit log to track and document authentication and controls in IT systems.
	Maintenance History	Displays all the firmware update, configuration and hardware replacement history.
	Alert Recipients	Manage who will be notified of system events. It allows you to configure each recipient, and manage settings that apply to all event recipients. You can also generate a test event to verify the notification configuration settings.
Inventory		Displays all the components in the system, along with their status and key information. You can click on a device to display additional information.
Utilization		Displays ambient/component temperature, power utilization, voltage levels, system subsystem utilization and fan speed information of the server and its components in either graphic or tabular formats.
Storage	Detail	Displays the storage devices' physical structure and storage configuration.
	RAID Setup	View or modify current RAID configuration, including the information of virtual disks and physical storage devices.
Remote Console		Provides access to remote console functionality. You can use the virtual media feature to mount ISO or IMG files that are located on your system or on a network location that can be accessed by the BMC using CIFS, NFS, HTTPS, or SFTP. The mounted disk appears as a USB disk drive that is attached to the server.
Firmware Update		• Displays firmware levels. • Update the XClarity Controller firmware and server firmware. • Update the XClarity Controller firmware from Repository.
Server Configuration	Adapters	Displays information of the network adapters installed and the settings that can be configured via the XClarity Controller.
	Boot Options	• Select the boot device for one-time boot during next server restart. • Change boot mode and boot order settings.

Table 1. XClarity Controller functions (continued)

Tab	Selection	Description
	Power Policy	• Configure the power redundancy during the event of a power supply failure. • Configure power capping policy. • Configure power restore policy.
	Server Properties	• Monitor various properties, status conditions, and settings for your server. • Manage server start timeouts to detect and recover from server hang. • Create Trespass Message. A Trespass Message is a message that you can create for users to see when they log in to the XClarity Controller.
BMC Configuration	Backup and Restore	Reset the configuration of the XClarity Controller to factory defaults, backup current configuration or restore configuration from a file.
	License	Manage activation keys for optional XClarity Controller features.
	Network	Configure networking properties, status, and settings for the XClarity Controller.
	Security	Configure security properties, status, and settings for the XClarity Controller.
	User/LDAP	• Configure the XClarity Controller login profiles and global login settings. • View user accounts that are currently logged in to the XClarity Controller. • The LDAP tab configures user authentication for use with one or more LDAP servers. It also allows you to enable or disable LDAP security and manage its certificates.
	Call Home	Configure call home option to collect information about system and send it to Lenovo for services.

Chapter 3. Configuring the XClarity Controller

Use the information in this chapter to understand the options available for XClarity Controller configurations.

When configuring the XClarity Controller, the following key options are available:

- Backup and Restore
- License
- Network
- Security
- User/LDAP

Configuring user accounts/LDAP

Use the information in this topic to understand how user accounts are managed.

Click **User/LDAP** under **BMC Configuration** to create, modify, and view user accounts, and to configure LDAP settings.

The **Local User** tab shows the user accounts that are configured in the XClarity Controller, and which are currently logged in to the XClarity Controller.

The **LDAP** tab shows the LDAP configuration for accessing user accounts that are kept on an LDAP server.

User authentication method

Use the information in this topic to understand the modes that the XClarity Controller can use to authenticate login attempts.

Click **Allow logons from** to select how user login attempts are authenticated. You can select one of the following authentication methods:

- **Local only:** Users are authenticated by a search of the local user account configured in the XClarity Controller. If there is no match of the user ID and password, access is denied.
- **LDAP only:** The XClarity Controller attempts to authenticate the user with credentials kept on an LDAP server. The local user accounts in the XClarity Controller *are not* searched with this authentication method.
- **Local first, then LDAP:** Local authentication is attempted first. If local authentication fails; then, LDAP authentication is attempted.
- **LDAP first, then local user:** LDAP authentication is attempted first. If LDAP authentication fails; then, local authentication is attempted.

Notes:

- Only locally administered accounts are shared with the IPMI and SNMP interfaces. These interfaces do not support LDAP authentication.
- IPMI and SNMP users can login using the locally administered accounts when the **Allow logons from** field is set to **LDAP only**.

Creating a new user account

Use the information in this topic to create a new local user.

© Copyright Lenovo 2017, 2020

Create user

Click **Create** to create a new user account.

Complete the following fields: **User name**, **Password**, **Confirm Password**, and **Authority Level**. For further details on the authority level, see the following section.

User authority level

The following user authority levels are available:

Supervisor
The Supervisor user authority level has no restrictions.

Read only
The Read only user authority level has read-only access and cannot perform actions such as file transfers, power and restart actions, or remote presence functions.

Custom
The Custom user authority level allows a more customized profile for user authority with settings for the actions that the user is allowed to perform.

Select one or more of the following Custom user authority levels:

Adapter Configuration - Networking & Security
A user can modify configuration parameters on the Security, Network, and Serial Port pages.

User Account Management
A user can add, modify, or delete users, and change the global login settings.

Remote Console Access
A user can access the remote console.

Remote Console and Remote Disk Access
A user can access the remote console and the virtual media feature.

Remote Server Power/Restart
A user can perform power-on and restart functions for the server.

Adapter Configuration - Basic
A user can modify configuration parameters on the Server Properties and Events pages.

Ability to Clear Event Logs
A user can clear the event logs. Anyone can look at the event logs; but, this authority level is required to clear the logs.

Adapter Configuration - Advanced (Firmware Update, Restart BMC, Restore Configuration)
A user has no restrictions when configuring the XClarity Controller. In addition, the user is said to have administrative access to the XClarity Controller. Administrative access includes the following advanced functions: firmware updates, PXE network boot, restoring XClarity Controller factory defaults, modifying and restoring XClarity Controller settings from a configuration file, and restarting and resetting the XClarity Controller.

When a user sets the authority level of an XClarity Controller login ID, the resulting IPMI privilege level of the corresponding IPMI User ID is set according to the following priorities:

- If a user sets the XClarity Controller login ID authority level to **Supervisor**, the IPMI privilege level is set to Administrator.
- If a user sets the XClarity Controller login ID authority level to **Read Only**, the IPMI privilege level is set to User.

- If a user sets the XClarity Controller login ID authority level to any of the following types of access, the IPMI privilege level is set to Administrator:
  - User Account Management Access
  - Remote Console Access
  - Remote Console and Remote Disk Access
  - Adapter Configuration - Networking & Security
  - Adapter Configuration - Advanced
- If a user sets the XClarity Controller login ID authority level to **Remote Server Power/Restart Access** or **Ability to Clear Event Logs**, the IPMI privilege level is set to Operator.
- If a user sets the XClarity Controller login ID authority level to **Adapter Configuration - Basic**, the IPMI privilege level is set to User.

SNMPv3 Settings

To enable SNMPv3 access for a user, select the check box next to the **SNMPv3 Settings**. The following user access options are explained:

Access type
Only **GET** operations are supported. The XClarity Controller does not support SNMPv3 **SET** operations. SNMP3 can only perform query operations.

Address for traps
Specify the trap destination for the user. This can be an IP address or hostname. Using traps, the SNMP agent notifies the management station about events, (for example, when a processor temperature exceeds the limit).

Authentication protocol
Only **HMAC-SHA** is supported as the authentication protocol. This algorithm is used by the SNMPv3 security model for authentication.

Privacy protocol
The data transfer between the SNMP client and the agent can be protected using encryption. The supported methods are **CBC-DES** and **AES**.

Notes: Even if repetitive strings of a password is used by an SNMPv3 user, access will still be allowed to the XClarity Controller. Two examples are shown for your reference.

- If the password is set to "*11111111*" (eight-digit number containing eight 1's), the user can still access the XClarity Controller if the password is accidentally inputted with more than eight 1's. For example, if the password is inputted as "*111111111* (ten-digit number containing ten 1's), access will still be granted. The repetitive string will be considered having the same key.
- If the password is set to "*bertbert*", the user can still access the XClarity Controller if the password is accidentally inputted as "*bertbertbert*". Both passwords are considered to have the same key.

For further details, refer to page 72 in the Internet Standard of RFC 3414 document (https://tools.ietf.org/html/rfc3414).

SSH Key

The XClarity Controller supports SSH Public Key Authentication (RSA key type). To add a SSH key to the local user account, select the check box next to the **SSH Key**. The following two options are provided:

Select key file
Select the SSH key file to be imported into the XClarity Controller from your server.

Enter key into a text field
Paste or type the data from your SSH key into the text field.

Notes:

- Some of Lenovo's tools may create a temporary user account for accessing the XClarity Controller when the tool is run on the server operating system. This temporary account is not viewable and does not use any of the 12 local user account positions. The account is created with a random user name (for example, "20luN4SB") and password. The account can only be used to access the XClarity Controller on the internal Ethernet over USB interface, and only for the CIM-XML and SFTP interfaces. The creation and removal of this temporary account is recorded in the audit log as well as any actions performed by the tool with these credentials.
- For the SNMPv3 Engine ID, the XClarity Controller uses a HEX string to denote the ID. This HEX string is converted from the default XClarity Controller host name. See the example below:

  The host name "XCC-7X06-S4AHJ300" is first converted into ASCII format: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  The HEX string is built using the ASCII format (ignore the spaces in between): 58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

Deleting a user account

Use the information in this topic to create a new local user.

To delete a local user account, click the trash can icon on the row of the account that you wish to remove. If you are authorized, you can remove your own account or the account of other users, even if they are currently logged in, unless it is the only account remaining with User Account Management privileges. Sessions that are already in progress when user accounts are deleted will not be automatically terminated.

Using hashed passwords for authentication

Use the information in this topic to understand how to use hashed passwords for authentication.

Aside from the use of passwords and LDAP/AD user accounts, the XClarity Controller also supports third-party hashed passwords for authentication. The special password uses a one-way hash (SHA256) format and is supported by the XClarity Controller web, OneCLI, and CLI interfaces. However, please note that authentication of XCC SNMP, IPMI and CIM interfaces do not support third-party hashed passwords. Only the OneCLI tool and XCC CLI interface can create a new account with a hashed password or perform a hashed password update. The XClarity Controller also allows the OneCLI tool and XClarity Controller CLI interface to retrieve the hashed password if the capability of reading hashed password is enabled.

Setting hashed password via XClarity Controller web

Click **Security** under **BMC Configuration**, and scroll to the **Security Password Manager** section to enable or disable the Third-party Password function. If enabled, a third-party hashed password is employed for log-in authentication. Retrieval of the third-party hashed password from the XClarity Controller can also be enabled of disabled.

Note: By default, the *Third-party Password* and *Allow Third-party Password Retrieval* functions are disabled.

To check if the user password is *Native* or a *Third-party Password*, click **User/LDAP** under **BMC Configuration** for details. The information will be under the **Advanced Attribute** column.

Notes:

- Users will not be able to change a password if it is a third-party password, and the **Password** and **Confirm password** fields have been greyed out.
- If the third-party password has expired, a warning message will be shown during the user login process.

Setting hashed password via OneCLI function

- Enabling feature

  ```
  $ sudo OneCli config set IMM.ThirdPartyPassword Enabled
  ```

- Creating hashed password (No Salt). The following shows an example logging to the XClarity Controller using the *password123* password.

  ```
  $ pwhash =`echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

- Creating user with hashed password (With Salt). The following shows an example logging to the XClarity Controller using the *password123* password. Salt=abc.

  ```
  $ pwhash =`echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  $ sudo OneCli config set IMM.Loginid.3 Admin

  $ sudo OneCli config set IMM.SHA256Password.3 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
  ```

- Retrieving the hashed password and salt.

  ```
  $ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled

  $ sudo OneCli config show IMM.SHA256Password.3

  $ sudo OneCli config show IMM.SHA256PasswordSalt.3
  ```

- Deleting the hashed password and salt.

  ```
  $ sudo OneCli config set IMM.SHA256Password.3 ""

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
  ```

- Setting the hashed password to an existing account.

  ```
  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.Password.2 Passw0rd123abc

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

  Note: While the hashed password is being set, this password will immediately take effect. The original standard password will no longer be effective. In this example, the original standard password *Passw0rd123abc* cannot be used anymore until the hashed password is deleted.

Setting hashed password via CLI function

- Enabling feature

```
> hashpw -sw enabled
```

- Creating hashed password (No Salt). The following shows an example logging to the XClarity Controller using the *password123* password.

  ```
  $ pwhash =`echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  > users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
  super
  ```

- Creating user with hashed password (With Salt). The following shows an example logging to the XClarity Controller using the *password123* password. Salt=abc.

  ```
  $ pwhash =`echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  > users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  -ssalt 'abc' -a super
  ```

- Retrieving the hashed password and salt.

  ```
  > hashpw -re enabled

  > users -3 -ghp -gsalt
  ```

- Deleting the hashed password and salt.

  ```
  > users -3 -shp "" -ssalt ""
  ```

- Setting the hashed password to an existing account.

  ```
  > users -2 -n admin -p Passw0rd123abc -shp
  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
  ```

  Note: While the hashed password is being set, this password will immediately take effect. The original standard password will no longer be effective. In this example, the original standard password *Passw0rd123abc* cannot be used anymore until the hashed password is deleted.

After the hashed password has been set up, remember you do not used this to login to the XClarity Controller. When logging in, you will need to use the plaintext password. In the example shown below, the plaintext password is “password123”.

```
$ pwhash= ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}''

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Configuring global login settings

Use the information in this topic to configure login and password policy settings that apply to all users.

Web inactivity session timeout

Use the information in this topic to set the web inactivity session timeout option.

In the **Web inactivity session timeout** field, you can specify how long, in minutes, the XClarity Controller waits before it disconnects an inactive web session. The maximum wait time is 1,440 minutes. If set to 0, the web session never expires.

The XClarity Controller firmware supports up to six simultaneous web sessions. To free up sessions for use by others, it is recommended that you log out of the web session when you are finished rather than relying on the inactivity timeout to automatically close your session.

Note: If you leave the browser open on an XClarity Controller web page that automatically refreshes, your web session will not automatically close due to inactivity.

Account security policy settings

Use this information to understand and set the account security policy for your server.

Notes: In a Flex System, the account security policy settings are managed by the Flex System Chassis Management Module (CMM) and cannot be modified through the XCC. When the CMM is used to configure the account security policy, make note of the following:

- Unlike the XCC, the CMM does not have the *Password expiration warning period (days)* setting. When the *Password expiration period* is configured to be longer than 5 days in the CMM, the XCC will set the password expiration warning period to be 5 days. Conversely, if the setting is shorter than 5 days, the password expiration warning period will be the same as the value inputted in the *Password expiration period*.
- For the *Maximum number of login failures (times)* setting, the range set forth in the CMM is 0-100 times. However, the range defined in the XCC is 0-10 times. Thus, when the user selects a value that exceeds 10 times in the CMM, the XCC will still set the maximum number of login failures as 10 times.
- For the *Minimum password change interval (hours)* setting, the range set forth in the CMM is 0-1440 hours. However, the range defined in the XCC is 0-240 hours. Thus, when the user selects a value that exceeds 240 hours in the CMM, the XCC will still set the minimum password change interval to be 240 hours.

The following information is a description of the fields for the security settings.

Force to change password on first access

After setting up a new user with a default password, selection of this check box will force that user to change their password the first time that the user logs in. The default value for this field is to have the check box enabled.

Force default account password must be changed on next login

A manufacturing option is provided to reset the default USERID profile after the first successful login. When this check box is enabled, the default password must be changed before the account can be used. The new password is subject to all active password enforcement rules. The default value for this field is to have the check box enabled.

Complex password required

The option box is checked by default and the complex password must adhere to the following rules:

- Only contain the following characters (no white-space characters allowed): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- Must contain at least one letter
- Must contain at least one number
- Must contain at least two of the following combinations:
  - At least one upper-case letter.
  - At least one lower-case letter.
  - At least one special character.
- No other characters (in particular, spaces or white-space characters) are allowed
- Passwords may have no more than two consecutive instances of the same character (i.e., “aaa”).

- The password cannot be literary same as the user name, simply repeating the user name one or more times, or a reverse character order of the user name.
- Passwords must be a minimum of 8 and a maximum of 32 characters long

If the option box is not checked, the number specified in the minimum password length can be set as 0–32 characters. The account password may be blank if minimum password length is set as 0.

Password expiration period (days)
This field contains the maximum password age that is permitted before the password must be changed. A value of 0 to 30 days is supported. The default value for this field is 14 days.

Password expiration warning period (days)
This field contains the number of days a user is warned before their password expires. If it is set to 0, no warnings are sent. A value of 0 to 30 days is supported. The default value for this field is 14 days.

Minimum password length
This field contains the minimum length of the password. 8 to 32 characters are supported for this field. The default value for this field is 10.

Minimum password reuse cycle
This field contains the number of previous passwords that cannot be reused. Up to ten previous passwords can be compared. Select 0 to allow the reuse of all previous passwords. A value of 0 to 10 is supported. The default value for this field is 5.

Minimum password change interval (hours)
This field contains how long a user must wait between password changes. A value of 0 to 240 hours is supported. The default value for this field is 1 hour.

Maximum number of login failures (times)
This field contains the number of failed login attempts that are allowed before the user is locked out for a period of time. A value of 0 to 10 is supported. The default value for this field is five login failures.

Lockout period after maximum login failures (minutes)
This field specifies how long (in minutes), the XClarity Controller subsystem will disable remote login attempts after the maximum number of login failures has been reached. A value of 0 to 2,880 minutes is supported. The default value for this field is 60 minutes.

Configuring LDAP

Use the information in this topic to view or change XClarity Controller LDAP settings.

LDAP support includes:

- Support for LDAP protocol version 3 (RFC-2251)
- Support for the standard LDAP client APIs (RFC-1823)
- Support for the standard LDAP search filter syntax (RFC-2254)
- Support for Lightweight Directory Access Protocol (v3) Extension for Transport Layer Security (RFC-2830)

The LDAP implementation supports the following LDAP servers:

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012)
- Microsoft Active Directory Application Mode (Windows 2003 Server)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012)
- Novell eDirectory Server, version 8.7 and 8.8

- OpenLDAP Server 2.1, 2.2, 2.3 and 2.4

Click the **LDAP** tab to view or modify XClarity Controller LDAP settings.

The XClarity Controller can remotely authenticate a user's access through a central LDAP server instead of, or in addition to the local user accounts that are stored in the XClarity Controller itself. Privileges can be designated for each user account using the IBMRBSPermissions string. You can also use the LDAP server to assign users to groups and perform group authentication, in addition to the normal user (password check) authentication. For example, an XClarity Controller can be associated with one or more groups, the user will pass group authentication only if the user belongs to at least one group that is associated with the XClarity Controller.

To configure an LDAP server, complete the following steps:

1. Under **LDAP Server Information**, the following options are available from the item list:
   - **Use LDAP server for Authentication only (with local authorization)**: This selection directs the XClarity Controller to use the credentials only to authenticate to the LDAP server and to retrieve group membership information. The group names and privileges can be configured in the Active Directory Settings section.
   - **Use LDAP server for Authentication and Authorization**: This selection directs the XClarity Controller to use the credentials both to authenticate to the LDAP server and to identify a user's permission.

   Note: The LDAP servers to be used for authentication can either be configured manually or discovered dynamically via DNS SRV records.

   - **Use Pre-Configured Servers**: You can configure up to four LDAP servers by entering each server's IP address or host name if DNS is enabled. The port number for each server is optional. If this field is left blank, the default value of 389 is used for non-secured LDAP connections. For secured connections, the default port value is 636. You must configure at least one LDAP server.
   - **Use DNS to Find Servers**: You can choose to discover the LDAP server(s) dynamically. The mechanisms described in RFC2782 (A DNS RR for specifying the location of services) are used to locate the LDAP server(s). This is known as DNS SRV. You need to specify a fully qualified domain name (FQDN) to be used as the domain name in the DNS SRV request.
     - **AD Forest**: In an environment with universal groups in cross domains, the forest name (set of domains) must be configured to discover the required Global Catalogs (GC). In an environment where cross-domain group membership does not apply, this field can be left blank.
     - **AD Domain**: You will need to specify a fully qualified domain name (FQDN) to be used as the domain name in the DNS SRV request.

   If you wish to enable secure LDAP, click the **Enable Secure LDAP** check box. In order to support secure LDAP, a valid SSL certificate must be in place and at least one SSL client trusted certificate must be imported into the XClarity Controller. Your LDAP server must support Transport Layer Security (TLS) version 1.2 to be compatible with the XClarity Controller secure LDAP client. For more information about certificate handling, see "SSL certificate handling" on page 37.
2. Fill in information under **Additional Parameters**. Below are explanations of the parameters.

   Binding method

   Before you can search or query the LDAP server, you must send a bind request. This field controls how this initial bind to the LDAP server is performed. The following bind methods are available:

   - **No Credentials Required**

Use this method to bind without a Distinguished Name (DN) or password. This method is strongly discouraged because most servers are configured to not allow search requests on specific user records.

- **Use Configured Credentials**

  Use this method to bind with the configured client DN and password.

- **Use Login Credentials**

  Use this method to bind with the credentials that are supplied during the login process. The user ID can be provided through a DN, a partial DN, a fully qualified domain name, or through a user ID that matches the UID Search Attribute that is configured on the XClarity Controller. If the credentials that are presented resemble a partial DN (e.g. cn=joe), this partial DN will be prepended to the configured Root DN in an attempt to create a DN that matches the user's record. If the bind attempt fails, a final attempt will be made to bind by prepending cn= to the login credential, and prepending the resulting string to the configured Root DN.

If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in. If necessary, a second attempt to bind is made, this time with the DN that is retrieved from the user's LDAP record and the password that was entered during the login process. If the second attempt to bind fails, the user is denied access. The second bind is performed only when the **No Credentials Required** or **Use Configured Credentials** binding methods are used.

Root Distinguished Name (DN)

This is the distinguished name (DN) of the root entry of the directory tree on the LDAP server (for example, dn=mycompany,dc=com). This DN is used as the base object for all search requests.

UID Search Attribute

When the binding method is set to **No Credentials Required** or **Use Configured Credentials**, the initial bind to the LDAP server is followed by a search request that retrieves specific information about the user, including the user's DN, login permissions, and group membership. This search request must specify the attribute name that represents the user IDs on that server. This attribute name is configured in this field. On Active Directory servers, the attribute name is usually **sAMAccountName**. On Novell eDirectory and OpenLDAP servers, the attribute name is **uid**. If this field is left blank, the default is **uid**.

Group Filter

The **Group Filter** field is used for group authentication. Group authentication is attempted after the user's credentials are successfully verified. If group authentication fails, the user's attempt to log on is denied. When the group filter is configured, it is used to specify to which groups the XClarity Controller belongs. This means that to succeed the user must belong to at least one of the groups that are configured for group authentication. If the **Group Filter** field is left blank, group authentication automatically succeeds. If the group filter is configured, an attempt is made to match at least one group in the list to a group that the user belongs. If there is no match, the user fails authentication and is denied access. If there is at least one match, group authentication is successful.

The comparisons are case sensitive. The filter is limited to 511 characters and can consist of one or more group names. The colon (:) character must be used to delimit multiple group names. Leading and trailing spaces are ignored, but any other space is treated as part of the group name.

Note: The wildcard character (*) is no longer treated as a wildcard. The wildcard concept has been discontinued to prevent security exposures. A group name can be specified as a full DN or by using only the *cn* portion. For example, a group with a DN of cn=adminGroup, dc=mycompany, dc=com can be specified using the actual DN or with adminGroup.

Nested group membership is supported only in Active Directory environments. For example, if a user is a member of GroupA and GroupB, and GroupA is also a member of GroupC, the user is said

to be a member of GroupC also. Nested searches stop if 128 groups have been searched. Groups in one level are searched before groups in a lower level. Loops are not detected.

Group Search Attribute

In an Active Directory or Novell eDirectory environment, the **Group Search Attribute** field specifies the attribute name that is used to identify the groups to which a user belongs. In an Active Directory environment, the attribute name is **memberOf**. In an eDirectory environment, the attribute name is **groupMembership**. In an OpenLDAP server environment, users are usually assigned to groups whose objectClass equals PosixGroup. In that context, this field specifies the attribute name that is used to identify the members of a particular PosixGroup. This attribute name is **memberUid**. If this field is left blank, the attribute name in the filter defaults to **memberOf**.

Login Permission Attribute

When a user is authenticated through an LDAP server successfully, the login permissions for the user must be retrieved. To retrieve the login permissions, the search filter that is sent to the server must specify the attribute name that is associated with login permissions. The **Login Permission Attribute** field specifies the attribute name. If this field is left blank, the user is assigned a default of read-only permissions, assuming that the user passes the user and group authentication.

The attribute value that is returned by the LDAP server searches for the keyword string IBMRBSPermissions=. This keyword string must be immediately followed by a bit string that is entered as 12 consecutive 0s or 1s. Each bit represents a set of functions. The bits are numbered according to their positions. The left-most bit is bit position 0, and the right-most bit is bit position 11. A value of 1 at a bit position enables the function that is associated with that bit position. A value of 0 at a bit position disables the function that is associated with that bit position.

The string IBMRBSPermissions=010000000000 is a valid example. The IBMRBSPermissions= keyword is used to allow it to be placed anywhere in this field. This enables the LDAP administrator to reuse an existing attribute; therefore, preventing an extension to the LDAP schema. This also enables the attribute to be used for its original purpose. You can add the keyword string anywhere in this field. The attribute that you use can allow for a free-formatted string. When the attribute is retrieved successfully, the value that is returned by the LDAP server is interpreted according to the information in the following table.

Table 2. Permission bits

Three column table containing bit position explanations.

Bit position	Function	Explanation
0	Deny Always	A user will always fail authentication. This function can be used to block a particular user or users associated with a particular group.
1	Supervisor Access	A user is given administrator privileges. The user has read/write access to every function. If you set this bit, you do not have to individually set the other bits.
2	Read Only Access	A user has read-only access, and cannot perform any maintenance procedures (for example, restart, remote actions, or firmware updates) or make modifications (for example, the save, clear, or restore functions. Bit position 2 and all other bits are mutually exclusive, with bit position 2 having the lowest precedence. When any other bit is set, this bit will be ignored.
3	Networking and Security	A user can modify the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port configurations.
4	User Account Management	A user can add, modify, or delete users and change the Global Login Settings in the Login Profiles window.

Table 2. Permission bits (continued)

Bit position	Function	Explanation
5	Remote Console Access	A user can access the remote server console.
6	Remote Console and Remote Disk Access	A user can access the remote server console and the remote disk functions for the remote server.
7	Remote Server Power/ Restart Access	A user can access the power on and restart functions for the remote server.
8	Basic Adapter Configuration	A user can modify configuration parameters in the System Settings and Alerts windows.
9	Ability to Clear Event Logs	A user can clear the event logs. **Note:** All users can view the event logs; but, to clear the event logs the user is required to have this level of permission.
10	Advanced Adapter Configuration	A user has no restrictions when configuring the XClarity Controller. In addition the user has administrative access to the XClarity Controller. The user can perform the following advanced functions: firmware upgrades, PXE network boot, restore XClarity Controller factory defaults, modify and restore adapter configuration from a configuration file, and restart/reset the XClarity Controller.
11	Reserved	This bit position is reserved for future use. If none of the bits are set, the user has read-only authority. Priority is given to login permissions that are retrieved directly from the user record. If the login permission attribute is not in the user's record, an attempt is made to retrieve the permissions from the groups to which the user belongs. This is performed as part of the group authentication phase. The user is assigned the inclusive OR of all the bits for all groups. The Read Only Access bit (position 2) is set only if all other bits are set to zero. If the Deny Always bit (position 0) is set for any of the groups, the user is refused access. The Deny Always bit (position 0) always has precedence over all other bits.

If none of the bits are set, the default will be set to **Read Only** for the user.

Note that priority is given to login permissions retrieved directly from the user record. If the user does not have the login permission attribute in its record, an attempt will be made to retrieve the permissions from the group(s) that the user belongs to, and, if configured, that match the group filter. In this case the user will be assigned the inclusive OR of all the bits for all of the groups. Similarly, the **Read Only Access** bit will only be set if all the other bits are zero. Moreover, note that if the **Deny Always** bit is set for any of the groups, the user will be refused access. The **Deny Always** bit always has precedence over every other bit.

Note: If you give a user the ability to modify basic, networking, and/or security related adapter configuration parameters, you should consider giving this same user the ability to restart the XClarity Controller (bit position 10). Otherwise, without this ability, a user might be able to change parameters (for example, IP address of the adapter), but will not be able to have them take effect.

3. Choose whether or not to **Enable enhanced role-based security for Active Directory Users** under **Active Directory Settings** (if **Use LDAP server for Authentication and Authorization** mode is used), or configure the **Groups for Local Authorization** (if **Use LDAP server for Authentication only** (**with local authorization**) mode is used).

   - **Enable enhanced role-based security for Active Directory Users**

If enhanced role-based security setting is enabled, a free-formatted server name must be configured to act as the target name for this particular XClarity Controller. The target name can be associated with one or more roles on the Active Directory server through a Role Based Security (RBS) Snap-In. This is accomplished by creating managed targets, giving them specific names, and then associating them to the appropriate roles. If a name is configured in this field, it provides the ability to define specific roles for users and XClarity Controllers (targets) who are members of the same role. When a user logs in to the XClarity Controller and is authenticated via Active Directory, the roles that the user is a member of are retrieved from the directory. The permissions that are assigned to the user are extracted from the roles that also have as a member a target that matches the server name that is configured here, or a target that matches any XClarity Controller. Multiple XClarity Controllers can share the same target name. This could be used to group multiple XClarity Controllers together and assign them to the same role (or roles) by using a single managed target. Conversely each XClarity Controller can be given a unique name.

- **Groups for Local Authorization**

  Group Names are configured to provide local authorization specifications for groups of users. Each group name can be assigned permissions (Roles) that are the same as described in the table above. The LDAP server associates users with a group name. When the user logs in he is assigned the permissions that are associated with the group to which the user belongs. Additional groups can be configured by clicking the “+” icon or deleted by clicking the “x” icon.

Configuring network protocols

Use the information in this topic to view or establish network settings for the XClarity Controller.

Configuring the Ethernet settings

Use the information in this topic to view or change how the XClarity Controller communicates by way of an Ethernet connection.

Note: The AMD servers do not support the Ethernet failover function.

The XClarity Controller uses two network controllers. One network controller is connected to the dedicated management port and the other network controller is connected to the shared port. Each of the network controllers is assigned its own burned in MAC address. If DHCP is being used to assign an IP address to the XClarity Controller, when a user switches between network ports or when a failover from the dedicated network port to the shared network port occurs, a different IP address may be assigned to the XClarity Controller by the DHCP server. It is recommended that when using DHCP, users should use the host name to access the XClarity Controller rather than relying on an IP address. Even if the XClarity Controller network ports are not changed, the DHCP server could possibly assign a different IP address to the XClarity Controller when the DHCP lease expires, or when the XClarity Controller reboots. If a user needs to access the XClarity Controller using an IP address that will not change, the XClarity Controller should be configured for a static IP address rather than DHCP.

Click **Network** under **BMC Configuration** to modify XClarity Controller Ethernet settings.

Configuring the XClarity Controller Host Name

The default XClarity Controller host name is generated using a combination of the string “XCC -“ followed by the server machine type and server serial number (for example. “XCC-7X03-1234567890”). You can change the XClarity Controller host name by entering up to a maximum of 63 characters in this field. The host name must not include a period (.) and can contain only alpha, numeric, hyphen and underscore characters.

Ethernet Ports

This setting controls the enablement of Ethernet ports used by management controller, including the shared and dedicated ports.

Once **disabled**, all Ethernet ports will not be assigned any IPv4 or IPv6 addresses, and prevents any further changes to any Ethernet configurations.

Note: This setting does not affect the USBLAN interface or the USB management port at the front of the server. Those interfaces have their own dedicated enablement settings.

Configuring IPv4 network settings

To use an IPv4 Ethernet connection, complete the following steps:

1. Enable the **IPv4** option.

   Note: Disabling the Ethernet interface prevents access to the XClarity Controller from the external network.
2. From the **Method** field, select one of the following options:
   - **Obtain IP from DHCP**: The XClarity Controller will obtain its IPv4 address from a DHCP server.
   - **Use static IP address**: The XClarity Controller will use the user specified value for its IPv4 address.
   - **First DHCP, then static IP address**: The XClarity Controller will attempt to obtain its IPv4 address from a DHCP server, but if that attempt fails, the XClarity Controller will use user specified value for its IPv4 address.
3. In the **Static address** field, type the IP address that you want to assign to the XClarity Controller.

   Note: The IP address must contain four integers from 0 to 255 with no spaces and separated by periods. This field will not be configurable if the method is set to **Obtain IP from DHCP**.
4. In the **Network mask** field, type the subnet mask that is used by the XClarity Controller.

   Note: The subnet mask must contain four integers from 0 to 255 with no spaces or consecutive periods and separated by periods. The default setting is 255.255.255.0. This field will not be configurable if the method is set to **Obtain IP from DHCP**.
5. In the **Default Gateway** field, type your network gateway router.

   Note: The gateway address must contain four integers from 0 to 255 with no spaces or consecutive periods and separated by periods. This field will not be configurable if the method is set to **Obtain IP from DHCP**.

Configuring advanced Ethernet settings

Click the **Advanced Ethernet** tab to set additional Ethernet settings.

Note: In a Flex System, the VLAN settings are managed by a Flex System CMM and cannot be modified on the XClarity Controller.

To enable Virtual LAN (VLAN) tagging select the **Enable VLAN** check box. When VLAN is enabled and a VLAN ID is configured, the XClarity Controller only accepts packets with the specified VLAN IDs. The VLAN IDs can be configured with numeric values between 1 and 4094.

From the **MAC selection** list choose one of the following selections:

- Use burned in MAC address

  The Burned-in MAC address option is a unique physical address that is assigned to this XClarity Controller by the manufacturer. The address is a read-only field.
- Use custom MAC address

  If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value from `000000000000` through `FFFFFFFFFFFF`. This value

must be in the form *xx:xx:xx:xx:xx:xx* where *x* is a hexadecimal number from 0 to 9 or “a” through “f”. The XClarity Controller does not support the use of a multicast address. The first byte of a multicast address is an odd number (the least significant bit is set to 1); therefore, the first byte must be an even number.

In the **Maximum transmission unit** field, specify the maximum transmission unit of a packet (in bytes) for your network interface. The maximum transmission unit range is from 60 to 1500. The default value for this field is 1500.

To use an IPv6 Ethernet connection, complete the following steps:

Configuring IPv6 network settings

1. Enable the **IPv6** option.
2. Assign an IPv6 address to the interface using one of the following assignment methods:
   - Use stateless address autoconfiguration
   - Use stateful address configuration (DHCPv6)
   - Use statically assigned IP address

     Notes: When the **Use statically assigned IP addres** is chosen, you will be asked to type the following information:

     – IPv6 Address
     – Prefix length
     – Gateway

Configuring DNS

Use the information in this topic to view or change XClarity Controller Domain Name System (DNS) settings.

Note: In a Flex System, DNS settings cannot be modified on the XClarity Controller. DNS settings are managed by the CMM.

Click **Network** under **BMC Configuration** to view or modify XClarity Controller DNS settings.

If you click the **Use additional DNS address servers** check box, specify the IP addresses of up to three Domain Name System servers on your network. Each IP address must contain integers from 0 to 255, separated by periods. These DNS server addresses are added to the top of the search list, so a host name lookup is done on these servers before one that is automatically assigned by a DHCP server.

Configuring DDNS

Use the information in this topic to enable or disable Dynamic Domain Name System (DDNS) protocol on the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify XClarity Controller DDNS settings.

Click the **Enable DDNS** check box, to enable DDNS. When DDNS is enabled, the XClarity Controller notifies a domain name server to change in real time, the active domain name server configuration of the XClarity Controller configured host names, addresses or other information that is stored in the domain name server.

Choose an option from the item list to decide how you want the domain name of the XClarity Controller to be selected.

- **Use custom domain name**: You can specify the domain name to which the XClarity Controller belongs.

- **Use domain name obtained from the DHCP server**: The domain name to which the XClarity Controller belongs is specified by the DHCP server.

Configuring Ethernet over USB

Use the information in this topic to control the Ethernet over USB interface used for in-band communication between the server and the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify the XClarity Controller Ethernet over USB settings.

The Ethernet over USB is used for in-band communications to the XClarity Controller. Click the check box to enable or disable the Ethernet over USB interface.

Important: If you disable the Ethernet over USB, you cannot perform an in-band update of the XClarity Controller firmware or server firmware using the Linux or Windows flash utilities.

Select the method that The XClarity Controller uses to assign addresses to the endpoints of the Ethernet over USB interface.

- **Use IPv6 link-local address for Ethernet over USB**: This method uses IPv6 addresses based off the MAC address that have been allocated to the endpoints of the Ethernet over USB interface. Normally, the IPv6 link local address is generated using the MAC address (RFC 4862) but Windows 2008 and newer 2016 operating systems do not support a static link local IPv6 address on the host end of the interface. Instead the default Windows behavior regenerates random link local addresses while running. If the XClarity Controller Ethernet over USB interface is configured to use the IPv6 link local address mode, various functions that make use of this interface will not work because the XClarity Controller does not know what address Windows has assigned to the interface. If the server is running Windows use one of the other Ethernet over USB address configuration methods, or disable the default Windows behavior by using this command: *netsh interface ipv6 set global randomizeidentifiers=disabled*
- **Use IPv4 link-local address for Ethernet over USB**: An IP address in the 169.254.0.0/16 range is assigned to the XClarity Controller and server side of the network.
- **Configure IPv4 setting for Ethernet over USB**: With this method, it specifies the IP addresses and network mask that are assigned to the XClarity Controller and the server side of the Ethernet over USB interface.

Notes:

1. The OS IP configuration settings is not used to set the OS IP address of Ethernet Over USB interface, but is used to notify BMC that OS IP address of Ethernet over USB has changed.
2. Before you configure three IP settings for Ethernet over USB, you need to manually configure the OS IP address of Ethernet over USB interface in your local operating system.

Mapping of external Ethernet port numbers to Ethernet over USB port numbers is controlled by clicking the **Enable external Ethernet to Ethernet over USB port forwarding** checkbox and completing the mapping information for ports you wish to have forwarded from the management network interface to the server.

Configuring SNMPv3

Use the information in this topic to configure SNMP agents.

Complete the following steps to configure the XClarity Controller SNMPv3 alert settings.

1. Click **Network** under **BMC Configuration**.
2. Check the corresponding check box to enable the SNMPv3 agent or SNMP Traps.
3. If enabling the SNMP Traps, select the following event types you wish to be alerted:

- **Critical**
- **Attention**
- **System**

4. If enabling the SNMPv3 agent, complete the following fields:
   a. In the **BMC Contact** field, enter the name of the contact person.
   b. In the **Location** field, enter the site (geographical coordinates).

Enabling or Disabling IPMI Network Access

Use the information in this topic to control IPMI network access to the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify XClarity Controller IPMI settings. Complete the following fields to view or modify IPMI settings:

IPMI over LAN Access
Click the switch to enable or disable IPMI network access to the XClarity Controller.

Important:

- If you are not using any tools or applications that access the XClarity Controller through the network using the IPMI protocol, it is highly recommended that you disable IPMI network access for improved security.
- IPMI over LAN access to the XClarity Controller is disabled by default.

Configuring Network Settings with IPMI commands

Use the information in this topic to configure the network settings using IPMI commands.

Because each BMC network setting is configured using separate IPMI requests and in no particular order, the BMC does not have the complete view of all of the network settings until the BMC is restarted to apply the pending network changes. The request to change a network setting may succeed at the time that the request is made, but later be determined to be invalid when additional changes are requested. If the pending network settings are incompatible when the BMC is restarted, the new settings will not be applied. After restarting the BMC, you should attempt to access the BMC using the new settings to ensure that they have been applied as expected.

Service Enablement and Port Assignment

Use the information in this topic to view or change the port numbers used by some services on the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify XClarity Controller port assignments. Complete the following fields to view or modify port assignments:

Web
The port number is 80. This field is not user-configurable.

Web over HTTPS
In this field specify the port number for Web Over HTTPS. The default value is 443.

REST over HTTPS
The port number will automatically change to the one specified in the Web over HTTPS field. This field is not user-configurable.

CIM over HTTP

In this field specify the port number for CIM over HTTP. The default value is 5989.

Note: CIM is disabled by default.

Remote Presence
In this field specify the port number for Remote Presence. The default value is 3900.

IPMI over LAN
The port number is 623. This field is not user-configurable.

Note: IPMI is disabled by default.

SFTP
In this field specify the port number that is used for the SSH File Transfer Protocol (SFTP). The port number is 115. This field is not user-configurable.

Note: IMM.SFTPPortControl=open is required for OneCLI in-band updates.

SLP
In this field specify the port number that is used for the SLP. The port number is 427. This field is not user-configurable.

Notes: There are two service types that XClarity Controller reports:

- service: management-hardware.Lenovo:lenovo-xclarity-controller
- service: wbem

SSDP
The port number is 1900. This field is not user-configurable.

SSH
In this field specify the port number that is configured to access the command line interface through the SSH protocol. The default value is 22.

SNMP Agent
In this field specify the port number for the SNMP agent that runs on the XClarity Controller. The default value is 161. Valid port number values are from 1 to 65535.

SNMP Traps
In this field specify the port number that is used for SNMP traps. The default value is 162. Valid port number values are from 1 to 65535.

Configuring Access Restriction

Use the information in this topic to view or change the settings that block access from IP addresses or MAC addresses to the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify XClarity Controller access control settings.

Block List and Time Restriction

These options allow you to block specific IP/Mac addresses for specific period of time.

- **List of Blocked IP Addresses**
  - You can enter up to three IPv4 addresses or ranges and three IPv6 addresses or ranges separated by commas, which are not allowed to access the XClarity Controller. Refer to the IPv4 examples below:

  - Single IPv4 address sample: 192.168.1.1
  - Supernet IPv4 address sample: 192.168.1.0/24
  - IPv4 range sample: 192.168.1.1–192.168.1.5
- **List of Blocked MAC address**
  - You can enter up to three MAC addresses separated by commas, which are not allowed to access the XClarity Controller. For example: 11:22:33:44:55:66.
- **Restricted Access (one time)**
  - You can schedule a one-time time interval during which the XClarity Controller cannot be accessed. For the time interval that you specify:
  - The beginning date and time must be later than the current XCC time.
  - The ending date and time must be later than the beginning date and time.
- **Restricted Access (daily)**
  - You can schedule one or more daily time intervals during which the XClarity Controller cannot be accessed. For each time interval that you specify:
  - The ending date and time must be later than the beginning date and time.

Externally Triggered Block List

These options allow you to setup automatic blocking of specific IP addresses (IPv4 and IPv6) from which client successively attempted to log in to XClarity Controller with different incorrect username or password.

Automatic blocking will dynamically determines when excessive login failures occur from a particular IP address and blocks that address from accessing XClarity Controller for a predetermined amount of time.

- **Maximum number of login failures from a particular IP**
  - The maximum number of times indicates the number of login failures allowed for a user with an incorrect password from a specific IP address before it becomes locked-out.
  - If set to 0, IP address will never be locked due to login failures.
  - The failed login counter for the specific IP address will be reset to zero after successful login from that IP address.
- **Lockout period for blocking an IP**
  - The minimum amount of time (in minutes) that must pass before a user can attempt to log back in again from a locked IP address.
  - If set to 0, access from the locked IP address remains blocked-out until the administrator explicitly unlocks it.
- **Block List**
  - The table Block List displays all locked IP addresses. You can unlock one or all IP addresses from the Block List.

Configuring Front Panel USB Port to Management

Use the information in this topic to configure the XClarity Controller Front Panel USB Port to Management.

On some servers the front panel USB port can be switched to attach either to the server or to the XClarity Controller. Connection to the XClarity Controller is primarily intended for use with a mobile device running the Lenovo XClarity Mobile app. When a USB cable is connected between the mobile device and the server's front panel, an Ethernet over USB connection will be established between the mobile app running on the device and the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify XClarity Controller front panel USB port to management settings.

There are four types of settings that you can choose from:

Host Only Mode
The front panel USB port is always connected only to the server.

BMC Only Mode
The front panel USB port is always connected only to the XClarity Controller.

Shared Mode: owned by BMC
The front panel USB port is shared by both the server and the XClarity Controller, but the port is switched to the XClarity Controller.

Shared Mode: owned by Host
The front panel USB port is shared by both the server and the XClarity Controller, but the port is switched to the host.

For additional information about the Mobile app, see the following site:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

Notes:

- If the front panel USB port is configured for Shared Mode, the port is connected to the XClarity Controller when there is no power, and is connected to the server when there is power. When there is power, the control of the front panel USB port can be switched back and forth between the server and the XClarity Controller. In shared mode, the port can also be switched between the host and the XClarity Controller by pressing and holding the front panel Identification button (for compute nodes it may be the USB management button) for more than 3 seconds.
- When configured in Shared Mode and the USB port is currently connected to the server, the XClarity Controller can support a request to switch the front panel USB port back to the XClarity Controller. When this request is executed, the front panel USB port will remain connected to the XClarity Controller until there is no USB activity to the XClarity Controller for the period specified by the inactivity timeout.

Configuring security settings

Use the information in this topic to configure security protocols.

Note: The default minimum TLS version setting is TLS 1.2, but you can configure the XClarity Controller to use other TLS versions if needed by your browser or management applications. For more information, see “tls command” on page 146.

Click **Security** under **BMC Configuration** to access and configure security properties, status, and settings for your XClarity Controller.

SSL overview

This topic is an overview of the SSL security protocol.

SSL is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that prevents eavesdropping, tampering, and message forgery. You can configure the XClarity Controller to use SSL support for different types of connections, such as secure web server (HTTPS), secure LDAP connection (LDAPS), CIM over HTTPS, and SSH server, and to manage the certificates that are required for SSL.

SSL certificate handling

This topic provides information about the administration of certificates that can be used with the SSL security protocol.

You can use SSL with a self-signed certificate or with a certificate that is signed by a third-party certificate authority. Using a self-signed certificate is the simplest method for using SSL; but, it does create a small security risk. The risk arises because the SSL client has no way of validating the identity of the SSL server for the first connection that is attempted between the client and server. For example, it is possible that a third party might impersonate the XClarity Controller web server and intercept data that is flowing between the actual XClarity Controller web server and the user's web browser. If, at the time of the initial connection between the browser and the XClarity Controller, the self-signed certificate is imported into the certificate store of the browser, all future communications will be secure for that browser (assuming that the initial connection was not compromised by an attack).

For more complete security, you can use a certificate that is signed by a certificate authority (CA). To obtain a signed certificate, you will need to select **Generate Certificate Signing Request (CSR)**. Select **Download Certificate Signing Request (CSR)** and send the Certificate-Signing Request (CSR) to a CA to obtain a signed certificate. When the signed certificate is received, select **Import Signed Certificate** to import it into the XClarity Controller.

The function of the CA is to verify the identity of the XClarity Controller. A certificate contains digital signatures for the CA and the XClarity Controller. If a well-known CA issues the certificate or if the certificate of the CA has already been imported into the web browser, the browser can validate the certificate and positively identify the XClarity Controller web server.

The XClarity Controller requires a certificate for use with HTTPS Server, CIM over HTTPS, and the secure LDAP client. In addition the secure LDAP client also requires one or more trusted certificates to be imported. The trusted certificate is used by the secure LDAP client to positively identify the LDAP server. The trusted certificate is the certificate of the CA that signed the certificate of the LDAP server. If the LDAP server uses self-signed certificates, the trusted certificate can be the certificate of the LDAP server itself. Additional trusted certificates must be imported if more than one LDAP server is used in your configuration.

SSL certificate management

This topic provides information about some of the actions that can be selected for certificate management with the SSL security protocol.

Click **Security** under **BMC Configuration** to configure the SSL certificate management.

When managing XClarity Controller certificates, you are presented with the following actions:

Download Signed Certificate

Use this link to download a copy of the currently installed certificate. The certificate can be downloaded in either PEM or DER format. The contents of the certificate can be viewed using a third-party tool such as OpenSSL (www.openssl.org). An example of the command line for viewing the contents of the certificate using OpenSSL would look something like the following:

```
openssl x509 -in cert.der -inform DER -text
```

Download Certificate Signing Request (CSR)

Use this link to download a copy of the certificate signing request. The CSR can be downloaded in either PEM or DER format.

Generate Signed Certificate

Generate a self-signed certificate. After the operation is completed, SSL may be enabled using the new certificate.

Note: When performing the **Generate Signed Certificate** action, a Generate self-signed certificate for HTTPS window opens. You will be prompted to complete the required and optional fields. You *must* complete the required fields. Once you have entered your information, click **Generate** to complete the task.

Generate Certificate Signing Request (CSR)
Generate a certificate signing request (CSR). After the operation is completed, the CSR file may be downloaded and sent to a certificate authority (CA) for signing.

Note: When performing the **Generate Certificate Signing Request (CSR)** action, a Generate Certificate Signing Request for HTTPS window opens. You will be prompted to complete the required and optional fields. You *must* complete the required fields. Once you have entered your information, click **Generate** to complete the task.

Import a Signed Certificate
Use this to import a signed certificate. To obtain a signed certificate, a certificate signing request (CSR) must first be generated and sent to a certificate authority (CA).

Configuring the Secure Shell server

Use the information in this topic to understand and enable the SSH security protocol.

Click **Network** under **BMC Configuration** to configure the Secure Shell server.

To use the SSH protocol, a key needs to be generated first to enable the SSH server.

Notes:

- No certificate management is required to use this option.
- The XClarity Controller will initially create a SSH server key. If you wish to generate a new SSH server key, click **Network** under **BMC Configuration**; then, click **Regenerate key**.
- After you complete the action, you must restart the XClarity Controller for your changes to take effect.

IPMI over Keyboard Controller Style (KCS) Access

Use the information in this topic to control IPMI over Keyboard Controller Style (KCS) access to the XClarity Controller.

The XClarity Controller provides an IPMI interface via the KCS channel that does not require authentication.

Click **Security** under **BMC Configuration** to enable or disable IPMI over KCS access.

Note: After you change the settings, you must restart the XClarity Controller for your changes to take effect.

Important: If you are not running any tools or applications on the server that access the XClarity Controller through the IPMI protocol, it is highly recommended that you disable the IPMI KCS access for improved security. XClarity Essentials does use the IPMI over KCS interface to the XClarity Controller. If you disabled the IPMI over KCS interface, re-enable it prior to running XClarity Essentials on the server. Then disable the interface after you have finished.

Prevent System Firmware Down-Level

Use the information in this topic to prevent system firmware from being changed to older firmware levels.

This feature allows you to decide whether or not to allow the system firmware to return to an older firmware level.

Click **Network** under **BMC Configuration** to prevent system firmware down-level

To enable of disable this feature, click **Network** under **BMC Configuration**. Any changes that are made will take effect immediately without the XClarity Controller requiring a restart.

Assert Physical Presence

Use the information in this topic to assert and de-assert Physical Presence from the XClarity Controller web page without being physically present at the server.

This feature is only available if the **Physical Presence Policy** is enabled through UEFI. Once enabled, you can access the physical presence feature by clicking **Security** under **BMC Configuration**.

Configuring the Security Key Lifecycle Manager (SKLM)

This topic provides information about the Security Key Lifecycle Manager (SKLM) software product that is used for creating and managing security keys.

The Security Key Lifecycle Manager (SKLM) is a software product for creating and managing security keys. The SKLM for ThinkSystem Self Encrypting Drives (SED) - Features on Demand (FoD) option is a ThinkSystem FoD option that enables centralized management of encryption keys. The encryption keys are used to gain access to data stored on SEDs in a ThinkSystem server.

A centralized SKLM (key repository) server provides the encryption keys to unlock the SEDs in the ThinkSystem server. The FoD option requires that a FoD Activation key be installed in the XClarity Controller FoD key repository. The Activation key for the FoD option is a unique identifier comprised of the machine type and serial number. To use the storage key/drive access functionality, the FoD key *ThinkSystem TKLM Activation for Secure Drive Encryption (Type 32796 or 801C)* must be installed in the XClarity Controller FoD key repository. See Chapter 8 “License Management” on page 85 for information pertaining to installing an activation key.

The SKLM FoD option is limited to ThinkSystem XClarity Controller-based servers. To increase security, the XClarity Controller can be placed in a separate management network. The XClarity Controller uses the network to retrieve encryption keys from the SKLM server; therefore, the SKLM server must be accessible to the XClarity Controller through this network. The XClarity Controller provides the communication channel between the SKLM server and the requesting ThinkSystem server. The XClarity Controller firmware attempts to connect with each configured SKLM server, stopping when a successful connection is established.

The XClarity Controller establishes communication with the SKLM server if the following conditions are met:

- A valid FoD activation key is installed in the XClarity Controller.
- One or more SKLM server host name/IP addresses are configured in the XClarity Controller.
- Two certificates (client and server) for communication with the SKLM server are installed in the XClarity Controller.

Note: Configure at least two (a primary and a secondary) SKLM servers for your device. If the primary SKLM server does not respond to the connection attempt from the XClarity Controller; connection attempts are initiated with the additional SKLM servers until a successful connection is established.

A Transport Layer Security (TLS) connection must be established between the XClarity Controller and the SKLM server. The XClarity Controller authenticates the SKLM server by comparing the *server* certificate submitted by the SKLM server, with the SKLM *server* certificate previously imported into the XClarity

Controller's trust store. The SKLM server authenticates each XClarity Controller that communicates with it and checks to verify that the XClarity Controller is permitted to access the SKLM server. This authentication is accomplished by comparing the *client* certificate that the XClarity Controller submits, with a list of trusted certificates that are stored on the SKLM server.

At least one SKLM server (key repository server) will be connected, and the device group is considered optional. The SKLM server certificate will need to be imported, while the client certificate needs to be specified. By default, the HTTPS certificate is used. If you wish to replace it, you can generate a new one.

Configuring the key repository servers

Use the information in this topic to create the host name or IP address and associated port information for the SKLM server.

The Key Repository Servers section consists of the following fields:

Host Name or IP address
Type the host name (if DNS is enabled and configured) or the IP address of the SKLM server in this field. Up to four servers can be added.

Port
Type the port number for the SKLM server in this field. If this field is left blank, the default value of 5695 is used. Valid port number values are 1 to 65535.

Configuring the device group

This topic contains information about the Device Group section .

A device group allows users to manage the self-encrypting drive (SED) keys on multiple servers as a group. A device group with the same name must also be created on the SKLM server.

The Device Group section contains the following field:

Device Group
A device group allows users to manage the keys for SEDs on multiple servers as a group. A device group with the same name must also be created on the SKLM server. The default value for this field is IBM_SYSTEM_X_SED.

Establishing certificate management

This topic provides information about client and server certificate management.

Client and server certificates are used to authenticate the communication between the SKLM server and the XClarity Controller located in the ThinkSystem server. Client and server certificate management are discussed in this section.

Client Certificate Management

This topic provides information about client certificate management.

Client certificates are classified as one of the following:

- An XClarity Controller self-assigned certificate.
- A certificate generated from an XClarity Controller certificate signing request (CSR) and signed (externally) by a third party CA.

A client certificate is required for communication with the SKLM server. The client certificate contains digital signatures for the CA and the XClarity Controller.

Notes:

- Certificates are preserved across firmware updates.
- If a client certificate is not created for communication with the SKLM server, the XClarity Controller HTTPS server certificate is used.
- The function of the CA is to verify the identity of the XClarity Controller.

To create a client certificate, click the plus icon ( ) and select one of the following items:

- Generate a New Key and a Self-Signed Certificate
- Generate a New Key and a Certificate Signing Request (CSR)

The **Generate a New Key and a Self-Signed Certificate** action item generates a new encryption key and a self-signed certificate. In the Generate New Key and Self-Signed Certificate window, type or select the information in the required fields and any optional fields that apply to your configuration, (see the following table). Click **OK** to generate your encryption key and certificate. A progress window displays while the self-signed certificate is being generated. A confirmation window is displayed when the certificate is successfully installed.

Note: The new encryption key and certificate replace any existing key and certificate.

Table 3. Generate a New Key and a Self-Signed Certificate

Two column table with headers documenting the required and optional fields for the Generate a new key and a self-signed certificate action. The bottom row spans across both columns.

Field	Description
Country[1]	From the list item, select the country where the BMC physically resides.
State or Providence[1]	Type the state or providence where the BMC physically resides.
City or Locality[1]	Type the city or locality where the BMC physically resides.
Organization Name[1]	Type the company or organization name that owns the BMC.
BMC Host Name[1]	Type the BMC host name that appears in the web address bar.
Contact Person	Type the name of the contact person that is responsible for the BMC.
Email address	Type the email address of the contact person responsible for the BMC.
Organization Unit	Type the unit within the company that owns the BMC.
Surname	Type the surname of the person responsible for the BMC. This field can contain a maximum of 60 characters.
Given Name	Type the given name of the person responsible for the BMC. This field can contain a maximum of 60 characters.
Initials	Type the initials of the person responsible for the BMC. This field can contain a maximum of 20 characters.
DN Qualifier	Type the Distinguished Name Qualifier for the BMC. This field can contain a maximum of 60 characters.
1. This is a required field.	

After the client certificate has been generated you can download the certificate to storage on your XClarity Controller by selecting the **Download Certificate** action item.

The **Generate a New Key and a Certificate Signing Request (CSR)** action item generates a new encryption key and a CSR. In the Generate a New Key and a Certificate Signing Request window, type or select the information in the required fields and any optional fields that apply to your configuration, (see the following table). Click **OK** to generate your new encryption key and CSR.

A progress window displays while the CSR is being generated and a confirmation window is displayed upon successful completion. After generation of the CSR, you must send the CSR to a CA for digital signing. Select the **Download Certificate Signing Request (CSR)** action item and click **OK** to save the CSR to your server. You can then submit the CSR to your CA for signing.

Table 4. Generate a New Key and a Certificate Signing Request

Two column table with headers documenting the required and optional fields for the Generate a new key and certificate signing request action. The bottom row spans across both columns.

Field	Description
Country[1]	From the list item, select the country where the BMC physically resides.
State or Providence[1]	Type the state or providence where the BMC physically resides.
City or Locality[1]	Type the city or locality where the BMC physically resides.
Organization Name[1]	Type the company or organization name that owns the BMC.
BMC Host Name[1]	Type the BMC host name that appears in the web address bar.
Contact Person	Type the name of the contact person that is responsible for the BMC.
Email address	Type the email address of the contact person responsible for the BMC.
Organization Unit	Type the unit within the company that owns the BMC.
Surname	Type the surname of the person responsible for the BMC. This field can contain a maximum of 60 characters.
Given Name	Type the given name of the person responsible for the BMC. This field can contain a maximum of 60 characters.
Initials	Type the initials of the person responsible for the BMC. This field can contain a maximum of 20 characters.
DN Qualifier	Type the Distinguished Name Qualifier for the BMC. This field can contain a maximum of 60 characters.
Challenge Password	Type the password to the CSR. This field can contain a maximum of 30 characters.
Unstructured Name	Type additional information, such as an unstructured name that is assigned to the BMC. This field can contain a maximum of 60 characters.
1. This is a required field.	

The CSR is digitally signed by the CA using the user's certificate processing tool, such as the *OpenSSL* or *Certutil* command line tool. All client certificates that are signed using the user's certificate processing tool have the same *base* certificate. This *base* certificate must also be imported to the SKLM server so that all servers digitally signed by the user are accepted by the SKLM server.

After the certificate has been signed by the CA you must import it into the BMC. Select the **Import a Signed Certificate** action item and select the file to upload as the client certificate; then, click **OK**. A progress window displays while the CA-signed certificate is being uploaded. A Certificate Upload window is displayed if the upload process is successful. A Certificate Upload Error window is displayed if the upload process is not successful.

Notes:

- For increased security, use a certificate that is digitally signed by a CA.
- The certificate that is imported into the XClarity Controller must correspond to the CSR that was previously generated.

After a CA-signed certificate is imported into the BMC, select the **Download Certificate** action item. When you select this action item, the CA-signed certificate is downloaded from the XClarity Controller to store on your system.

Server certificate management

This topic provides information about server certificate management.

The server certificate is generated in the SKLM server and must be imported into the XClarity Controller before the secure drive access functionality will work. To import the certificate that authenticates the SKLM server to the BMC, click **Import a Certificate** from the Server Certificate Status section of the Drive Access page. A progress indicator is displayed as the file is transferred to storage on the XClarity Controller.

After the server certificate is successfully transferred to the XClarity Controller, the Server Certificate Status area displays the following content: `A server certificate is installed.`

If you want to remove a trusted certificate, click the corresponding **Remove** button.

Extended Audit Log

Use the information in this topic to control extended audit log.

This feature allows you to decide whether or not to include the log entries of IPMI set command (raw data) from LAN and KCS channels into the audit log.

Click **Security** under **BMC Configuration** on XCC web to enable/disable extended audit log.

Note: If the IPMI set command is from LAN channel, user name and source IP address will be included in the log message. And all IPMI commands with sensitive security information (e.g. password) are excluded.

Configuring Call Home

Use the information in this topic to configure call home.

You can create a service forwarder that automatically sends service data for any managed device to Lenovo Support using the Call Home function.

Lenovo is committed to security. When enabled, Call Home automatically contacts Lenovo to open a service ticket and sends in service data collected from a managed device whenever that device reports a hardware failure. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later, your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel.

Entering the call home page for the first time

When entering the Call Home page for the first time, you'll see a warning window, click on "View Terms and Conditions" to continue.

Attention: You must accept the **Lenovo Privacy Statement** before you can transfer data to Lenovo Support. This action only needs to be once when first enter the page.

Note: You can find "View Terms and Conditions" and **Lenovo Privacy Statement** on top of the page to review them anytime.

Configure Call Home

There are nine required fields to be filled in:

- Country
- Contact Name
- Phone
- Email
- Postal Code
- Company Name
- Address
- City
- State/Province

Attention: All the required fields must be filled in or you won't be able to apply the changes and enable **Reporting to Lenovo Service**.

Ticket Status

Each ticket can have the one of the five status:

- **Pending:** The service information is being sent or waiting for response.
- **Active:** The service information was sent successfully and the problem is currently being processed.
- **Failed:** The service information was not sent successfully.
- **Closed:** The problem has been processed and closed.
- **Cancelled:** The problem has been processed and cancelled.

Test Call Home

You can test call home function by click on "Test Call Home", a message will display on top of the page to indicate whether the operation was successful. And you will be able to check the event log below for test result.

- **Action — Cancel:** When a ticket's status is "Active", you can click the "Undo" icon in the "Action" column to cancel the ticket.
- **Action — Note:** When you click the "Note" icon in the "Action" column, you'll be prompted to leave notes for the corresponding event.

  Note: Both Title and Message Body must be filled in to be sent successfully. This function **ONLY sends information to the server**. It is not for saving and displaying the information. If you click Note again, you'll be prompted with a new Note window to leave another message.

Attention: To successfully Call Home, please ensure that DNS settings are valid and a connection exists to the Internet address required by Call Home. If XClarity Controller access the Internet through an HTTP proxy, ensure that the proxy server is configured to use basic authentication and is set up as a non-terminating proxy.

HTTP Proxy

HTTP Proxy serves two intermediary roles as an HTTP Client and an HTTP Server for security, management, and caching functionality. The HTTP Proxy routes HTTP Client requests from a Web browser to the Internet, while supporting the caching of Internet data.

- **Proxy Server Address:** This field is required to enable the HTTP Proxy. It can only accept a maximum of 63 characters, allowing users to specify IP address or hostname. The host name only contains alphanumeric, hyphen ('-'), and underscore ('_') characters.
- **Port:** This field is required to specify the port of the HTTP Proxy. This field only allows numbers to be entered, ranging from 1-65535.
- **Test Proxy:** To enable this feature, you need to fill in the correct Proxy Location and Proxy Port to test whether the current HTTP Proxy function is available.
- **User Name:** If the'**Requires authentication** option is checked, the username will be required and represent a proxy credential. This field allows a maximum length of 30 characters and spaces are invalid.
- **Password:** This field is optional and will be displayed if the 'Requires authentication' option is checked. This field allows a maximum length of 15 characters and spaces are invalid.

Backing up and Restoring the BMC configuration

The information in this topic describes how to restore or modify the BMC configuration.

Select **Backup and Restore** under **BMC Configuration** to perform the following actions:

- View management controller configuration summary
- Backup or restore the management controller configuration
- View backup or restore status
- Reset the management controller configuration to its factory default settings
- Access the management controller initial setup wizard

Backing up the BMC configuration

The information in this topic describes how to back up the BMC configuration.

Select **Backup and Restore** under **BMC Configuration**. At the very top is the **Backup BMC configuration** section.

If a backup was previously made, you will see the details in the **Last backup** field.

To backup the current BMC configuration, follow the steps shown below:

1. Specify the password for the BMC backup file.
2. Select if you wish to encrypt the whole file or only sensitive data.
3. Begin the backup process by clicking **Start Backup**. During the process, you are not allowed to perform any restore/reset actions.
4. When the process is completed, a button will appear to let you download the and save the file.

Note: When the user sets up a new XClarity Controller user/password and performs a backup of the configuration, the default account/password (USERID/PASSWORD) is included as well. Subsequently deleting the default account/password from the backup will result in the system showing a message notifying the user that there is a failure in restoring the XClarity Controller account/password. Users can ignore this message.

Restoring the BMC configuration

The information in this topic describes how to restore the BMC configuration.

Select **Backup and Restore** under **BMC Configuration**. Located below **Backup BMC Configuration** is the **Restore BMC from Configuration File** section.

To restore the BMC to a previously saved configuration, follow the steps shown below:

1. Browse to select the backup file and input the password when prompted.
2. Verify the file by clicking **View content** to view the details.
3. After verifying the content, click **Start Restore**.

Resetting the BMC to Factory Default

The information in this topic describes how to reset the BMC to the factory default settings.

Select **Backup and Restore** under **BMC Configuration**. Located below **Restore BMC from Configuration File** is the **Reset BMC to factory default** section.

To reset the BMC to factory defaults, follow the steps shown below:

1. Click **Start to Reset BMC to Factory Defaults**.

   Notes:

   - Only users with Supervisor user authority level can perform this action.
   - The Ethernet connection is temporarily disconnected. You must log in the XClarity Controller web interface again after the reset operation is completed.
   - Once you click **Start to Reset BMC to Factory Defaults**, all previous configuration changes will be lost. If you wish to enable LDAP when restoring the BMC configuration, you will need to first import a trusted security certificate before doing so.
   - After the process is completed, the XClarity Controller will be restarted. If this is a local server, your TCP/IP connection will be lost and you may need to reconfigure the network interface to restore connectivity.
   - Resetting the BMC to Factory Default is not affecting UEFI settings.

Restarting the XClarity Controller

The information in this topic explains how to restart your XClarity Controller.

For details on how to restart the XClarity Controller, see “Power actions” on page 58

Chapter 4. Monitoring the server status

Use the information in this topic to understand how to view and monitor information for the server that you are accessing.

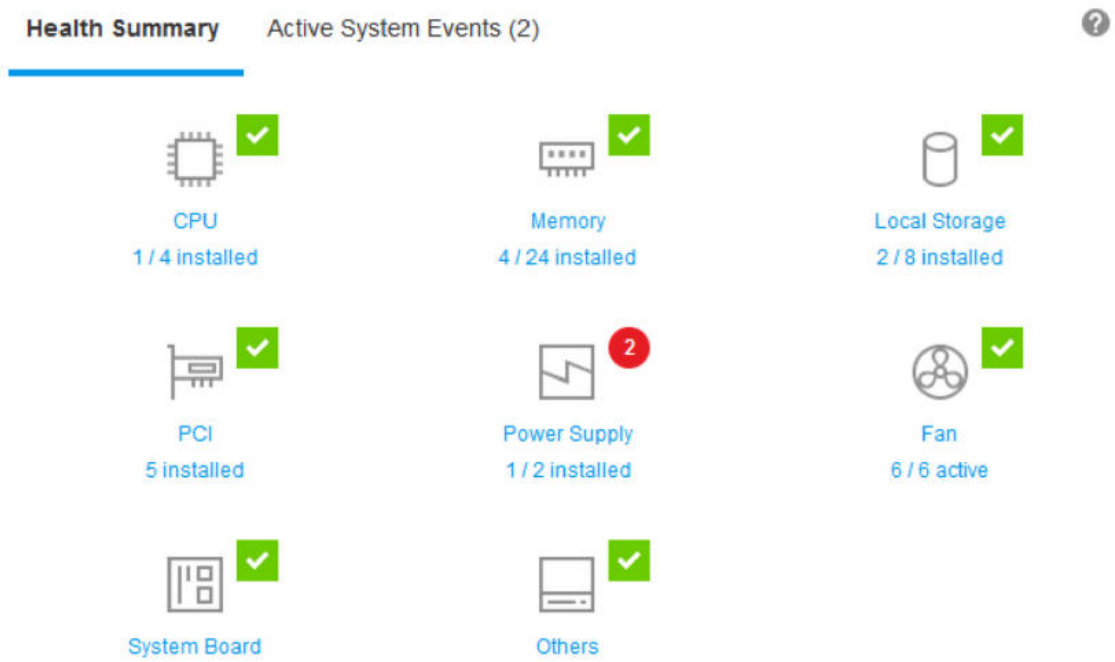
Once you log into the XClarity Controller, a system status page will be displayed. From this page, you can view the server hardware status, event and audit logs, system status, maintenance history and alert recipients.

Viewing the Health Summary/Active System Events

Use the information in this topic to understand how to view the Health Summary/Active System Events.

When you access the XClarity Controller homepage, the **Health Summary** is shown by default. A graphical representation is given, which shows the number of hardware components that have been installed and their respective health status. The hardware components that are being monitored include the following:

- Processor (CPU)
- Memory
- Local Storage
- PCI Adapters
- Power Supply
- Fan
- System Board
- Others



© Copyright Lenovo 2017, 2020

If any of the hardware components is not operating normally, it will be marked by a critical or warning icon. A critical condition is indicated by a red circle icon, while a warning condition is indicated by a yellow triangle icon. By hovering the mouse icon over the critical or warning sign, up to three currently active events for that component will be shown.



To view the other events, click the **Active System Events** tab. A window will appear showing the events that are currently active in the system. Click **View all event logs** to view the entire event history.

If the hardware component is marked by a green check mark, it is operating normally, and there are no active events.

The text underneath the hardware component states the number of components installed. If you click the text, you will be directed to the **Inventory** page.

Viewing the System Information

This topic explains how to obtain a summary of common server information.

The **System Information and Settings** pane located to the left of the home page provides a summary of common server information, which includes the following:

- Machine name, power and operating system state
- Machine Type-Model
- Serial number
- System name
- Front USB ownership
- BMC license
- BMC IP address
- BMC host name
- UEFI version
- BMC version
- LXPM version
- Location

The server can be in one of the system states listed in the following table.

Table 5. System state descriptions

Two column table with headers documenting the system states of the server.

Table 5. System state descriptions (continued)

State	Description
System power off/State unknown	The server is powered off.
System on/starting UEFI	The server is powered on; but, UEFI is not running.
System running in UEFI	The server is powered on and UEFI is running.
System stopped in UEFI	The server is powered on; UEFI has detected a problem and has stopped running.
Booting operating system or in unsupported operating system	The server might be in this state for one of the following reasons: • The operating system loader has started; but, the operating system is not running • The BMC Ethernet over USB interface is disabled. • The operating system does not have the drivers loaded that support the Ethernet over USB interface.
Operating system booted	The server operating system is running.
Suspend to RAM	The server has been placed in standby or sleep state.
System running in memory test	The server is powered on and running memory diagnostic tools.
System running in Setup	The server is powered on and the system has booted into UEFI F1 setup menu or LXPM menu.
System running in LXPM maintenance mode	The server is powered on and the system has booted into the LXPM maintenance mode under which users can't navigate through the LXPM menu.

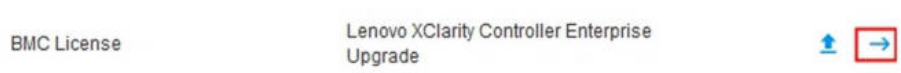
If you wish to change the system name, click the pencil icon. Type the system name you wish to use; then, click the green checkmark.

If you wish to change the front USB ownership, click the pencil icon and select the **Front USB Ownership** mode that you wish from the drop-down menu. Then, click the green checkmark.

If your server has a license other than the XClarity Controller Enterprise license, you may be able to purchase a license upgrade to enable enhanced features. To install the upgrade license after you have obtained an upgrade license, click the upward-pointing arrow icon.



To add, delete or export a license, click the rightward-pointing arrow icon.



To change the relevant settings for the BMC IP address, BMC host name, UEFI version, BMC version and location items, click the right-ward pointing arrow.

- For the IP address and host name, you will be led to the **Ethernet Configuration** section under **Network**.
- For the UEFI and BMC version items, you will be led to the **Firmware Update** page.

- For the location item, you will be led to the **Server Properties** section on the **Server Configuration** page.



Viewing the System Utilization

By clicking **Utilization** in the left pane, a summary of common server utilization information is provided.

System utilization is a composite metric based on the real-time utilization of processor, memory, and I/O subsystems. The utilization data are all coming from the ME(Node manager) side, which includes the following:

- **CPU Utilization**
  - Aggregated C-State Residency
  - Measured time in C0 as a percentage of the used and max C0 residency (per second).
- **Memory Utilization**
  - Aggregated R/W volume of all Memory Channels.
  - Measured bandwidth calculated as a percentage of the used and max memory bandwidth available (per second).
- **I/O Utilization**
  - Aggregated R/W volume of Root Ports in the PCIe* Bus.
  - Measured bandwidth calculated as a percentage of the used and max I/O bandwidth available (per second).

Viewing Event Logs

The **Event Log** provides a historical list of all hardware and management events.

Select the **Event Log** tab in **Events** to display the **Event Log** page. All events in the log are time stamped, using the XClarity Controller date and time settings. Some events also generate alerts when they occur, if they are configured to do so in **Alert Recipients**. You can sort and filter events in the event log.

The following is a description of the actions that can be performed in the **Event Log** page.

- **Customize table**: Select this action item to choose the type of information you wish to display in the table. A sequence number can be displayed to assist in determining the order of events when more than one event has the same timestamp.

  Note: Some sequence numbers are used by internal BMC processes, so it is normal that there may be gaps in the sequence numbers when the events are sorted by sequence number.
- **Clear logs**: Select this action item to delete the event logs.
- **Refresh**: Select this action item to update the display with any event log entries that may have occurred since the page was last displayed.

- **Type**: Select which event types to show. The event types include the following:

  
  Shows Error entries in the log

  
  Shows Warning entries in the log

  
  Shows Informational entries in the log

  Click each icon to turn off or on the types of errors to be displayed. Clicking the icon successively will toggle between showing and not showing the events. A blue box surrounding the icon indicates that type of event will be displayed.
- **Source type filter**: Select an item from the drop-down menu to display only the type of event log entries that you wish to be shown.
- **Time filter**: Select this action item to specify the interval of the events that you want to show.
- **Search**: To search for specific types of events or keywords, click the magnifying glass icon, and type a word to search for in the **Search** box. Note that the input is case-sensitive.

Note: The maximum number of event log records is 1024. When the event logs are full, the new log entry will automatically overwrite the oldest one.

Viewing Audit Logs

The **Audit Log** provides a historical record of user actions, such as logging in to the XClarity Controller, creating a new user, and changing a user password.

You can use the audit log to track and document authentication, changes, and system actions.

Both the event log and the audit log support similar maintenance and viewing actions. To see the description of the display and filtering actions that can be performed on the Audit Log page, see “Viewing Event Logs” on page 50.

Notes:

- After running Lenovo’s tools on your server operating system, the Audit Log may contain records showing actions performed by a username (for example user “20luN4SB”) that you may not recognize. When some of the tools are run on the server operating system, they may create a temporary user account for accessing the XClarity Controller. The account is created with a random username and password and can only be used to access the XClarity Controller on the internal Ethernet over USB interface. The account can only be used to access the XClarity Controller CIM-XML and SFTP interfaces. The creation and removal of this temporary account is recorded in the audit log as well any actions performed by the tool with these credentials.
- The maximum number of audit log records is 1024. When the audit logs are full, the new log entry will automatically overwrite the oldest one.

Viewing the Maintenance History

The **Maintenance History** page includes information about the firmware update, configuration and hardware replacement history.

The contents of the maintenance history can be filtered to display certain types of events or certain intervals of time.

Note: The maximum number of maintenance history records is 250. When the maintenance history logs are full, the new log entry will automatically overwrite the oldest one.

Configuring Alert Recipients

To add and modify email and syslog notifications or SNMP TRAP recipients, use the information in this topic.

The following is a description of the actions that can be performed in the **Alert Recipients** tab.

The following actions items can be performed in the **Email/Syslog** recipients section.

- **Create**: Select this action item to create additional new Email recipients and Syslog recipients. Up to 12 Email and Syslog recipients can be configured.
  - **Create Email Recipient**: Select this action item to create an Email recipient.
    - Enter the name and email address of the recipient.
    - Select to enable or disable the event notification. If disable is selected, the account will remain configured, but no emails will be sent.
    - Select the types of events that the recipient will be notified of. If you click the drop-down next to the Critical, Attention, or System category labels you can select or deselect notifications for specific components in the category.
    - You can choose whether or not to have the event log contents included in the email alert.
    - The index specifies which of the 12 recipient slots is assigned.
    - You can configure the email server to which the events will be forwarded here or by clicking the SMTP Server action at the top of the section. See SMTP Server below for configuration details.
  - **Create Syslog Recipient**: Select this action item to create syslog recipients.
    - Enter the name and IP address or host name of the Syslog server.
    - Select to enable or disable the event notification. If disable is selected, the account will remain configured but no emails will be sent.
    - The index specifies which of the 12 recipient slots is assigned.
    - Select the types of events that will be sent to the Syslog server. If you click the drop-down menu next to the Critical, Attention, or System category labels you can select or deselect notifications for specific components in the category.
- **SMTP Server**: Select this action item to configure the relevant settings for the SMTP Email server. Only one email server can be configured. The same email configuration is used when sending alerts to all of the configured email recipients. The BMC automatically upgrades a plain text connection to an encrypted connection for mail transfer if the designated mail server supports STARRTLS.
  - Enter the host name or IP address and network port number of the Email server.
  - If the Email server requires authentication, select the **Require Authentication** check box and enter the username and password. Select the type of authentication that is required by the Email server, either a challenge-response method (**CRAM-MD5**) or simple credentials (**LOGIN**).
  - Some networks may block outgoing emails if the reverse path value is not as expected. By default, the XClarity Controller will use alertmgr@domain, where the domain is the Domain name as specified in the DDNS section of the XClarity Controller network web page. You can specify your own sender information in place of the default.

  - You can test the connection to the Email server to ensure that the email settings have been configured correctly. The XClarity Controller will display a message indicating whether or not the connection is successful.
- **Retry and Delay**: Select this action item to configure the relevant settings for the retry and delay options.
  - The retry limit specifies the number of times that the XClarity Controller will attempt to send an alert if the initial attempt did not succeed.
  - The delay between entries specifies the amount of time that the XClarity Controller will wait after sending an alert to one recipient before sending an alert to the next recipient.
  - The delay between attempts specifies the amount of time that the XClarity Controller will wait after a failed attempt before retrying to send the alert.
- **Protocol**: Select this action item to configure the relevant settings for connection protocol.
  - You can choose between **TCP Protocol** or **UDP Protocol**, please note that this setting will apply to all syslog recipients.
- If Email or Syslog Recipients have been created, they will be listed in this section.
  - To edit the settings for an Email or Syslog Recipient click the pencil icon below the action header on the row next of the recipient that you wish to configure.
  - To delete an Email or Syslog Recipient click the trash can icon.
  - To send a test alert to an Email or Syslog Recipient, click the paper airplane icon.

The following actions can be performed in the **SNMPv3** user segment.

- **Create**: Select this action item to create SNMPv3 TRAP recipients.
  - Select the user account that is to be associated with the SNMPv3 TRAPs. The user account must be one of the twelve local user accounts.
  - Specify the host name or IP address of the SNMPv3 manager that will receive the SNMPv3 TRAPs.
  - The XClarity Controller uses the HMAC-SHA hash algorithm to authenticate with the SNMPv3 manager. This is the only algorithm supported.
  - The privacy password is used with the privacy protocol to encrypt the SNMP data.
  - The **SNMPv3 global setting** applies to all SNMPv3 TRAP recipients. These settings can be configured while creating an SNMPv3 TRAP recipient or by clicking the SNMPv3 Settings action at the top of the **SNMPv3** user segment.
    - Select to enable or disable SNMPv3 TRAPs. If disabled, the settings will remain configured but no SNMPv3 TRAPs will be sent.
    - The BMC Contact and Location information is required and is configured on the Server Properties web page. See “Setting Location and Contact” on page 75 for more information.
    - Select the types of events that will be cause TRAPs to be sent to the SNMPv3 manager. If you click the drop-down menu next to the Critical, Attention, or System category labels you can select or deselect notifications for specific components in the category.

  Note: Data transfer between the SNMP client and the agent can be protected using encryption. The supported methods for **privacy protocol** are CBC-DES and AES.
- If SNMPv3 TRAP recipients have been created, they will be listed in this section.
  - To edit the settings for a SNMPv3 recipient, click the pencil icon below the action header on the row next of the recipient that you wish to configure.
  - To delete a SNMPv3 recipient, click the trash can icon.

Capturing the latest OS failure screen data

Use the information in this topic to capture and view an operating system failure screen.

The operating system screen is automatically captured when the OS Watchdog timeout occurs. If an event occurs that causes the OS to stop running, the OS Watchdog feature is triggered and the screen contents are captured. The XClarity Controller stores only one screen capture. When the OS Watchdog timeout occurs, a new screen capture overwrites the previous screen capture. The OS Watchdog feature must be enabled to capture the OS failure screen. To set the OS Watchdog Time, see “Setting server timeouts” on page 76 for more information. The OS failure screen capture feature is available only with the XClarity Controller Advanced or Enterprise Level of functionality. See the documentation for your server for information about the level of XClarity Controller functionality that is installed in your server.

Click the **Latest Failure Screen** action in the **Remote Console** section of the XClarity Controller home page to view an image of the operating system display that was captured when the OS Watchdog timeout occurred. The capture can also be viewed by clicking **Service,** then **Latest Failure Screen** in the **Quick Action** section of the home page. If the system has not experienced an OS Watchdog timeout and captured the OS screen, a message indicating that the failure screen has not been created is displayed.

Chapter 5. Configuring the Server

Use the information in this chapter to understand the options available for server configurations.

When configuring the server, the following options are available:

- Adapters
- Boot options
- Power policy
- Server properties

Viewing the adapter information and configuration settings

Use the information in this topic to view information about the adapters installed in the server.

Click **Adapters** under **Server Configuration** to view information about the adapters installed in the server.

Notes:

- If the adapter does not support status monitoring, it will not be visible for monitoring or configuration. For inventory related information of all the installed PCI adapters, refer to the **Inventory** page.

Configuring system boot mode and order

To configure the system boot mode and order, use the information in this topic.

When you select **Boot Options** under **Server Configuration** , you can configure the system boot mode and order.

Note: No unauthenticated in-band method is allowed to change security related system settings. For example, Secure Boot must NOT be able to configure over unauthenticated in-band APIs from the OS or UEFI shell. This includes OneCLI running in-band and obtaining temporary credentials using IPMI, or any tools and APIs to configure Secure Boot, TPM, UEFI Setup password related settings. All security related settings must require proper authentication with sufficient privilege.

For the system boot mode, the following two options are available:

UEFI Boot
Select this option to configure a server that supports Unified Extensible Firmware Interface (UEFI). If you are booting UEFI-enabled operating systems, this option might shorten boot time by disabling legacy option ROMs.

Legacy Boot
Select this option if you are configuring a server to boot an operating system that requires legacy (BIOS) firmware. Select this option only if you are booting non-UEFI enabled operating systems.

To configure the system boot order, select a device from the list of **Available devices** and click the right arrow to add the device to the boot order. To remove a device from the boot order, select a device from the boot order list and click the left arrow to move the device back to the list of available devices. To change the boot order, select a device and click the up or down arrow to move the device up or down in priority.

When you make a change to the boot order, you must select a restart option before applying the change. The following options are available:

© Copyright Lenovo 2017, 2020

- **Restart server immediately**: The boot order changes are saved and the server is restarted immediately without shutting down the operating system.
- **Restart server normally**: The boot order changes are saved and the operating system is shutdown before restarting the server.
- **Manually restart later**: The boot order changes will be saved, but will not take effect until the next time the server is rebooted.

Configuring one-time boot

To temporarily ignore the configured boot and instead boot to a specified device one time, use the information in this topic.

Click **Boot Options** under **Server Configuration** and select a device from the drop-down menu to configure the device that the system will boot to one-time on the next server restart. The following choices are available:

PXE network
Sets up your server to attempt a Preboot Execution Environment network boot.

Primary removable media
The server is booted from the default USB device.

Default CD/DVD
The server is booted from the default CD/DVD drive.

F1 system setup
The server is booted into the Lenovo XClarity Provisioning Manager.

Diagnostic Partition
The server is booted into the Diagnostics section of the Lenovo XClarity Provisioning Manager.

Default Hard Disk
The server is booted from the default disk drive.

Primary remote media
The server is booted from the mounted virtual media.

No one-time boot
The configured boot order is used. There is no one-time boot override of the configured boot order.

When you change the type of boot to be performed with the one-time boot device, you can also specify the boot to be a legacy boot or a UEFI boot. Click the **Prefer Legacy Boot** check box if you would like the boot to be a legacy BIOS boot. Uncheck the box if would like a UEFI boot. When you select a one-time change to the boot order, you must select a restart option before applying the change.

- **Restart server immediately**: The boot order change is saved and the server is restarted immediately without shutting down the operating system.
- **Restart server normally**: The boot order change is saved and the operating system is shutdown before restarting the server.
- **Manually restart later**: The boot order change is saved, but will not take effect until the next time the server is rebooted.

Managing the server power

To view power management information and perform power management functions, use the information in this topic.

Select **Power Policy** under **Server Configuration** to view power management information and perform power management functions.

Note: In a chassis containing blade or high-density server nodes, the chassis cooling and power is controlled by the chassis management controller instead of the XClarity Controller.

Configuring the power redundancy

To configure the power redundancy, use the information in this topic.

Note: The AMD processor servers do not support the configuration of power redundancy.

Available fields in the Power Redundancy section include the following:

- **Redundant (N+N)**: In this mode, the server will remain operational in the event of a loss of one power supply.
  - **Zero Output Mode**: Once enabled under Redundant configuration, some PSUs will automatically enter into standby state under light load conditions. In this manner, the remaining PSU delivers the entire power load to increase efficiency.
- **Redundant (N+1)**: In this mode, the server will remain operational in the event of a loss of one power supply when four power supplies are installed.
- **Non-redundant mode**: In this mode, the server is not guaranteed to remain operational if a power supply is lost. The server will throttle if a power supply fails in an attempt to remain running.

Click **Apply** after making the configuration changes.

Configuring the power capping policy

To configure the power capping policy, use the information in this topic.

Note: The AMD processor servers do not support users to configure the power capping policy function.

You can choose to enable or disable the power capping function. If power capping is enabled, a selection can be made to limit the amount of power used by the server. If power capping is disabled, the maximum power used by the server is determined by the Power Redundancy policy. To change the setting, first click **Reset**. Choose your preferred setting; then, click **Apply**.

Power capping can be enabled using AC power consumption measurements or DC power consumption measurements. From the drop-down menu, select the type of measurements that will be used to determine the power capping limit. When switching between AC and DC, the number on the slider will change accordingly.

There are two ways to change the power capping value:

- **Method 1**: Move the slider mark to the desired wattage to set the overall server power limit.
- **Method 2**: Input the value in the input box. The slider mark will automatically move to the corresponding position.

Click **Apply** after making the configuration changes.

Note: The **Power Policies** option is not available when the XClarity Controller is in a chassis containing blade or high-density server nodes. The power policy is controlled by the chassis management controller instead of the XClarity Controller.

Configuring the power restore policy

To configure how the server reacts when the power is restored after a power loss, use the information in this topic.

When configuring the power restore policy, the following three options are available:

Always Off
The server will remain powered off even when power is restored.

Restore
The server will automatically be powered on when power is restored if the server was powered on at the time that the power failure occurred. Otherwise, the server power will remain off when power is restored.

Always On
The server will automatically power on when power is restored.

Click **Apply** after making the configuration changes.

Note: The **Power Restore Policies** option is not available in a chassis containing blade or high-density server nodes. The power restore policy is controlled by the chassis management controller instead of the XClarity Controller.

Power actions

See the information in this topic to understand the power actions that can be made to the server.

Click **Power Action** in the **Quick Action** section of the XClarity Controller homepage.

The following table contains a description of the power and restart actions that can be performed on the server.

Table 6. Power actions and descriptions

Two column table containing descriptions of the server power and restart actions.

Power Action	Description
Power on server	Select this action item to power on the server and boot the operating system.
Power off server normally	Select this action item to shut down the operating system and power off the server.
Power off server immediately	Select this action item to power off the server without first shutting down the operating system.
Restart server normally	Select this action item to shut down the operating system and power cycle the server.
Restart server immediately	Select this action item to power cycle the server immediately without first shutting down the operating system.
Boot server to system setup	Select this item to power on or reboot the server and automatically boot into system setup without needing to press F1 during boot.

Table 6. Power actions and descriptions (continued)

Power Action	Description
Trigger non-maskable interrupt (NMI)	Select this action item to force a Non-maskable Interrupt (NMI) on a “hung” system. Selection of this action item allows the platform operating system to perform a memory dump that can be used for debug purposes of the system hang condition. The auto reboot on NMI setting from the F1 system setup menu determines whether or not the XClarity Controller will reboot the server after the NMI.
Schedule power actions	Select this action item to schedule daily and weekly power and restart actions for the server.
Restart management controller	Select this action item to restart the XClarity Controller
AC Power Cycle Server	Select this action to power cycle the server.
Note: If the operating system is in the screen saver or locked mode when a shutdown of the operating system is attempted, the XClarity Controller might not be able to initiate a normal shutdown. The XClarity Controller will perform a hard reset or shutdown after the power off delay interval expires, while the operating system might still be running.	

Managing and monitoring power consumption with IPMI commands

Use the information in this topic to manage and monitor power consumption using IPMI commands.

This topic describes how the Intel Intelligent Power Node Manager and the Data Center Manageability Interface (DCMI) can be used to provide power and thermal monitoring and policy-based power management for a server using Intelligent Platform Management Interface (IPMI) power management commands.

For servers using Intel Node Manager SPS 3.0, XClarity Controller users can use IPMI power management commands provided by Intel's Management Engine (ME) to control the Node Manager features and to monitor server power consumption. Server power management can also be accomplished using DCMI power management commands. Example Node Manager and DCMI power management commands are provided in this topic.

Managing the server power using Node Manager commands

Use the information in this topic to manage the server power using the Node Manager.

The Intel Node Manager firmware does not have an external interface; therefore, the Node Manager commands must first be received by the XClarity Controller and then sent to the Intel Node Manager. The XClarity Controller functions as a relay and a transport device for the IPMI commands using standard IPMI bridging.

Note: Changing Node manager policies using Node Manager IPMI commands might create conflicts with the XClarity Controller power management functionality. By default, bridging of the Node Manager commands is disabled to prevent any conflict.

For users who want to manage the server power using the Node Manager instead of the XClarity Controller, an OEM IPMI command consisting of (network function: *0x3A*) and (command: *0xC7*) is available for use.

To enable native Node Manager IPMI commands type:`ipmitool -H` <*$XClarity_Controller_IP*> `-U` <*USERID*> `-P` <*PASSW0RD*> `raw` *0x3a 0xc7 0x01*

To disable native Node Manager IPMI commands type:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x3a 0xc7 0x00`

The following information are examples of Node Manager power management commands.

Notes:

- By specifying IPMI *channel 0* and a target address of *0x2c*, you can use the IPMITOOL to send commands to the Intel Node Manager for processing. A request message is used to initiate an action and a response message is returned to the requester.
- Commands are displayed in the following format due to space limitations.

Power monitoring using the Get Global System Power Statistics, (command code 0xC8): Request: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> -b 0x00 -t 0x2c raw 0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00` Response:57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Power capping using the Set Intel Node Manager Policy, (command code 0xC1): Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00`Response:57 01 00

Power savings using the Set Intel Node Manager Policy, (command code 0xC1): Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00`

Get device ID function using the Get Intel Management Engine Device ID: Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> -b 0x00 -t 0x2c raw 0x06 0x01`Response:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

For additional Intel Node Manager commands, see the latest release of the *Intel Intelligent Power Node Manager External Interface Specification Using IPMI* at https://businessportal.intel.com.

Managing the server power using DCMI commands

Use the information in this topic to manage the server power using DCMI commands.

The DCMI provides monitoring and control functions that can be exposed through standard management software interfaces. Server power management functions can also be accomplished using DCMI commands.

The following information are examples of commonly used DCMI power management functions and commands. A request message is used to initiate an action and a response message is returned to the requester.

Note: Commands are displayed in the following formats due to space limitations.

Get Power Reading: Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x02 0xdc 0x01 0x00 0x00` Response:`dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40`

Set Power Limit: Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P PASSW0RD raw 0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03` Response:`dc`

Get Power Cap: Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x03 0xdc 0x00 0x00` Response:`dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00`

Activate the Power Limit: Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x05 0xdc 0x01 0x00 0x00` Response:`dc`

Deactivate the Power Limit: Request:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x05 0xdc 0x00 0x00 0x00` Response:`dc`

Note: On some servers, the Exception Actions for the **Set Power Limit** command might not be supported. For example, the *Hard Power Off system and log events to SEL* parameter might not be supported.

For the complete list of commands that are supported by the DCMI specification, see the latest release of the *Data Center Manageability Interface Specification* at https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf.

Remote Console Functionality

Use the information in this topic to understand how to remotely view and interact with the server console.

You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console. You can assign a disk image (ISO or IMG file) as a virtual drive on the server. The remote console functionality is available with the XClarity Controller Advanced and XClarity Controller Enterprise features and is only available through the web interface. You must log in to the XClarity Controller with a user ID that has Supervisor access or Remote Console Access privileges to use the remote console features. For more information about upgrading from XClarity Controller Standard to XClarity Controller Advanced or XClarity Controller Enterprise, see “Upgrading XClarity Controller” on page 6.

Use the remote console features to do the following:

- Remotely view video with graphic resolution up to 1280 x 1024 at 72 or 75Hz, regardless of the server state.
- Remotely access the server using the keyboard and mouse from a remote client.
- Mount ISO and IMG files that are located on your local system or on a remote system as virtual drives that are available for use by the server.
- Upload an IMG or ISO image to the XClarity Controller memory and mount it to the server as a virtual drive. Up to two files with a maximum total size of 50 MB may be uploaded into the XClarity Controller memory.

Notes:

- When the remote console feature is started in multi-user mode, (the XClarity Controller with the XClarity Controller Enterprise feature set supports up to six simultaneous sessions), the remote disk feature can be exercised by only one session at a time.
- The remote console is able to display only the video that is generated by the video controller on the system board. If a separate video controller adapter is installed and is used in place of the system's video controller, the XClarity Controller remote console cannot display the video content from the added adapter.
- If you have firewalls in your network, a network port must be opened to support the remote console feature. To view or change the network port number used by the remote console feature, see “Service Enablement and Port Assignment” on page 33.
- The remote console feature uses HTML5 for displaying the server video on web pages. To use this feature your browser must support displaying video content using HTML5 elements.
- If you are using self-signed certificates and an IPv6 address to access the BMC with the Internet Explorer browser, the remote console session may fail to start due to a certificate error. To avoid this issue, the self-signed certificate can be added to the Internet Explorer Trust Root certificate Authorities:
  - Select **Security** under **BMC Configuration** and download the self-signed certificate.
  - Change certificate file extension to *.crt and double-click the Web certificate file.

– Clear IE11 browser cache.
– Click **Install Certificate** to install the certificate to the Certificate Store by following the Certificate Import Wizard steps.

Enabling the remote console functionality

This topic provides information about the remote console functionality.

As mentioned earlier, the XClarity Controller remote console functionality is available only in the XClarity Controller Advanced and XClarity Controller Enterprise features. If you do not have the privilege to operate the remote console, you will see a lock icon.

After you have purchased and obtained the activation key for the XClarity Controller Advanced upgrade install it using the instructions under “Installing an activation key” on page 85.

To use the remote console functionality, complete the following steps:

1. Click the image with a white diagonally pointing arrow in the Remote Console section of the XClarity Controller homepage or the Remote Console web page.
2. Select one of the following modes:
   - Start remote console in single-user mode
   - Start remote console in multiuser mode

   Note: The XClarity Controller with XClarity Controller Enterprise feature set supports up to six simultaneous video sessions in the multiuser mode.
3. Select whether or not to allow others to request to send a disconnection request to a remote console user when someone wishes to use the remote console feature and the feature is already in use in Single User Mode, or when the maximum number of users are using the remote console feature in Multi User Mode. The **No response time interval** specifies how long the XClarity Controller will wait before automatically disconnecting the user if no response is received to the disconnection request.
4. Select whether or not to allow record the latest three server boot videos.
5. Click **Launch Remote Console** to open the remote console page in another tab. When all possible remote console sessions are in use, a dialog box will pop up. From this dialog box, the user can send a disconnection request to a remote console user who has enabled the setting to **Allow others to request my remote session disconnect**. The user can accept or deny the request to disconnect. If the user does not respond within the interval specified by the **No response time interval** setting, the user session will automatically be ended by the XClarity Controller.

Remote power control

This topic explains how to send server power and restart commands from the remote console window.

You can send server power and restart commands from the remote console window without returning to the main web page. To control the server power with the remote console, click **Power** and select one of the following commands:

Power On Server
Select this action item to power on the server and boot the operating system.

Power Off Server Normally
Select this action item to shut down the operating system and power off the server.

Power Off Server Immediately
Select this action item to power off the server without first shutting down the operating system.

Restart Server Normally
Select this action item to shut down the operating system and power cycle the server.

Restart Server Immediately
Select this action item to power cycle the server immediately without first shutting down the operating system.

Boot Server to System Setup
Select this item to power on or reboot the server and automatically boot into system setup without needing to press F1 during boot.

Remote console capture screen

Use the information in this topic to understand how to use the remote console screen capture feature.

The screen capture feature in the remote console window captures the video display contents of the server. To capture and save a screen image, complete the following steps:

Step 1. In the remote console window, click **Capture Screen**.

Step 2. In the pop-up window, click **Save File** and press **OK**. The file will be named rpviewer.png and will be saved to your default download folder.

Note: The screen capture image is saved as a PNG file type.

Remote console keyboard support

In the remote console window under **Keyboard**, the following option items are provided:

- Click **Virtual Keyboard** to launch the virtual keyboard. This feature is useful if you are using a tablet device that does not have a physical keyboard. The following options can be used to create macros and key combinations that can be sent to the server. The operating system on the client system that you are using may trap certain key combinations (for example Ctrl+Alt+Del) instead of transmitting them to the server. Other keys, such as F1 or Esc, may be intercepted by the program or browser that you are using. Macros provides a mechanism to send keystrokes to the server that the user might not be able to send.
- Click **Server Macros** to use server defined macros. Some server macros are predefined by the XClarity Controller firmware. Other server defined macros can be defined using Lenovo XClarity Essentials and downloaded from the XClarity Controller. These macros are defined for all users of the remote console feature.
- Click **Configure** to add or remove user defined macros. The user defined macros are defined only for the current remote console user. Other remote console users will not see each other's user defined macros.
  - Click the Add Macros icon and press the key sequences that you desire; then, click **Add** to add a new macro.
  - To remove a user defined macro, select the macro from the list and click the trash can icon.
  - To send a user defined macro to the server select the **User Defined Macros** option, and click on the macro that you want to send.

Remote console mouse support

Use this information to understand the options for remote mouse control.

The remote console window offers several options for mouse control, including absolute mouse control, relative mouse control (no acceleration), and mouse control (RHEL, older Linux).

Absolute and relative mouse control

Use this information to access the absolute and relative options for controlling the mouse.

To access the absolute and relative options for controlling the mouse, complete the following steps:

Step 1. In the remote console window, click **Mouse**.

Step 2. Click **Mouse Settings** from the drop-down menu.

Step 3. Select one of the following **Mouse Acceleration** modes:

Absolute Positioning (Windows, Newer Linux & Mac OS X)
The client sends mouse location messages to the server that are relative to the origin (upper left area) of the viewing area.

Relative Positioning, no acceleration
The client sends the mouse location as an offset from the previous mouse position.

Relative Positioning (older Linux)
This mode applies an acceleration factor to align the mouse better on some Linux targets. The acceleration settings have been selected to maximize compatibility with older Linux distributions.

Screen Video Record/Replay

Use the information in this topic to record or replay remote presence screen videos.

The XClarity Controller web interface provides a DVR-like feature to support recording and playback remote presence screen videos. This function only supports video recording to a network folder. Currently, NFS and CIFS protocols are supported. Below are the steps in using the record and replay function.

1. On the remote console web page, click **Screen Recording** to open the settings window.
2. In the settings window, the following information may need to be specified.
   - If the “CIFS” mount type is selected, specify the **Remote Folder**, **User Name**, and **Password** parameters. The format for the CIFS remote folder is “**//<remote IP address>/<folder name>**”. For example: //xxx.xxx.xxx.xxx/folder.
   - If the “NFS” mount type is selected, specify the **Remote Folder** parameter. The format for the NFS remote folder is “**<remote IP address>:/<folder name>**”. For example: xxx.xxx.xxx.xxx:/folder.
   - Specify the video file name if necessary. If a file name has already been provided, an error message box will shown. To overwrite the existing file name, choose “Overwrite File Name”. If the “Auto” box is ticked, the video file name will be automatically generated.
   - “Max File Size” denotes the maximum video file size before the video recording will automatically stop.
   - “Max Recording Duration” denotes the maximum video recording duration before the recording will automatically stop.
3. Click **Start Recording** to start the video recording.
4. Click **Stop Recording** to stop the video recording. A popup window saying “Video Recording Completed” will appear, showing relevant video recording information.
5. Download the recorded videos from NFS or CIFS to your local folder. In the Remote Console Preview section of the XClarity Controller homepage, click **Recorded Videos** and select the video file to replay.

Remote console screen modes

Use the information in this topic to configure the remote console screen modes.

To configure the remote console screen modes, click **Screen Mode** .

The following menu options are available:

Full Screen
This mode fills the client desktop with the video display. Pressing the Esc key in this mode will exit full screen mode. Because the remote console menu is not visible in full screen mode, you will have to exit full screen mode to use any of the features provided by the remote console menu such as the keyboard macros.

Fit Screen
This is the default setting when the remote console is launched. In this setting, the target desktop is completely displayed without scroll bars. The aspect ratio is maintained.

Scaling Screen
With scaling enabled, the video image is sized so that the complete image is scaled to fill the console window.

Origin Screen
The video image has the same dimensions as the server end. Scroll bars are displayed if needed to allow viewing of video image areas that do not fit within the window.

Color Mode
Adjusts the color depth of the remote console window. There are two color-mode choices:

- Color: 7, 9, 12, 15, and 23 bit
- Grayscale: 16, 32, 64, and 128 shades

Note: Color mode adjustments are usually made if your connection to the remote server has limited bandwidth and you wish to reduce the bandwidth demand.

Media mount methods

Use the information in this topic to understand how to perform media mounts.

Three mechanisms are provided to mount ISO and IMG files as virtual drives.

- Virtual drives can be added to the server from the remote console session by clicking **Media**.
- Directly from the remote console web page, without establishing a remote console session.
- Standalone tool

Users need **Remote Console and Remote Disk Access** privileges to use the virtual media features.

Files can be mounted as virtual media from your local system or from a remote server, and can be accessed over the network or uploaded into the XClarity Controller memory using the RDOC feature. These mechanisms are described below.

- Local media are ISO or IMG files that are located on the system that you are using to access the XClarity Controller. This mechanism is only available through the remote console session, not directly from the remote console web page and is only available with the XClarity Controller Enterprise features. To mount local media, click **Activate** in the **Mount Local Media** section. Up to four files can be concurrently mounted to the server.

  Notes:

  – When using the Google Chrome browser, an additional mounting option called **Mount files/folders** is available to let you drag and drop the file(s)/folder.

- If multiple concurrent remote console sessions are in progress with an XClarity Controller, this feature can be activated only by one of the sessions.

- Files that are located on a remote system can also be mounted as virtual media. Up to four files can be concurrently mounted as virtual drives. The XClarity Controller supports the following file sharing protocols:

  - **CIFS - Common Internet File System**:
    - Enter the URL that locates the file on the remote system.
    - If you want the file to be presented to the server as read-only virtual media, tick the check box.
    - Enter the credentials that are needed for the XClarity Controller to access the file on the remote system.

      Note: The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space.
    - Mount options are optional and defined by the CIFS protocol.
    - If the remote server belongs to a collection of servers, where the security is centrally handled, enter the domain name to which the remote server belongs.
  - **NFS - Network File System**:
    - Enter the URL that locates the file on the remote system.
    - If you want the file to be presented to the server as read-only virtual media, tick the checkbox.
    - Mount options are optional and defined by the NFS protocol. Both NFSv3 and NFSv4 are supported. For example, to use NFSv3, you need to specify option 'nfsvers=3'. If the NFS server uses AUTH_SYS security flavor to authenticate NFS operations, you need to specify option 'sec=sys'.
  - **HTTPFS – HTTP Fuse-based File System**:
    - Enter the URL that locates the file on the remote system
    - If you want the file to be presented to the server as read-only virtual media, tick the check box.

    Note: Errors may occur during the mounting process for security certificates generated by Microsoft IIS. If this occurs, see "Media mount error issues" on page 73.

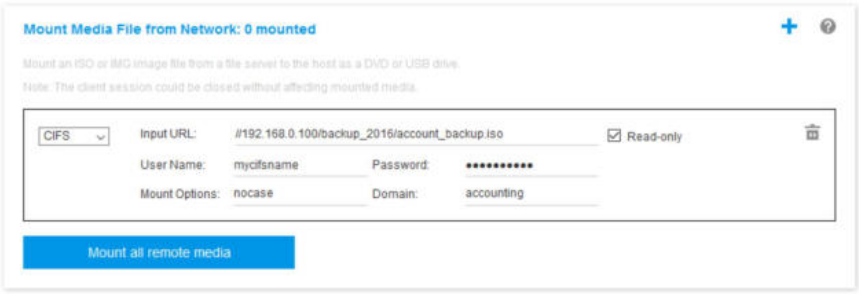
  Click **Mount all remote media** to mount the file as virtual media. To remove virtual media, click the trash can icon to the right of the mounted media.

- Up to two files can be uploaded in the XClarity Controller memory and mounted as virtual media using the XClarity Controller RDOC feature. The total size for both files must not exceed 50 MB. These files will remain in the XClarity Controller memory until they are removed, even if the remote console session has ended. The RDOC feature supports the following mechanisms when uploading the files:

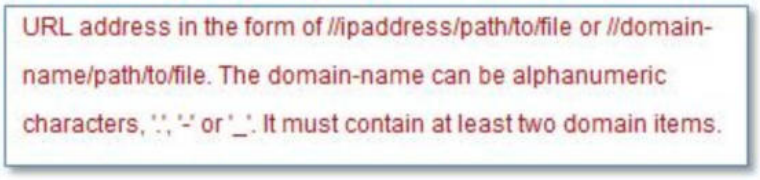
  - **CIFS - Common Internet File System**: See the description above for details.

    Example:

    To mount an ISO file named account_backup.iso that is located on the backup_2016 directory of a CIFS server at the 192.168.0.100 IP address as a read-only virtual drive on the server, you would fill in the fields as shown in the figure below. In this example, the server located at 192.168.0.100 is a member of a collection of servers under the domain "accounting". The domain name is optional. If your CIFS server is not part of a domain, leave the **Domain** field blank. The CIFS "nocase" mount option is specified in the **Mount Options** field in this example indicating to the CIFS server that the uppercase/lowercase checking of the file name should be ignored. The **Mount Options** field is optional. The information entered by the user in this field is not used by the BMC and is simply passed on to the CIFS server when the mount request is made. Refer to the documentation for your CIFS server implementation to determine which options are supported by your CIFS server.



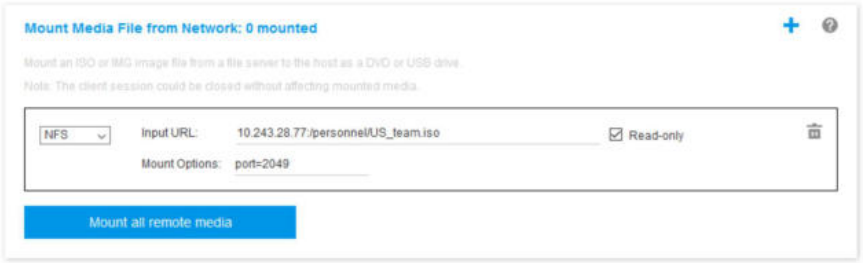
The BMC provides guidance when specifying the URL. If the URL being entered is not valid, the mount button will be greyed out and red text will be displayed under the URL field showing the expected format for the URL.



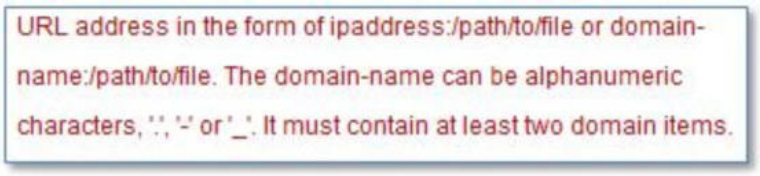
– **NFS - Network File System**: See the description above for details.

  Example:

  To mount an ISO file named US_team.iso that is located on the “personnel” directory of an NFS server at the 10.243.28.77 IP address as a read-only virtual drive on the server, you would fill in the fields as shown in the figure below. The NFS “port=2049” mount option specifies that network port 2049 should be used to transfer the data. The **Mount Options** field is optional. The information entered by the user in this field is passed on to the NFS server when the mount request is made. Refer to the documentation for your NFS server implementation to determine which options are supported by your NFS server.



The BMC provides guidance when specifying the URL. If the URL being entered is not valid, the mount button will be greyed out and red text will be displayed under the URL field showing the expected format for the URL.



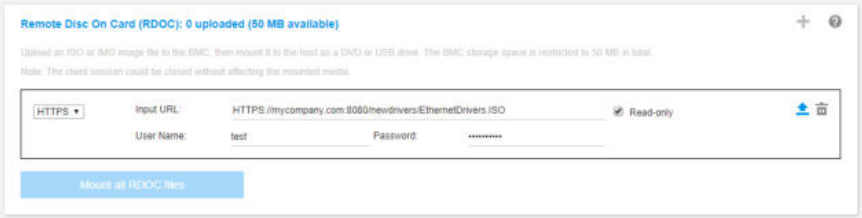
– **HTTPS – Hypertext Transfer Protocol Secure**:
  – Enter the URL that locates the file on the remote system.
  – If you want the file to be presented to the server as read-only virtual media, tick the check box.

- Enter the credentials that are needed for the XClarity Controller to access the file on the remote system.

Notes:

- Errors may occur during the mounting process for security certificates generated by Microsoft IIS. If this occurs, see “Media mount error issues” on page 73.
- The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space. **Example**:

  To mount an ISO file named EthernetDrivers.ISO that is located on the “newdrivers” directory of a HTTPS server with the domain name “mycompany.com” using network port 8080 as a read-only virtual drive on the server, you would fill in the fields as shown in the figure below.



  The BMC provides guidance when specifying the URL. If the URL being entered is not valid, the mount button will be greyed out and red text will be displayed under the URL field showing the expected format for the URL.

  URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

- **SFTP – SSH File Transfer Protocol**
  - Enter the URL that locates the file on the remote system.
  - If you want the file to be presented to the server as read-only virtual media, tick the checkbox.
  - Enter the credentials that are need to for the XClarity Controller to access the file on the remote system.

  Notes:

  - The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space.
  - When the XClarity Controller connects to a HTTPS server, a pop-up window will appear showing information of the security certificate used by the HTTPS sever. The XClarity Controller is unable to verify the authentic of the security certificate.
- **LOCAL - Common Internet File System**:
  - Browse your system for the ISO or IMG file that you want to mount.
  - If you want the file to be presented to the server as read-only virtual media, check the check box.

Click **Mount all RDOC files** to mount the file as virtual media. To remove the virtual media, click the trash can icon to the right of the mounted media.

Standalone tool

For users that require mounting of the devices or images(.iso / .img) using the XClarity Controller, users can use the rdmount standalone code part of the OneCLI package. Specifically, rdmount will open a connection to XClarity Controller and will mount the device or images to the host.

rdmount has the following syntax:

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

Example to mount an iso file:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

Remote disk using Java client

This sections describe how to mount local media using Java client.

you can use Java client to assign to the server a CD or DVD drive, a diskette drive, USB flash drive that is on your computer, or you can specify a disk image on your computer for the server to use. You can use the drive for functions such as restarting (booting) the server, updating code, installing new software on the server, and installing or updating the operating system on the server. You can access the remote disk. Drives and disk images are displayed as USB drives on the server.

Notes: The Remote Console Java supports one of the following Java environment, and it can be opened only if the HTML5 client is not running.

1. Oracle Java Runtime Environment 1.8/Java SE 8 or newer versions
2. OpenJDK 8. Distribution of AdoptOpenJDK with HotSpot JVM is supported.

If you use AdoptOpenJDK, you must use https://openwebstart.com/ under OSX, Windows, and Linux.

Creating an image file

To create a new image file from a specified source folder, complete the following steps:

1. Click the **Create Image** option under the **Virtual Media** tab in the Virtual Media Java Client window. The Create Image from Folder window is displayed.
2. Click the **Browse** button associated with the **Source Folder** field to select the specific source folder.
3. Click the **Browse** button associated with the **New Image File** field to select the image file to use.
4. Click the **Create Image** button.

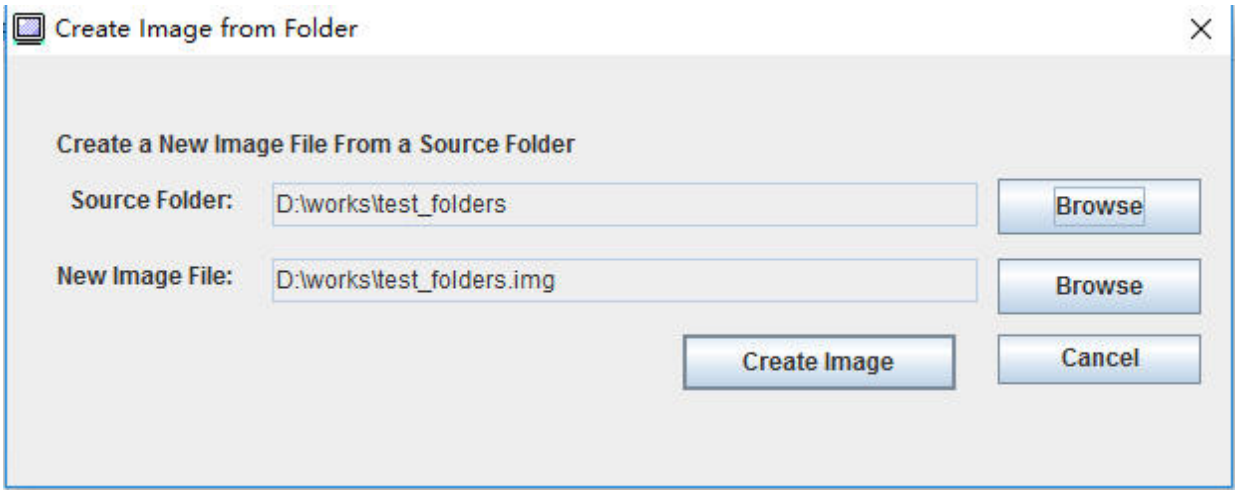


Figure 1. Creating an image file

Selecting devices to mount

To mount local image, folder and CD/DVD/USB drive, complete the following steps:

Click the **Select Devices to Mount** option under the **Virtual Media** tab in the Virtual Media Java Client window. The Select Devices to Mount window is displayed.

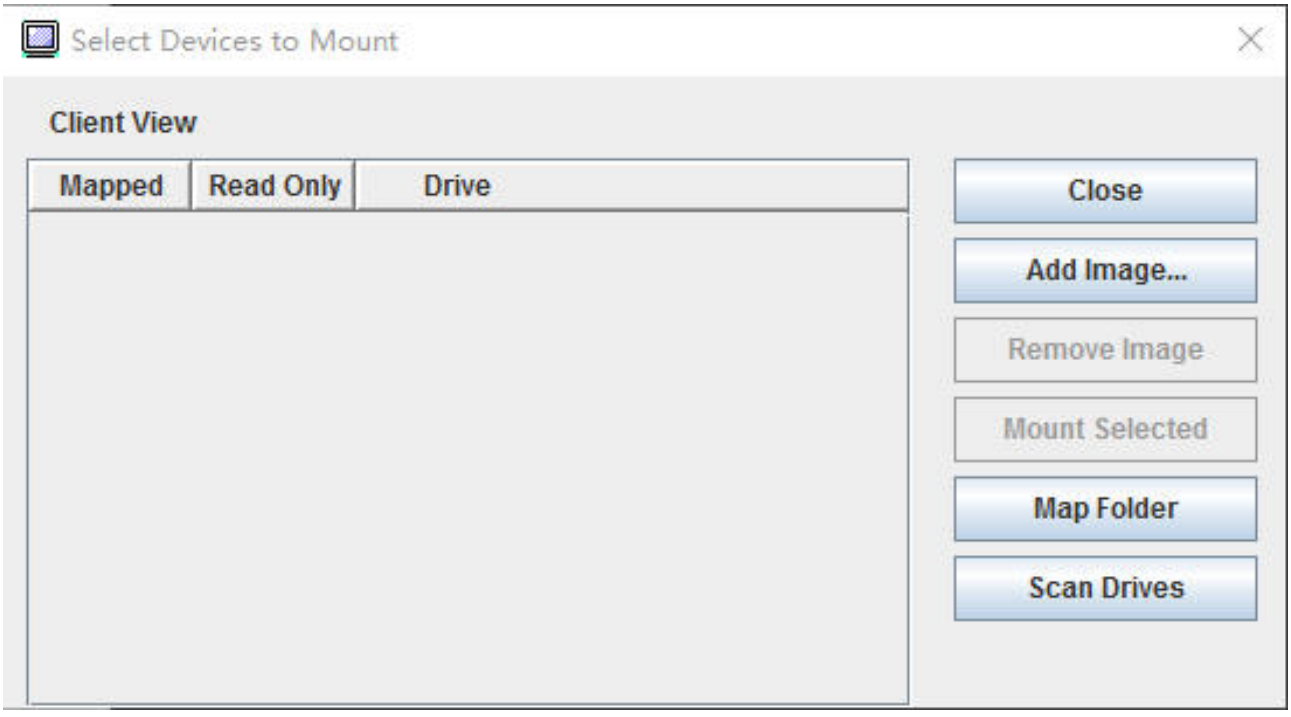


Figure 2. Select Devices to Mount Window

You can mount local image, folder and CD/DVD/USB drive by performing the following steps:

- **Mount Local Image**:
  1. Click the **Add Image** button to select the image you want to mount.
  2. Check the **Mapped** option.

3. Check the **Read Only** option to enable the function if needed.
4. Click the **Mount Selected** button and you can mount the local image successfully.

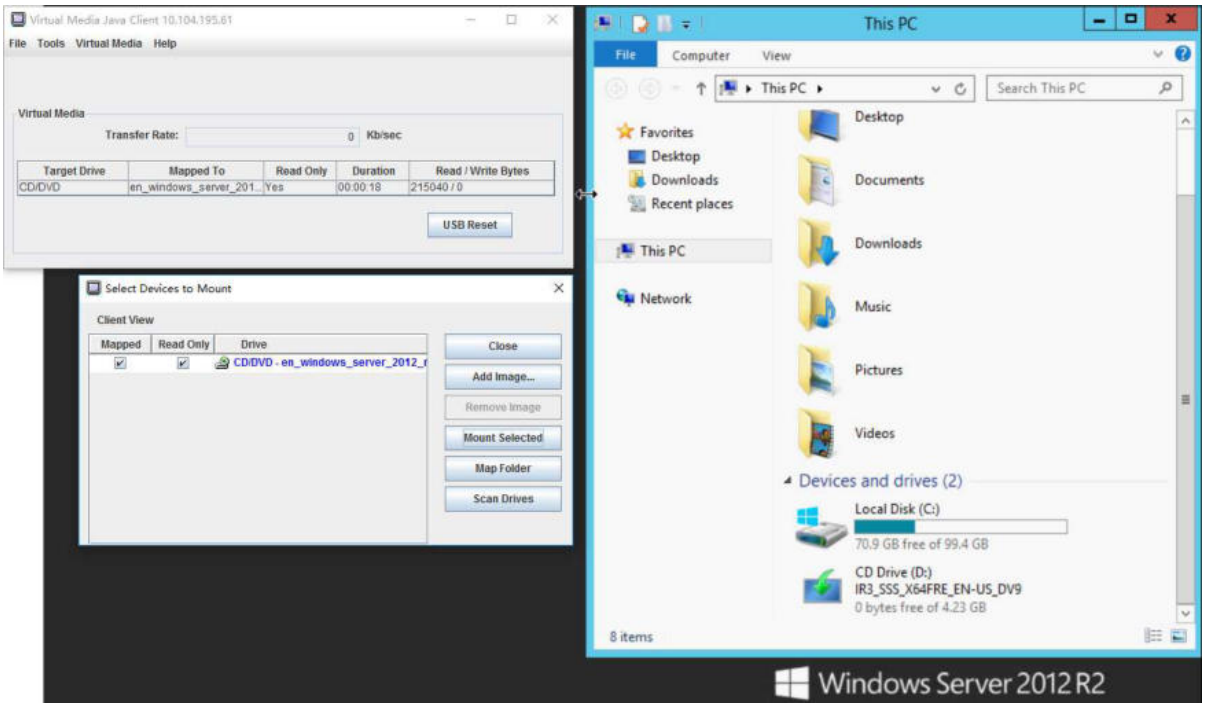


Figure 3. Mount Local Image

- **Mount Local Folder**:
  1. Click the **Map Folder** button to select the local folder you want to mount.
  2. Click the **Mount Selected** button and you can mount the local folder successfully.

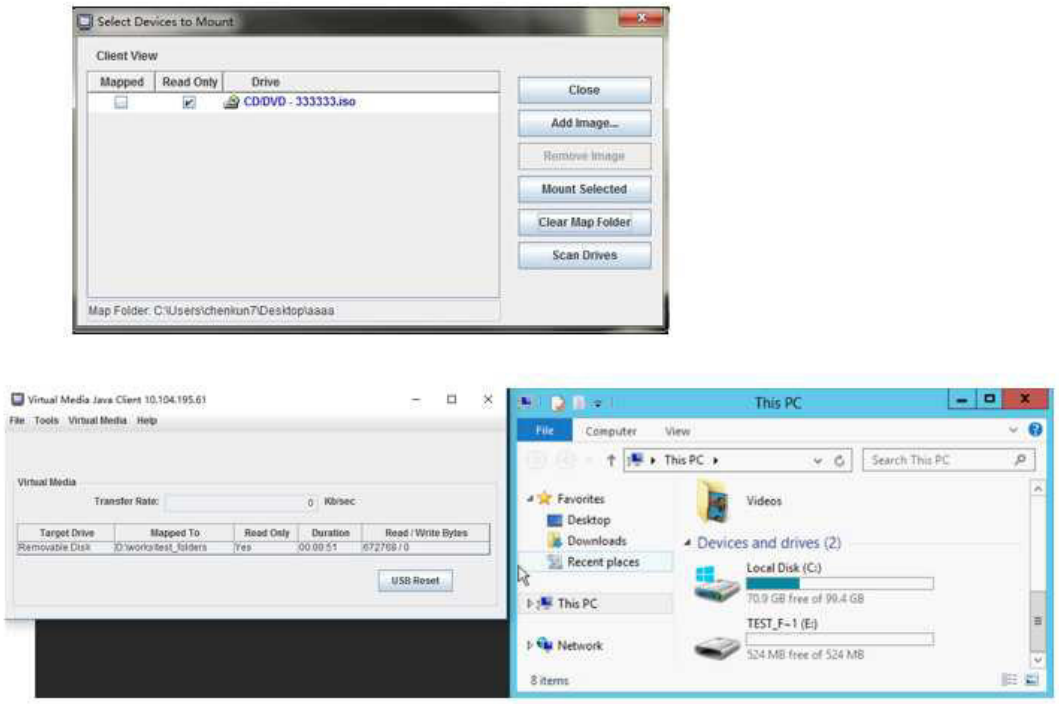


Figure 4. Mount Local Folder

- **Mount CD/DVD or USB Drive**:
  1. Click the **Scan Drives** button to detect plugged CD/DVD or USB Drive.
  2. Check the **Mapped** option.
  3. Check the **Read Only** option to enable the function if needed.
  4. Click the **Mount Selected** button and you can mount the local image successfully.

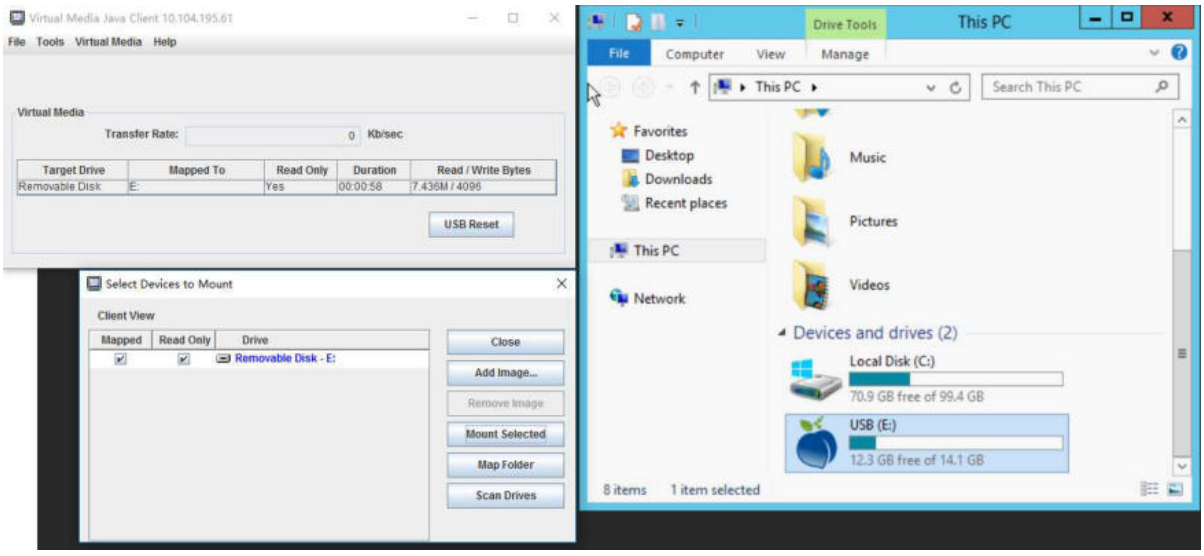


Figure 5. Mount CD/DVD or USB Drive

The Select Devices to Mount window contains a list of the current local devices that are available for mounting. This window contains the following fields and buttons:

- The **Mapped** field contains the check box that allows you to select the devices to mount or map.
- The **Read Only** field contains the check box that allows you to select the mapped or mounted devices that will be *read-only* on the host server.
- The **Drive** field contains the device path on the local machine.
- Click the **Close** button to close the Select Devices to Mount window.
- Click the **Add Image** button to browse for the diskette image and ISO image file in your local file system that you want to add to the list of devices.
- Click the **Remove Image** button to remove an image that has been added to the list of devices.
- Click the **Mount Selected** button to mount or map all devices that are checked for mounting or mapping in the **Mapped** field.

  Note: The folder will be mounted as read-only.
- Click the **Scan Drives** button to refresh the list of local devices.

Selecting devices to unmount

To unmount the host server devices, complete the following steps:

1. Click the **Unmount All** option under the **Virtual Media** tab in the Virtual Media Java Client window.
2. After selecting the **Unmount All** option you are presented with an Unmount All confirmation window. If you accept, *all* host server devices on the server are unmounted.

   Note: You cannot unmount drives individually.

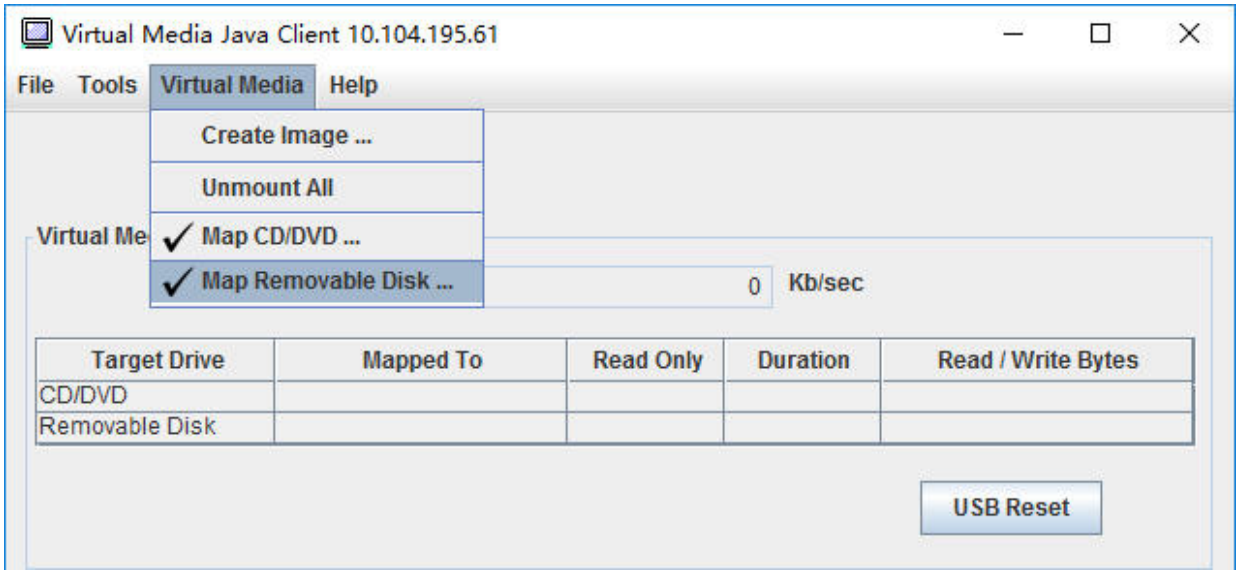


Figure 6. Unmount All

Media mount error issues

Use the information in this topic to troubleshoot media mount error issues.

When using security certificates generated by Microsoft IIS, you may encounter errors during the mounting process. If this occurs, replace the security certificate with a new one generated by openssl. Specifically, the newly generated pfx file is loaded into the Microsoft IIS server.

Below is an example showing how the new security certificate is generated via openssl in the Linux operating system.

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

Exiting the remote console session

This topic explains how to end your remote console session.

To exit your remote console session, close the remote console and the virtual media session windows.

Downloading service data

Use the information in this topic to collect service information about your server. This process is normally only done at the request of service personnel to assist in resolving a server problem.

In the XClarity Controller home page, click the **Service** option in the **Quick Action** section and select **Download Service Data**. Click **OK** to download the service data.

The process of collecting the service and support data takes a few minutes to generate the service data. The file will be saved to your default download folder. The naming convention for the service data file follows this convention:<machine type and model>_<serial number>_xcc_<date>-<time>.tgz

For example: 7X2106Z01A_2345678_xcc_170511-175656.tgz.

In addition to the tgz format, the service data can also be downloaded using the tzz format. Tzz uses a different compression algorithm and can be extracted with a utility such as “lzop”.

Server Properties

Use the information in this topic to change or view relevant server properties.

Setting Location and Contact

Use the information in this topic to set various parameters to help identify the system for operations and support personnel.

Select **Server Properties** under **Server Configuration**, to configure the **Location and Contact** information.

Contact
Allows you to specify the name and phone number of the person who should be contacted if the system experiences a problem.

Note: This field is the same as the Contact field in the SNMPv3 configuration and is required to enable SNMPv3.

Rack Name
Allows you to locate the server more easily by specifying which rack it is in.

Note: The field is optional and is not configurable in a Flex node.

Room Number
Allows you to locate the server more easily by specifying which room it is in.

Building
Allows you to locate the server more easily by specifying which building it is in.

Lowest U
Allows you to locate the server more easily by specifying the position in the rack.

Note: The field is optional and is not configurable in a Flex node.

Address
Allows you to specify the full postal address where the server is located.

Note: When the relevant information has been inputted, it will appear as a single line in the **Location** field in the SNMPv3 section and XClarity Controller home page.

Setting server timeouts

Use the information in this topic to set timeouts for the server.

These timeouts are used to restore operation to a server that has hung.

Select **Server Properties** under **Server Configuration**, to configure the server timeouts. The following server timeout selections are provided:

OS Watchdog
The OS watchdog is used to monitor the operating system to ensure that it is not hung. The Ethernet over USB interface must be enabled for this feature. See “Configuring Ethernet over USB” on page 32 for details. The XClarity Controller contacts the operating system at an interval configured in the **OS Watchdog Time** selection. If the operating system does not respond before it is time for the next check, the XClarity Controller assumes that the operating system has hung. The XClarity Controller will capture the contents of the server display and then reboot the server in an attempt to restore operation. The XClarity Controller will reboot the server only once. If the operating system continues to hang after the reboot, instead of continually rebooting the server, the server will be left in the hung state so that the problem can be investigated and corrected. To rearm the OS watchdog, power the server off and back on. To enable the OS watchdog, select an interval from the OS Watchdog Time drop-down and click **Apply**. To disable the OS watchdog, select **None** on the OS Watchdog Time drop-down menu.

Loader Watchdog
The loader watchdog monitors the interval between the completion of POST and when the operating system begins running. The Ethernet over USB interface must be enabled for this feature. See “Configuring Ethernet over USB” on page 32 for details. When POST is completed, the XClarity Controller starts a timer and begins to contact the operating system. If the operating system does not respond with the time configured in the Loader Watchdog selection, the XClarity Controller assumes that the operating system boot has hung. The XClarity Controller will then reboot the server in an attempt to restore operation. The XClarity Controller will reboot the server only once. If the operating system boot continues to hang after the reboot, instead of continually rebooting the server, the server will be left in the hung state so that the problem can be investigated and corrected. The loader watchdog is rearmed when server is switched off and back on or when the server successfully boots into the operating system. To enable the loader watchdog, select an interval from the Loader Watchdog drop-down and click **Apply**. To disable the loader watchdog select **None** on the Loader Watchdog drop-down.

Enable Power Off Delay
Use the Power Off Delay field to specify the number of minutes that the XClarity Controller subsystem will wait for the operating system to shutdown before forcing power off. To set the power off delay timeout value, select time interval from the drop-down and click **Apply**. To disable the XClarity Controller from forcing power off, select **None** from the drop-down selection.

Trespass message

To create a message that is displayed when a user logs in to the XClarity Controller, use the information in this topic.

Select **Server Properties** under **Server Configuration**. Use the **Trespass Message** option to configure a message that you want displayed to the user. When you are finished, click **Apply**.

The message text will be displayed in the Message area of the XClarity Controller login page when a user logs in.

Setting the XClarity Controller date and time

Use the information in this topic to understand XClarity Controller date and time settings. Instructions are provided to configure the XClarity Controller date and time. The XClarity Controller date and time is used to time stamp all events that are logged in the event log and alerts that are sent.

At the XClarity Controller home page, click the clock icon on the upper right-hand corner to view or change the XClarity Controller date and time. The XClarity Controller does not have its own real-time clock. You can configure the XClarity Controller to sync its time and date with a Network Time Protocol server or with the server's real-time clock hardware.

Syncing with NTP

Complete the following steps to synchronize the XClarity Controller clock with the NTP server:

- Select **Sync up time with NTP** and specify the NTP server address.
- Additional NTP servers can be specified by clicking the "+" icon.
- Specify how frequently you want the XClarity Controller to sync with the NTP server.
- The time obtained from the NTP server is in Coordinated Universal Time (UTC) format.
  - If you want the XClarity Controller to adjust its time and date for your local region, select the time zone offset for your locale from the drop-down menu.
  - If your location observes Daylight Saving Time, tick the **Automatically adjust for Daylight Saving Time (DST)** checkbox.
- When your configuration changes are complete, click **Apply**.

Syncing with the Host

The time kept in the server's real-time clock hardware may be in Coordinated Universal Time (UTC) format or may already have been adjusted and stored in local time format. Some operating systems store the real-time clock in UTC format while others store the time as local time. The server real-time clock does not indicate which format the time is in. Therefore when the XClarity Controller is configured to sync with the host's real-time clock, the user can choose how the XClarity Controller uses the time and date that is obtained from the real-time clock.

- Local (example: Windows): In this mode, the XClarity Controller treats the time and date that is obtained from the real-time clock as local time with any applicable time zone and DST offsets already applied.
- UTC (example: Linux): In this mode, the XClarity Controller treats the time and date that is obtained from the real-time clock as Coordinated Universal Time, with no time zone or DST offsets already applied. In this mode, you can choose to adjust the time and date for your local region by selecting the time zone offset for your locale from the drop-down menu. If your location observes Daylight Saving Time, you can also tick the **Automatically adjust for Daylight Saving Time (DST)** check box.
- When your configuration changes are complete, click **Apply**.

Notes:

- When daylight saving occurs, any actions that were scheduled for the XClarity Controller to perform during the interval when the clock jumps forward will not be performed. For example, if the US daylight start time is 2:00 am on March 12th, and a power action is scheduled for 2:10 am on March 12th, this action will not occur. Once the time reaches 2:00 am, the XClarity Controller will instead read the time as 3:00 am.
- XClarity Controller Date and Time settings cannot be modified in a Flex System.

Chapter 6. Configuring the Storage

Use the information in this chapter to understand the options available for storage configurations.

When configuring the storage, following options are available:

- Detail
- RAID setup

RAID Detail

For using RAID detail function, use the information in this topic.

This function displays the storage devices' physical structure and storage configuration along with details like their location, manufacturer, product name, status, capacity, interface, media, form factor and other info.

RAID Setup

To perform RAID setup functions, use the information in this topic.

Use the information in this topic to view and configure storage pools, associated virtual disks and drives for the RAID adapter. If the system is powered off, power it on in order to view the RAID information.

Viewing and configuring the virtual drives

Use the information in this topic to view and configure the virtual drives.

When you select **RAID Setup** under **Server Configuration**, the **Array Configuration** tab will be chosen and the existing virtual disks will be displayed by default. The logical drives are sorted by disk arrays and controllers. Detailed information about the virtual disk, such as the virtual disk strip size and bootable information is displayed.

To configure the RAID settings, click **Enable Edit mode**.

In edit mode, you can click the controller action menu, view the current RAID virtual disks and create new RAID virtual disks.

From the Controller Actions menu, you can perform the following actions:

Clear RAID configuration
Clears all the configuration and data on the selected controller.

Manage foreign configuration
Import any foreign drives that were detected. A foreign drive is a drive that was moved from a different RAID configuration to the current RAID controller

Note: You will be notified if no foreign drives are detected.

Information of the current RAID virtual disks for a particular controller are shown as respective "virtual disk cards". Each card displays information such as the virtual disk name, status, capacity and actions. The pencil icon allows you to edit the information, and the trash can icon enables you to delete the "virtual disk card".

© Copyright Lenovo 2017, 2020

Note: The capacity and RAID level cannot be changed.

If you click the virtual disk name, a virtual disk properties window will appear.

To create a new RAID virtual disk, follow the steps shown below:

Note: If there is no remaining storage capacity, you are unable to create a new virtual disk.

1. **Select drives or a disk array which has free storage capacity**
   a. When creating a virtual disk in a new disk array, you need to specify the RAID level. If there are not enough drives to select, and you click **Next**, an error message will appear under the RAID level field.

      For some RAID levels, span is required . There is also a minimum amount of drives that need to be present in the span.

      1) For these types of situations, the web interface will display **Span 1** by default.
      2) Select the drives and click **Add member** to add the drives to **Span 1**. When **Span 1** does not have enough drives, disable the **Add Span** link.
      3) Click **Add Span** to add **Span 2**. Select the drives and click **Add member** to add to **Span 2**.
      4) Click **Add member** to add drives to the last span. If you want to add drives to **Span 1** again, you need to click Span 1 and select the drives to add to **Span 1**.
      5) If the number of spans reaches the maximum amount, disable **Add span**.

   b. To create virtual disks in an existing disk array, you need to select a disk array that has free capacity.
2. **Creating a virtual disk**
   a. By default, create a virtual disk that uses all the storage capacity. The **Add** icon is disabled when all of the storage is used. You can click the pencil icon to change the capacity or other properties.
   b. When you edit the first virtual disk to use only some of the storage capacity, the **Add** icon will be enabled. Click the icon to show the **Add Virtual Disk** window.
   c. If there is more than one virtual disk, the **Remove** icon will be enabled. This icon will not be shown if there is only one virtual disk. When you click the **Remove** icon, the selected row will be immediately deleted. There will be no confirmation window as the virtual disk has not been created yet.
   d. Click **Start Creating Virtual Disk** to start the process.

Note: When the controller is not supported, a message will appear.

Viewing and configuring the storage inventory

Use the information in this topic to view and configure the storage inventory.

Under the **Storage Inventory** tab , you can view and configure disk arrays, associated virtual drives and drives for the RAID controller.

- **For storage devices that support RAID configuration**:
  1. If the controller includes configured disk arrays, it will display the installed drives based on the disk array. The following describes the items that appear in the window.
     - **Table title**: Shows the disk array ID, RAID level and the total number of drives.
     - **Table content**: Lists the basic properties - drive name, RAID state, type, serial number, part number, FRU number and actions. You can go to the **Inventory** page to view all the properties that the XClarity Controller can detect.
     - **Actions**: The following shows the action items that can be performed. Some actions will not be available when the drive is in a different state.
       - **Assign hot spare**: Specifies the drive as global hot spare or a dedicated hot spare.
       - **Remove hot spare**: Removes the drive from the hot spare.

- **Make disk drive offline**: Sets the drive to offline.
- **Make disk drive online**: Sets the drive to online.
- **Make disk drive as reusable**: Sets the drive to reusable.
- **Make disk drive as missing**: Sets the drive as missing.
- **Make drive good to JBOD**: Adds drive to JBOD disk arrangement.
- **Make drive unconfigured good**: Makes the drive available to be configured into an array, or for use as an emergency hot spare.
- **Make drive unconfigured bad**: Marks the drive bad, preventing it from being used in an array or as an emergency hot spare.
- **Make disk drive as prepare for removal**: Sets the drive for removal.

2. If the controller includes drives that have not yet been configured, they will be displayed in the **Non-RAID drives** table. By clicking the **Convert JBOD to Ready to Configure** option, a window will appear showing all the drives that support this action item. You can select one or more drives to convert.

For storage devices that do not support RAID configuration: The XClarity Controller may not be able to detect the properties of some drives.

Chapter 7. Updating Server Firmware

To update server firmware, use information in this topic.

Overview

General Information about updating server firmware.

The **Firmware Update** option on the navigation panel has 4 features:

- **System Firmware:** Overview of system firmware status and version. And to perform system firmware update.
- **Adapter Firmware:** Overview of adapter firmware installed, their status and version. And to perform adapter firmware update.
- **PSU Firmware:** Overview of power supply unit firmware version. And to perform PSU firmware update.
- **Update from Repository:** Sync server firmware with remote CIFS/NFS repository for batch update.

The current status and versions of firmware for the BMC, UEFI, LXPM, LXPM drivers, and adapters are displayed, including the BMC primary and backup versions. There are four categories for the firmware status:

- **Active:** The firmware is active.
- **Inactive:** The firmware is not active.
- **Pending:** The firmware is waiting to become active.
- **N/A:** No firmware has been installed for this component.

Attention:

- Installing the wrong firmware update might cause the server to malfunction. Before you install a firmware or device-driver update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware or device-driver version to the latest version. As the web browser may contain XCC cache data, it is recommended to reload the web page after the XCC firmware has been upgraded.
- With the exception of SATA M.2 adapter, AMD processor servers do not support out-of-band adapter firmware update.
- Some firmware updates require system restarting, which performs firmware activation or internal update. This process in system booting is called “system maintenance mode”, that does not allow user power actions temporarily. The mode is also enabled during firmware update. User shall not disconnect AC power when the system enters maintenance mode.

System, Adapter and PSU Firmware Update

Steps to update System firmware, Adapter firmware and PSU firmware.

To manually apply update for **System Firmware**, **Adapter Firmware** and **PSU Firmware**, complete the following steps:

1. Click **Update Firmware** within each feature. The Update Server Firmware window opens.
2. Click **Browse** to select the firmware update file that you want to use.
3. Navigate to the file you want to select and click **Open**. You are returned to the Update Server Firmware window with the selected file displayed.

© Copyright Lenovo 2017, 2020

4. Click **Next >** to begin the upload and verify process on the selected file. A progress meter will be displayed as the file is being uploaded and verified. You can view this status window to verify that the file you selected to update is the correct file. For **System Firmware**, the status window will have information regarding the type of firmware file that is to be updated such as BMC, UEFI, or LXPM. After the firmware file is uploaded and verified successfully, click **Next** to select the device you want to update.
5. Click **Update** to begin the firmware update. A progress meter shows the progress of the update. When the firmware update is completed successfully, click **Finish**. If the update requires the XClarity Controller to be restarted in order to take effect, a warning message will be displayed. For details on how to restart the XClarity Controller, see “Power actions” on page 58.

Update From Remote Repository

Steps to update server firmware from a remote repository

With **Update from Repository**, user can configure XCC to sync server firmware with a remote CIFS/NFS firmware repository. The firmware repository should contain SUP packages including binary and metadata XML files, or UXSP metadata XML and corresponding binary files. XCC parses the metadata XML files to pick out firmware packages that support OOB update for this specific system hardware then starts a batch update.

There are five update status:

- **Green check mark** : The firmware’s upgrade has finished successfully.
- **Red X mark** : The firmware’s upgrade has failed.
- **Updating:** The firmware is undergoing the process of upgrading.
- **Cancel:** The firmware’s upgrade is cancelled.
- **Waiting:** The firmware’s upgrade is waiting to be deployed.

When user clicks **Stop Updating** it will cancel the upgrades in queue after the current installation package update is complete.

To update from repository, complete the following steps:

1. Click **Connect** to remote repository after entering remote repository information.
2. Click **Update** to start the batch update.
3. Click **View Details** to see updating status, there are 5 categories of status as mentioned above.
4. Click **Stop Updating** will cancel the upgrades in queue after the current installation package update is completed.
5. Click **Disconnect** to disconnect from the remote repository.
6. If the update requires the XClarity Controller to be restarted in order to take effect, a warning message will be displayed. For details on how to restart the XClarity Controller, see “Power actions” on page 58.

Chapter 8. License Management

The Lenovo XClarity Controller License Management allows you to install and manage optional server and systems management features.

There are multiple levels of XClarity Controller firmware functionality and features available for your server. The level of the firmware features installed on your server vary based on hardware type.

You can upgrade the XClarity Controller functionality by purchasing and installing an activation key.

To order an activation key, contact your sales representative or business partner.

Use the XClarity Controller web interface or the XClarity Controller CLI to manually install an activation key that lets you use an optional feature you have purchased. Before activating a key:

- The activation key must be on the system that you are using to login to the XClarity Controller.
- You must have ordered the license key and received its authorization code via mail or email.

See “Installing an activation key” on page 85, “Removing an activation key” on page 86 or “Exporting an activation key” on page 86 for information about managing an activation key using the XClarity Controller web interface. See “keycfg command” on page 122 for information about managing an activation key using the XClarity Controller CLI.

To register an ID in administering your XClarity Controller license, click the following link: http://thinksystem.lenovofiles.com/help/index.jsp

Additional information about license management for Lenovo servers is available at the following **Lenovo Press** website:

https://lenovopress.com/redp4895-using-lenovo-features-on-demand

Attention: You cannot directly upgrade from Standard XClarity Controller to Enterprise Level functionality. You will need to first upgrade to Advanced Level before the Enterprise Level functionality can be activated.

Installing an activation key

Use the information in this topic to add an optional feature to your server.

To install an activation key, complete the following steps:

Step 1. Click **License** under **BMC Configuration**.

Step 2. Click **Upgrade License**.

Step 3. In the **Add a new license** window, click **Browse**; then, select the activation key file to add in the File Upload window and click **Open** to add the file or click **Cancel** to stop the installation. To finish adding the key, click **OK**, in the Add Activation Key window, or click **Cancel** to stop the installation.

The Success window indicates that the activation key is installed.

Notes:

- If the activation key is not valid, an error window will appear.

Step 4. Click **OK** to close the Success window.

© Copyright Lenovo 2017, 2020

Removing an activation key

Use the information in this topic to delete an optional feature from your server.

To remove a activation key, complete the following steps:

Step 1. Click **License** under **BMC Configuration**.

Step 2. Select the activation key to remove; then, click **Delete**.

Step 3. In the Confirm Activation Key Deletion window, click **OK** to confirm activation key deletion or click **Cancel** to keep the key file.
The selected activation key is removed from the server and no longer appears in the License Management page.

Exporting an activation key

Use the information in this topic to export an optional feature from your server.

To export an activation key, complete the following steps:

Step 1. Click **License** under **BMC Configuration**.

Step 2. From the License Management page, select the activation key to export; then, click **Export**.

Step 3. In the **Export the selected license** window, click **Export** to confirm activation key exporting or click **Cancel** to cancel the key exporting request.

Step 4. Select the directory to save the file.
The selected activation key is exported from the server.

Chapter 9. Lenovo XClarity Controller Redfish REST API

The Lenovo XClarity Controller provides a Redfish compliant set of easy-to-use REST APIs that can be used to access Lenovo XClarity Controller data and services from applications running outside of the Lenovo XClarity Controller framework.

This allows for easy integration of Lenovo XClarity Controller capabilities into other software, whether the software is running on the same system as the Lenovo XClarity Controller server, or on a remote system within the same network. These APIs are based on the industry standard Redfish REST API and are accessed via the HTTPS protocol.

The XClarity Controller Redfish REST API user guide can be found here: https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.restapi.doc/xcc_restapi_book.pdf.

Lenovo provides open source sample Redfish scripts that can be used as reference for developing software that communicates with Lenovo Redfish REST API. These sample scripts can be found here:

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

DMTF specifications related to the Redfish API are available at: https://redfish.dmtf.org/. This website provides general specifications and other reference material on the Redfish REST API.

© Copyright Lenovo 2017, 2020

Chapter 10. Command-line interface

Use the information in this topic to enter commands that manage and monitor the XClarity Controller without having to use the XClarity Controller web interface.

Use the XClarity Controller command line interface (CLI) to access the XClarity Controller without having to use the web interface. It provides a subset of the management functions that are provided by the web interface.

You can access the CLI through a SSH session. You must be authenticated by the XClarity Controller before you can issue any CLI commands.

Accessing the command-line interface

Use the information in this topic to access the CLI.

To access the CLI, start an SSH session to the XClarity Controller IP address (see “Configuring serial-to-SSH redirection” on page 89 for more information).

Logging in to the command-line session

Use the information in this topic to log in to the command line session.

To log in to the command line, complete the following steps:

Step 1. Establish a connection with the XClarity Controller.

Step 2. At the user name prompt, type the user ID.

Step 3. At the password prompt, type the password that you use to log in to the XClarity Controller.

You are logged in to the command line. The command-line prompt is `system>`. The command-line session continues until you type `exit` at the command line. You are logged off and the session is ended.

Configuring serial-to-SSH redirection

This topic provides information about using the XClarity Controller as a serial terminal server.

Serial-to-SSH redirection enables a system administrator to use the XClarity Controller as a serial terminal server. A server serial port can be accessed from a SSH connection when serial redirection is enabled.

Note: The CLI **console 1** command is used to start a serial redirection session with the COM port.

Example session

```
$ ssh USERID@10.240.1.12
Password:

system>
```

All traffic from the SSH session is routed to COM2.

```
ESC (
```

© Copyright Lenovo 2017, 2020

Type the exit key sequence to return to the CLI. In this example, press Esc and then type a left parenthesis. The CLI prompt displays to indicate return to the IMM CLI.

```
system>
```

Command syntax

Review the guidelines in this topic to understand how to enter commands in the CLI.

Read the following guidelines before you use the commands:

- Each command has the following format:
  `command [arguments] [-options]`
- The command syntax is case sensitive.
- The command name is all lowercase.
- All arguments must immediately follow the command. The options immediately follow the arguments.
- Each option is always preceded by a hyphen (-). An option can be a short option (single letter) or a long option (multiple letters).
- If an option has an argument, the argument is mandatory, for example:
  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`
  where **ifconfig** is the command, eth0 is an argument, and -i, -g, and -s are options. In this example, all three options have arguments.
- Brackets indicate that an argument or option is optional. Brackets are not part of the command that you type.

Features and limitations

This topic contains information about CLI features and limitations.

The CLI has the following features and limitations:

- Multiple concurrent CLI sessions are allowed via SSH.
- One command is allowed per line (1024-character limit, including spaces).
- There is no continuation character for long commands. The only editing function is the Backspace key to erase the character that you just typed.
- The Up Arrow and Down Arrow keys can be used to browse through the last eight commands. The **history** command displays a list of the last eight commands, which you can then use as a shortcut to execute a command, as in the following example:

```
system > history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
```

```
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- In the CLI, the output buffer limit is 2 KB. There is no buffering. The output of an individual command cannot exceed 2048 characters. This limit does not apply in serial redirect mode (the data is buffered during serial redirect).
- Simple text messages are used to denote command execution status, as in the following example:
```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```
- The command syntax is case sensitive.
- There must be at least one space between an option and its argument. For example, `ifconfig eth0 -i192.168.70.133` is incorrect syntax. The correct syntax is `ifconfig eth0 -i 192.168.70.133`.
- All commands have the `-h`, `-help`, and `?` options, which give syntax help. All of the following examples will give the same result:
```
system> power -h
system> power -help
system> power ?
```
- Some of the commands that are described in the following sections might not be available for your system configuration. To see a list of the commands that are supported by your configuration, use the `help` or `?` option, as shown in the following examples:
```
system> help
system> ?
```
- In a Flex System, some settings are managed by the CMM and cannot be modified on the XClarity Controller.

Alphabetical command listing

This topic contains a list of CLI commands in alphabetic order. Links are provided to topics for each command. Each command topic provides information about the command, its function, syntax, and usage.

The complete list of all XClarity Controller CLI commands, in alphabetical order, is as follows:

- “accseccfg command” on page 107
- “adapter command” on page 170
- “alertcfg command” on page 109
- “alertentries command” on page 153
- “asu command” on page 109
- “backup command” on page 112
- “batch command” on page 155
- “chconfig command” on page 158
- “chlog command” on page 160
- “chmanual command” on page 160
- “clearcfg command” on page 156
- “clearlog command” on page 94
- “clock command” on page 156

- “console command” on page 107
- “dbgshimm command” on page 173
- “dhcpinfo command” on page 113
- “dns command” on page 114
- “encaps command” on page 116
- “ethtousb command” on page 116
- “exit command” on page 93
- “fans command” on page 95
- “ffdc command” on page 95
- “firewall command” on page 117
- “fuelg command” on page 105
- “gprofile command” on page 118
- “hashpw command” on page 119
- “help command” on page 93
- “history command” on page 93
- “hreport command” on page 96
- “identify command” on page 156
- “ifconfig command” on page 120
- “info command” on page 157
- “keycfg command” on page 122
- “ldap command” on page 124
- “led command” on page 97
- “mhlog command” on page 97
- “mvstor command” on page 172
- “ntp command” on page 125
- “portcfg command” on page 126
- “portcontrol command” on page 127
- “ports command” on page 128
- “power command” on page 103
- “pxeboot command” on page 106
- “rdmount command” on page 129
- “readlog command” on page 99
- “reset command” on page 105
- “restore command” on page 130
- “restoredefaults command” on page 131
- “roles command” on page 131
- “seccfg command” on page 133
- “set command” on page 133
- “smtp command” on page 133
- “snmp command” on page 134
- “snmpalerts command” on page 136

- “spreset command” on page 158
- “srcfg command” on page 137
- “sshcfg command” on page 138
- “ssl command” on page 139
- “sslcfg command” on page 140
- “storage command” on page 161
- “storekeycfg command” on page 143
- “syncrep command” on page 144
- “syshealth command” on page 100
- “temps command” on page 101
- “thermal command” on page 145
- “timeouts command” on page 146
- “tls command” on page 146
- “trespass command” on page 147
- “uefipw command” on page 148
- “usbeth command” on page 148
- “usbfp command” on page 148
- “users command” on page 149
- “volts command” on page 101
- “vpd command” on page 102

Utility commands

This topic provides an alphabetic list of utility CLI commands.

There are currently 3 utility commands:

exit command

Use this command to log off the CLI session,

Use the **exit** command to log off and end the CLI session.

help command

This command displays a list of all commands.

Use the **help** command to display a list of all commands with a short description for each. You can also type ? at the command prompt.

history command

This command provides a list of previously issued commands.

Use the **history** command to display an indexed history list of the last eight commands that were issued. The indexes can then be used as shortcuts (preceded by !) to reissue commands from this history list.

Example:
```
system> history
```

```
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Monitor commands

This topic provides an alphabetic list of monitor CLI commands.

There are currently 11 monitor commands:

clearlog command

This command is used to clear the IMM event log.

Use the **clearlog** command to clear the event log of the IMM. You must have the authority to clear event logs to use this command.

Note: This command is intended only for support personnel use.

The following table shows the arguments for the options.

Table 7. clearlog command

The following table is a one-row two column table consisting of the option and option descriptions.

Option	Description
-t <all | platform | audit>	Event type, choose which type of event to clear. If not specified, all event types will be selected.

Event type descriptions

- all: All event type, including platform event and audit event.
- platform: Platform event type.
- audit: Audit event type.

Example:

```
system> clearlog
All event log cleared successfully
system> clearlog -t all
All event log cleared successfully
system> clearlog -t platform
```

```
Platform event log cleared successfully
system> clearlog -t audit
Audit event log cleared successfully
```

fans command

This command is used to display the velocity of the server fans.

Use the **fans** command to display the speed for each of the server fans.

Example:

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

ffdc command

This command is used to generate a new service data file.

Use the first failure data capture (**ffdc**) command to generate and transfer service data to Support.

The following list consist of commands to be used with the **ffdc** command:

- **generate**, create a new service data file
- **status**, check status of service data file
- **copy**, copy existing service data
- **delete**, delete existing service data

The following table shows the arguments for the options.

Table 8. ffdc command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-t	Type number	1 (processor dump) and 4 (service data). The processor dump contains all logs and files available. The service data contains only a subset of the logs and files. The default value is 1.
-f [1]	Remote filename or sftp target directory.	For sftp, use full path or trailing / on directory name (~/ or /tmp/). The default value is the system generated name.
-ip [1]	Address of the tftp/sftp server	
-pn [1]	Port number of the tftp/sftp server	The default value is 69/22.
-u [1]	Username for the sftp server	
-pw [1]	Password for the sftp server	

1. Additional argument for **generate** and **copy** commands

Syntax:

```
ffdc [options]
option:
  -t 1 or 4
  -f
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Example:

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

hreport command

Use this command to show embedded health report.

The following table shows the hreport commands.

Table 9. hreport commands

The following table is a multi-row two column table consisting of the different hreport command descriptions.

Option	Description
generate	Create new health report
status	Check status
copy	Copy existing health report
delete	Delete existing health report

The following table shows the arguments for the generate and copy options.

Table 10. generate and copy command

The following table is a multi-row two column table consisting of the generate and copy command options and option descriptions.

Option	Description
-f	Remote filename or sftp target directory (default is system generated name ((for sftp, use full path or trailing / on directory name (~/ or /tmp/))
-ip	Address of tftp/sftp server
-pn	Port number of tftp/sftp server (default 69/22)
-u	Username for sftp server
-pw	Password for sftp server

mhlog command

Use this command to display maintenance history activity log entries.

The following table shows the arguments for the options.

Table 11. mhlog command

The following table is a multi-row two column table consisting of the options and option descriptions.

Option	Description
-c <count>	Display 'count' entries (1-250)
-i <index>	Display entries starting at index (1-250)
-f	Remote filename of log file
-ip	Address of tftp/sftp server
-pn	Port number of tftp/sftp server (default 69/22)
-u	Username for sftp server
-pw	Password for sftp server

Example

Display will look something like this:

```
Type            Message                                                                  Time
-------------   ------------                                                             ----
Hardware        SAS Backplane1(SN: XXXX9CE009L) is added.                               05/08/2020,04:23:18
Hardware        CPU 1(SKU NO: 50844440) is added.                                        05/08/2020,04:23:22
Hardware        CPU 2(SKU NO: 50844440) is added.                                        05/08/2020,04:23:22
Hardware        M2 Card(SN: R1SH9AJ0037) is added.                                      05/08/2020,04:23:22
Firmware        Primary XCC firmware is updated to TGBT99T by XCC Web.                  05/08/2020,06:40:37
Firmware        Primary XCC firmware is activated to TGBT99T .                          05/08/2020,06:41:26
Hardware        PSU1(SN: D1DG94C0075) is added.                                          05/08/2020,06:43:28
```

led command

Use this command to display and set LED states.

The **led** command displays and sets the server LED states.

- Running the **led** command with no options displays the status of the front panel LEDs.
- The **led -d** command option must be used with **led -identify on** command option.

The following table shows the arguments for the options.

Table 12. led command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-l	Get the status of all system and system subcomponent LEDs	
-chklog	Turn off check log LED	off
-identify	Change state of enclosure identify LED	off, on, blink
-d	Turn on identification LED for specified time period	Time period (seconds)

Syntax:

```
led [options]
option:
  -l
  -chklog off
  -identify state
  -d time
```

Example:

```
system> led
Fault                Off
Identify             On            Blue
Chklog               Off
Power                Off

system> led -l
Label                Location                 State          Color
Battery              Planar                   Off
BMC Heartbeat        Planar                   Blink          Green
BRD                  Lightpath Card           Off
Channel A            Planar                   Off
Channel B            Planar                   Off
Channel C            Planar                   Off
Channel D            Planar                   Off
Channel E            Planar                   Off
Chklog               Front Panel              Off
CNFG                 Lightpath Card           Off
CPU                  Lightpath Card           Off
CPU 1                Planar                   Off
CPU 2                Planar                   Off
DASD                 Lightpath Card           Off
DIMM                 Lightpath Card           Off
DIMM 1               Planar                   Off
DIMM 10              Planar                   Off
DIMM 11              Planar                   Off
DIMM 12              Planar                   Off
DIMM 13              Planar                   Off
```

```
DIMM 14                 Planar                  Off
DIMM 15                 Planar                  Off
DIMM 16                 Planar                  Off
DIMM 2                  Planar                  Off
DIMM 3                  Planar                  Off
DIMM 4                  Planar                  Off
DIMM 5                  Planar                  Off
DIMM 6                  Planar                  Off
DIMM 7                  Planar                  Off
DIMM 8                  Planar                  Off
DIMM 9                  Planar                  Off
FAN                     Lightpath Card          Off
FAN 1                   Planar                  Off
FAN 2                   Planar                  Off
FAN 3                   Planar                  Off
Fault                   Front Panel (+)         Off
Identify                Front Panel (+)         On              Blue
LINK                    Lightpath Card          Off
LOG                     Lightpath Card          Off
NMI                     Lightpath Card          Off
OVER SPEC               Lightpath Card          Off
PCI 1                   FRU                     Off
PCI 2                   FRU                     Off
PCI 3                   FRU                     Off
PCI 4                   FRU                     Off
Planar                  Planar                  Off
Power                   Front Panel (+)         Off
PS                      Lightpath Card          Off
RAID                    Lightpath Card          Off
Riser 1                 Planar                  Off
Riser 2                 Planar                  Off
SAS ERR                 FRU                     Off
SAS MISSING             Planar                  Off
SP                      Lightpath Card          Off
TEMP                    Lightpath Card          Off
VRM                     Lightpath Card          Off
system>
```

readlog command

This command displays the IMM event logs.

Use the **readlog** command to display the IMM event log entries. Five event logs are displayed at a time. The entries are displayed from the most recent to the oldest.

readlog displays the first five entries in the event log, starting with the most recent, on its first execution, and then the next five for each subsequent call.

readlog -a displays all entries in the event log, starting with the most recent.

readlog -f resets the counter and displays the first 5 entries in the event log, starting with the most recent.

readlog -date *date* displays event log entries for the specified date, specified in mm/dd/yy format. It can be a pipe (|) separated list of dates.

readlog -sev *severity* displays event log entries for the specified severity level (E, W, I). It can be a pipe (|) separated list of severity levels.

readlog -i *ip_address* sets the IPv4 or IPv6 IP address of the TFTP or SFTP server where the event log is saved. The **-i** and **-l** command options are used together to specify the location.

readlog -l *filename* sets the file name of the event log file. The **-i** and **-l** command options are used together to specify the location.

readlog -pn *port_number* displays or sets the port number of the TFTP or SFTP server (default 69/22).

readlog -u *username* specifies the user name for the SFTP server.

readlog -pw *password* specifies the password for the SFTP server.

Syntax:
```
readlog [options]
option:
  -a
  -f
  -date date
  -sev severity
  -i ip_address
  -l filename
  -pn port_number
  -u username
  -pw password
```

Example:
```
system> readlog -f
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

syshealth command

This command provides a summary of the health or active events.

Use the **syshealth** command to display a summary of the health or active events of the server. The power state, system state, hardware state (includes fan, power supply, storage, processor, memory), restart count, and IMM software status are displayed.

Syntax:
```
syshealth [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
  cooling - display cooling devices health status
  power - display power modules health status
  storage - display local storage health status
  processors - display processors health status
  memory - display memory health status
```

Example:
```
system> syshealth summary
Power    On
State    OS booted
Restarts 29
```

```
system> syshealth activeevents
No Active Event Available!
```

temps command

This command displays all temperature and temperature threshold information.

Use the **temps** command to display all the temperatures and temperature thresholds. The same set of temperatures are displayed as in the web interface.

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

         WR       W       T      SS      HS
-------------------------------------------
CPU1     N/A     N/A    80/27    N/A     N/A
CPU2     N/A     N/A    80/27    N/A     N/A
DASD1  66/19   73/23   82/28   88/31   92/33
Amb    59/15   70/21   83/28   90/32   95/35
system>
```

Notes:

1. The output has the following column headings:

   WR: warning reset (Positive-going Threshold Hysteresis value)

   W: warning (Upper non-critical Threshold)

   T: temperature (Current value)

   SS: soft shutdown (Upper critical Threshold)

   HS: hard shutdown (Upper non-recoverable Threshold)
2. All temperature values are in degrees Fahrenheit/Celsius.
3. N/A represents not applicable.

volts command

Use this command to display the server voltage information.

Use the **volts** command to display all the voltages and voltage thresholds. The same set of voltages are displayed as in the web interface.

```
Example:
system> volts

      i HSL    SSL    WL     WRL    V      WRH    WH    SSH     HSH
-------------------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75   6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70   3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40  12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40  -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80  -2.70
VRM1                          3.45
VRM2                          5.45
system>
```

Note: The output has the following column headings:

HSL: hard shutdown low (Lower non-recoverable Threshold)

SSL: soft shutdown low (Lower critical Threshold)

WL: warning low (Lower non-critical Threshold)

WRL: warning reset low (Negative-going Threshold Hysteresis value)

V: voltage (current value)

WRH: warning reset high (Positive-going Threshold Hysteresis value)

WH: warning high (Upper non-critical Threshold)

SSH: soft shutdown high (Upper critical Threshold)

HSH: hard shutdown high (Upper non-recoverable Threshold)

vpd command

This command displays configuration and informational data (vital product data) associated with the hardware and software of the server.

Use the **vpd** command to display vital product data for the system (sys), IMM (bmc), server BIOS (uefi), Lenovo XClarity Provisioning Manager (lxpm), server firmware (fw), server components (comp) and PCIe devices (pcie). The same information is displayed as in the web interface.

Syntax:

```
vpd sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw   - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

Example:

```
system> vpd bmc
Type            Status      Version     Build     ReleaseDate
----            -------      -----      ------
BMC (Primary)   Active      0.00       DVI399T    2017/06/06
BMC (Backup)    Inactive    1.00       TEI305J    2017/04/13

system>
```

Server power and restart control commands

This topic provides an alphabetic list of power and restart CLI commands.

There are currently 4 server power and restart commands:

power command

This command describes how to control the server power.

Use the **power** command to control the server power. To issue **power** commands, you must have the Remote Server Power/Restart Access authority level.

The following table contains a subset of commands that can be used with the **power** command.

Table 13. power command

The following table is a multi-row three column table consisting of the power commands, command descriptions, and associated values for the commands.

Command	Description	Value
power on	Use this command to turn on the server power.	on, off
power off	Use this command to turn off the server power. **Note:** The **-s** option shuts down the operating system before the server is turned off.	on, off
power cycle	Use this command to turn off the server power and then turn on the server power. **Note:** The **-s** option shuts down the operating system before the server is turned off.	
power enterS3	Use this command to place the operating system into the S3 (sleep) mode. **Note:** This command is used only when the operating system is on. The S3 mode is not supported on all servers.	
power rp	Use this option to specify the host power restore policy.	alwayson|alwaysoff|restore
power S3resume	Use this command to wake up the operating system from the S3 (sleep) mode. **Note:** This command is used only when the operating system is on. The S3 mode is not supported on all servers.	
power state	Use this command to display the server power state and the current state of the server.	on, off

The following table contains the options for the **power on**, **power off**, and **power cycle** commands.

Table 14. power command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 14. power command (continued)

Option	Description	Values
-s	Use this option to shut down the operating system before the server is turned off. **Note:** The **-s** option is implied when using the **-every** option for the **power off** and **power cycle** commands.	
-every	Use this option with the **power on**, **power off**, and **power cycle** commands to control the server power. You can set up the dates, times, and frequency (daily or weekly) to power on, power off, or power cycle your server.	**Note:** The values for this option are presented on separate lines due to space limitations. Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear
-t	Use this option to specify the time in hours and minutes to power on the server, shut down the operating system, and power off or restart the server.	Use the following format: hh:mm
-d	Use this option to specify the date to power on the sever. This is an additional option for the **power on** command. **Note:** The **-d** and **-every** options, cannot be used together on the same command.	Use the following format: mm/dd/yyyy
-clear	Use this option to clear the scheduled power on date. This is an additional option for the **power on** command.	

Syntax:

```
power on
power off [-s]
power state
power cycle [-s]
```

The following information are examples of the **power** command.

To shut down the operating system and power off the server every Sunday at 1:30, enter the following command:

```
system> power off
-every Sun -t 01:30
```

To shut down the operating system and restart the server every day at 1:30, enter the following command:

```
system> power cycle
-every Day -t 01:30
```

To power on the server every Monday at 1:30, enter the following command:

```
system> power on
-every Mon -t 13:00
```

To power on the server on Dec 31 2013 at 11:30 PM, enter the following command:

```
system> power on
-d 12/31/2013 -t 23:30
```

To clear a weekly power cycle, enter the following command:

```
system> power cycle
-every clear
```

reset command

This command describes how to reset the server.

Use the **reset** command to restart the server. To use this command, you must have power and restart access authority.

The following table shows the arguments for the options.

Table 15. reset command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-s	Shut down the operating system before the server is reset.	
-d	Delay performing the reset for the given number of seconds.	0 - 120
-nmi	Generate a non-maskable interrupt (NMI)) on the server.	

Syntax:

```
reset [option]
option:
-s
-d
-nmi
```

fuelg command

This command displays information about the server power.

Use the **fuelg** command to display information about server power usage and configure server power management. This command also configures policies for power redundancy loss. The following table shows the arguments for the options.

Table 16. fuelg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-pme	Enable or disable power management and capping on the server.	on, off
-pcapmode	Set the power capping mode for the server.	input, output
-pcap	A numeric value that falls within the range of power capping values displayed when running the fuelg command, with no options, on the target.	numeric wattage value
-history	Display power consumption or performance history	pc, perf
-period	A numeric value to display history (1, 6, 12, 24 hours)	numeric value in hours

Table 16. fuelg command (continued)

Option	Description	Values
-pm	Set the policy mode for loss of redundant power.	• **bt**- basic with throttling • **rt**- redundant with throttling (default) • **ort**- N_1 redundant with throttling
-zm	Enable or disable zero output mode. This setting can only be set when the policy mode is set to redundant with throttling.	on, off
-perf	Display the current compute utilization, including system, microprocessor, and I/O.	percentage
-pc	Display current power consumption	• **output**- display current DC power consumption. For Rack and Tower servers it will include the power consumption of the system, CPU, memory and other components, For ITE blade servers it will only include the system power consumption. • **input**- Display current input power consumption, including system power consumption.

Syntax:
```
fuelg [options]
option:
  -pme on|off
  -pcapmode input|output
  -pcap
  -history
  -period
  -pm bt|r|rt
  -zm on|off
  -perf
  -pc input|output
```

Example:
```
system> fuelg
-pme: on
system>
```

pxeboot command

This command displays and sets the condition of the Preboot eXecution Environment.

Running **pxeboot** with no options, returns the current Preboot eXecution Environment setting. The following table shows the arguments for the options.

Table 17. pxeboot command

The following table is a single-row three column table consisting of the option, option description, and associated values for the option.

Table 17. pxeboot command (continued)

Option	Description	Values
-en	Sets the Preboot eXecution Environment condition for the next system restart.	enabled, disabled

Syntax:
```
pxeboot [options]
option:
  -en state
```

Example:
```
system> pxeboot
-en disabled
system>
```

Serial redirect command

This topic contains the serial redirect command.

There is only one serial redirect command: the “console command” on page 107.

console command

This command is used to start a serial redirect console session.

Use the **console** command to start a serial redirect console session to the designated serial port of the IMM.

Syntax:
```
console 1
```

Configuration commands

This topic provides an alphabetic list of configuration CLI commands.

There are currently 41 configuration commands:

accseccfg command

Use this command to display and configure account security settings.

Running the **accseccfg** command with no options displays all account security information. The following table shows the arguments for the options.

Table 18. accseccfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-am	Sets user authentication method.	local, ldap, localldap, ldaplocal
-lp	Lockout period after maximum login failures (minutes).	Between 0 and 2880, 0 = lockout period does not expire

Table 18. accseccfg command (continued)

Option	Description	Values
-pe	Password expiration time period (days).	Between 0 and 365, 0 = never expire
-pew	Password expiration warning time period **Note:** The Password expiration warning time period must be less than Password expiration time period.	Between 0 and 30, 0 = never warn
-pl	Password length.	If password complexity rules are enabled, the password length is between 8 and 32. Otherwise, it is between 0 and 32.
-ci	Minimum password change interval (hours).	between 0 and 240, 0 = change immediately
-lf	Maximum number of login failures.	Between 0 and 10, 0 = never locked
-chgdft	Change default password after first login.	on, off
-chgnew	Change new user password after first login.	on, off
-rc	Password reuse cycle.	Between 0 and 10, 0 = reuse immediately
-wt	Web and Secure Shell inactivity session timeout (minutes).	Between 0 and 1440

Syntax:

```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication method
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgdft state
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

Example:

```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
```

```
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

alertcfg command

Use this command to display and configure the IMM global remote alert parameters.

Running the **alertcfg** command with no options displays all global remote alert parameters. The following table shows the arguments for the options.

Table 19. alertcfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-dr	Sets wait time between retries before the IMM resends an alert.	0 to 4.0 minutes, in 0.5 minute increments
-da	Sets wait time before the IMM sends an alert to the next recipient in the list.	0 to 4.0 minutes, in 0.5 minute increments
-rl	Sets the number of additional times that the IMM attempts to send an alert, if previous attempts were unsuccessful.	0 to 8

Syntax:

```
alertcfg [options]
  options:
   -rl retry_limit
   -dr retry_delay
   -da agent_delay
```

Example:

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

asu command

This command is used to configure UEFI settings.

Advanced Settings Utility commands (ASU) are used to configure UEFI settings. The host system must be rebooted for any UEFI setting changes to take effect.

The following table contains a subset of commands that can be used with the **asu** command.

Table 20. asu command

The following table is a multi-row three column table consisting of a subset of commands that can be used in conjunction with the **asu** command. Descriptive information and associated values for the commands are provided.

Command	Description	Value
delete	Use this command to delete an instance or record of a setting. The setting must be an instance that allows deletion, for example, iSCSI.AttemptName.1.	*setting_instance*
help	Use this command to display help information for one or more settings.	*setting*
set	Use this command to change the value of a setting. Set the UEFI setting to the input value. **Notes:** • Set one or more setting/value pairs. • The setting can contain wildcards if it expands to a single setting. • The value must be enclosed in quotes if it contains spaces. • Ordered list values are separated by the equal symbol (=). For example, set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network."	*setting value*
showgroups	Use this command to display the available setting groups. This command displays the names of known groups. Group names may vary depending on the installed devices.	*setting*
show	Use this command to display the current value of one or more settings.	*setting*
showvalues	Use this command to display all possible values for one or more settings. **Notes:** • This command will display information about the allowable values for the setting. • The minimum and maximum number of instances allowed for the setting is displayed. • The default value will be displayed if available. • The default value is enclosed with opening and closing angle brackets (< and >). • Text values show the minimum and maximum length and regular expression.	*setting*
Notes: • In the command syntax, *setting* is the name of a setting that you want to view or change, and *value* is the value that you are placing on the setting. • *Setting* can be more than one name, except when using the **set** command. • *Setting* can contain wildcards, for example an asterisk (*) or a question mark (?). • *Setting* can be a group, a setting name, or **all**.		

Examples of the syntax for the **asu** command are presented in the following list:

- To display all of the asu command options enter `asu --help`.
- To display verbose help for all commands enter `asu -v --help`.
- To display verbose help for one command enter `asu -v set --help`.
- To change a value enter `asu set` *setting value*.
- To display the current value enter `asu show` *setting*.
- To display settings in long batch format enter `asu show -l -b all`
- To display all possible values for a setting enter `asu showvalues` *setting*. Example **show values** command:

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

The following table shows the arguments for the options.

Table 21. asu options

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-b	Display in batch format.	
--help[1]	Display command usage and options. The --help option is placed before the command, for example **asu --help show**.	
--help[1]	Display help for the command. The --help option is placed after the command, for example, **asu show --help**.	
-l	Long format setting name (include the configuration set).	
-m	Mixed format setting name (use the configuration id).	
-v[2]	Verbose output.	

1. The --help option can be used with any command.
2. The -v option is used only between **asu** and the command.

Syntax:

```
asu [options] command [cmdopts]
options:
   -v verbose output
   --help display main help
cmdopts:
   --help help for the command
```

Note: See individual commands for more command options.

Use the asu transaction commands to set multiple UEFI settings and create and execute batch mode commands. Use the **tropen** and **trset** commands to create a transaction file containing multiple settings to be applied. A transaction with a given id is opened using the **tropen** command. Settings are added to the set

using the **trset** command. The completed transaction is committed using the **trcommit** command. When you are finished with the transaction, it can be deleted with the **trrm** command.

Note: The UEFI settings restore operation will create a transaction with an id using a random three digit number.

The following table contains transaction commands that can be used with the **asu** command.

Table 22. asu transaction commands

The following table is a multi-row three column table consisting of the transactions commands, the command descriptions, and associated values for the commands.

Command	Description	Value
tropen *id*	This command creates a new transaction file containing several settings to be set.	*Id* is the identifying string, 1 - 3 alphanumeric characters.
trset *id*	This command adds one or more settings or value pairs to a transaction.	*Id* is the identifying string, 1 - 3 alphanumeric characters.
trlist *id*	This command displays the contents of the transaction file first. This can be useful when the transaction file is created in the CLI shell.	*Id* is the identifying string, 1 - 3 alphanumeric characters.
trcommit *id*	This command commits and executes the contents of the transaction file. The results of the execution and any errors will be displayed.	*Id* is the identifying string, 1 - 3 alphanumeric characters.
trrm *id*	This command removes the transaction file after it has been committed.	*Id* is the identifying string, 1 - 3 alphanumeric characters.

Example of establishing multiple UEFI settings:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

backup command

Use this command to create a backup file containing the current system security settings.

The following table shows the arguments for the options.

Table 23. backup command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 23. backup command (continued)

Option	Description	Values
-f	Backup file name	Valid file name
-pp	Password or pass-phrase used to encrypt passwords inside the backup file	Valid password or quote-delimited pass-phrase
-ip	IP address of TFTP/SFTP server	Valid IP address
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22)
-u	Username for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password
-fd	Filename for XML description of backup CLI commands	Valid filename

Syntax:

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

Example:

```
system> backup f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

dhcpinfo command

Use this command to view the DHCP server-assigned IP configuration for eth0.

Use the **dhcpinfo** command to view the DHCP server-assigned IP configuration for eth0, if the interface is configured automatically by a DHCP server. You can use the **ifconfig** command to enable or disable DHCP.

Syntax:

```
dhcpinfo eth0
```

Example:

```
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

The following table describes the output from the example.

Table 24. dhcpinfo command

The following table is a multi-row two column table describing the options that are used in the previous example.

Option	Description
-server	DHCP server that assigned the configuration
-n	Assigned host name
-i	Assigned IPv4 address
-g	Assigned gateway address
-s	Assigned subnet mask
-d	Assigned domain name
-dns1	Primary IPv4 DNS server IP address
-dns2	Secondary IPv4 DNS IP address
-dns3	Tertiary IPv4 DNS server IP address
-i6	IPv6 address
-d6	IPv6 domain name
-dns61	Primary IPv6 DNS server IP address
-dns62	Secondary IPv6 DNS IP address
-dns63	Tertiary IPv6 DNS server IP address

dns command

Use this command to view and set the DNS configuration of the IMM.

Note: In a Flex System, DNS settings cannot be modified on the IMM. DNS settings are managed by the CMM.

Running the **dns** command with no options displays all DNS configuration information. The following table shows the arguments for the options.

Table 25. dns command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-state	DNS state	on, off
-ddns	DDNS state	enabled, disabled
-i1	Primary IPv4 DNS server IP address	IP address in dotted decimal IP address format.
-i2	Secondary IPv4 DNS IP address	IP address in dotted decimal IP address format.
-i3	Tertiary IPv4 DNS server IP address	IP address in dotted decimal IP address format.
-i61	Primary IPv6 DNS server IP address	IP address in IPv6 format.
-i62	Secondary IPv6 DNS IP address	IP address in IPv6 format.
-i63	Tertiary IPv6 DNS server IP address	IP address in IPv6 format.
-p	IPv4/IPv6 priority	ipv4, ipv6

Syntax:

```
dns [options]
option:
  -state state
  -ddns state
  -i1 first_ipv4_ip_address
  -i2 second_ipv4_ip_address
  -i3 third_ipv4_ip_address
  -i61 first_ipv6_ip_address
  -i62 second_ipv6_ip_address
  -i63 third_ipv6_ip_address
  -p priority
```

Note: The following example shows an IMM configuration where DNS is disabled.

Example:

```
system> dns
   -state   :  disabled
   -i1      :  0.0.0.0
   -i2      :  0.0.0.0
   -i3      :  0.0.0.0
   -i61     :  ::
   -i62     :  ::
   -i63     :  ::
   -ddns    :  enabled
   -dnsrc   :  DHCP
   -ddn     :
   -ddncur  :  labs.lenovo.com
   -p       :  ipv6
   -dscvry  :  enabled

system>
```

The following table describes the options used in the previous example.

Table 26. dns command output

The following table is a multi-row two column table describing the options used in the previous example.

Table 26. dns command output (continued)

Option	Description
-state	State of DNS (`on` or `off`)
-i1	Primary IPv4 DNS server IP address
-i2	Secondary IPv4 DNS IP address
-i3	Tertiary IPv4 DNS server IP address
-i61	Primary IPv6 DNS server IP address
-i62	Secondary IPv6 DNS IP address
-i63	Tertiary IPv6 DNS server IP address
-ddns	State of DDNS (`enabled` or `disabled`)
-dnsrc	Preferred DDNS domain name (`dhcp` or `manual`)
-ddn	Manually specified DDN
-ddncur	Current DDN (read only)
-p	Preferred DNS servers (`ipv4` or `ipv6`)

encaps command

Use this command to let the BMC quit encapsulation mode.

The following table shows the arguments for the options.

Table 27. encaps command

The following table is a one-row two column table consisting of the options and option descriptions.

Option	Description
lite off	Let BMC quit encapsulation mode and open global access to all users

ethtousb command

Use the **ethtousb** command to display and configure Ethernet to Ethernet-over-USB port mapping.

The command allows you to map an external Ethernet port number to a different port number for Ethernet-over-USB.

Running the **ethtousb** command with no options displays Ethernet-over-USB information. The following table shows the arguments for the options.

Table 28. ethtousb command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 28. ethtousb command (continued)

Option	Description	Values
-en	Ethernet-over-USB state	enabled, disabled
-m*x*	Configure port mapping for index *x*	Port pair, separated by a colon (:), of the form *port1:port2* Where: • The port index number, *x*, is specified as an integer from 1 to 10 in the command option. • *port1* of the port pair is the External Ethernet port number. • *port2* of the port pair is the Ethernet-over-USB port number.
-rm	Remove port mapping for specified index	1 through 10 Port map indexes are displayed using the **ethtousb** command with no options.

Syntax:
```
ethtousb [options]
option:
  -en state
  -mxport_pair
  -rm map_index
```

Example:
```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

firewall command

Use this command to configure the firewall to restrict access from certain addresses and optionally limits access time frame. If no option is specified, the current settings will be displayed.

The following table shows the arguments for the options.

Table 29. firewall command

The following table is a multi-row three column table consisting of the options and option descriptions.

Option	Description	Values
-bips	Block 1-3 IP addresses (comma separated, CIDR or range)	Valid IP addresses **Note:** IPv4 and IPv6 addresses can use CIDR format to block a range of addresses.
-bmacs	Block 1-3 MAC addresses (comma separated)	Valid MAC addresses **Note:** MAC address filtering works only with specific addresses.
-bbd	Block begin date	Date with format <YYYY-MM-DD>
-bed	Block end date	Date with format <YYYY-MM-DD>
-bbt	Block begin time	Time with format <HH:MM>

Table 29. firewall command (continued)

Option	Description	Values
-bet	Block end time	Time with format <HH:MM>
-bti	Block 1-3 time intervals (comma separated) e.g., *firewall - bti 01:00–02:00,05:05–10:30* will block access during 01:00-02:00 & 05:05-10:30 every day	Time range with format <HH:MM-HH:MM>
-clr	Clear the firewall rule for a given type	ip, mac, datetime, interval, all
The following options are for IP address blocking		
-iplp	IP address lockout period in minutes.	Numeric value between 0 and 2880, 0 = never expire
-iplf	Maximum number of login failures before IP address is locked out. **Note:** If this value is not 0, then it must be greater than or equal to <Maximum number of login failures> that is set by <*accseccfg -lf*>	Numeric value between 0 and 32, 0 = never lock
-ipbl	Show/configure the list of IP addresses being locked out.	del, clrall, show • **-del**: delete an IPv4 or IPv6 address from block list • **-clrall**: clear all blocking IP • **-show**: show all blocking IPs

Example:

```
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips  192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”:  Delete all blocking IP addresses.
· “firewall –ipbl –show”:    Show all blocking IP addresses.
```

gprofile command

Use this command to display and configure group profiles for the IMM.

The following table shows the arguments for the options.

Table 30. gprofile command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 30. gprofile command (continued)

Option	Description	Values
-clear	Delete a group	enabled, disabled
-n	The name of the group	String of up to 63 characters for *group_name*. The *group_name* must be unique.
-a	Role-based authority level	supervisor, operator, rbs <role list>: nsc|am|rca|rcvma|pr|bc|cel|ac Role list values are specified using a pipe separated list of values.
-h	Display the command usage and options	

Syntax:

```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n  group_name
-a  authority level:
    -nsc network and security
    -am user account management
    -rca remote console access
    -rcvma remote console and remote disk access
    -pr remote server power/restart access
    -bc basic adapter configuration
    -cel ability to clear event logs
    -ac advanced adapter configuration
-h help
```

hashpw command

Use this command with the -sw option to enable/disable the third-party password function or with the -re option to enable/disable the allowance of retrieving third-party password.

The following table shows the arguments for the options.

Table 31. hashpw command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-sw	Third-Party Password switch status	enabled, disabled
-re	Third-Party Password read status **Note:** Read can be set if the switch is enabled.	enabled, disabled

Example:

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f - r Administrator
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account      Login ID      Advanced Attribute               Role            Password Expires
 -------      --------      ------------------             ------            ----------------
```

```
    1           USERID                    Native                  Administrator      Password doesn't expire
5           guest5    Third-party Password              Administrator                    90 day(s)
```

ifconfig command

Use this command to configure the Ethernet interface.

Type `ifconfig eth0` to display the current Ethernet interface configuration. To change the Ethernet interface configuration, type the options, followed by the values. To change the interface configuration, you must have at least Adapter Networking and Security Configuration authority.

Note: In a Flex System, the VLAN settings are managed by a Flex System CMM and cannot be modified on the IMM.

The following table shows the arguments for the options.

Table 32. ifconfig command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-b	Burned-in MAC Address (read-only and not configurable)	
-state	Interface state	disabled, enabled
-c	Configuration method	dhcp, static, dthens (dthens corresponds to the **try dhcp server, if it fails use static config** option on the web interface)
-i	Static IP address	Address in valid format.
-g	Gateway address	Address in valid format.
-s	Subnet mask	Address in valid format.
-n	Host name	String of up to 63 characters. The string can include letters, digits, periods, underscores, and hyphens.
-r	Data rate	10, 100, auto
-d	Duplex mode	full, half, auto
-m	MTU	Numeric between 60 and 1500.
-l	LAA	MAC address format. Multicast addresses are not allowed (the first byte must be even).
-dn	Domain name	Domain name in valid format.
-auto	Autonegotiation setting, which determines whether the Data rate and Duplex network settings are configurable	true, false
-ghn	Obtain hostname from DHCP	disabled, enabled
-nic	switch NIC mode[1]	shared, dedicated, shared:nixX[2]
-failover[2]	Failover mode	none, shared, shared:nicX
-nssync[3]	Network setting synchronization	enabled, disabled

Table 32. ifconfig command (continued)

Option	Description	Values
-address_table	Table of automatically-generated IPv6 addresses and their prefix lengths **Note:** The option is visible only if IPv6 and stateless auto-configuration are enabled.	This value is read-only and is not configurable.
-ipv6	IPv6 state	disabled, enabled
-lla	Link-local address **Note:** The link-local address only appears if IPv6 is enabled.	The link-local address is determined by the IMM. This value is read-only and is not configurable.
-ipv6static	Static IPv6 state	disabled, enabled
-i6	Static IP address	Static IP address for Ethernet channel 0 in IPv6 format.
-p6	Address prefix length	Numeric value between 1 and 128.
-g6	Gateway or default route	IP address for the gateway or default route for Ethernet channel 0 in IPv6.
-dhcp6	DHCPv6 state	enabled, disabled
-sa6	IPv6 stateless autoconfig state	enabled, disabled
-vlan	Enable or disable the VLAN tagging	enabled, disabled
-vlanid	Network packet identification tag for the IMM	Numeric value between 1 and 4094.

Notes:

1. -nic will also show the status of nic. [active] indicates which nic XCC is currently using

   For example:
   ```
   -nic: shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot 5 [active]
   ```
   Indicates that nic3 is in shared mode, on slot 5, nic2 is on slot3, nic1 is XCC dedicated port and XCC is using nic3.
2. The shared:nicX value is available on servers that have an optional mezzanine network card installed. This mezzanine network card can be used by the IMM.
3. If the IMM is configured to use the dedicated management network port, the -failover option will direct the IMM to switch to the shared network port if the dedicated port is disconnected.
4. If the failover mode is enabled, the -nssync option directs the IMM to use the same network settings that are used on the dedicated management network port for the shared network port.

Syntax:

```
ifconfig eth0 [options]
options:

  -state interface_state
  -c config_method
  -i static_ipv4_ip_address
  -g ipv4_gateway_address
  -s subnet_mask
  -n hostname
  -r data_rate
  -d duplex_mode
  -m max_transmission_unit
```

-l *locally_administered_MAC*
-b *burned_in_MAC_address*
-dn *domain_name*
-auto *state*
-nic *state*
-failover mode
-nssync *state*
-address_table
-lla ipv6_link_local_addr
-dhcp6 *state*
-ipv6 *state*
-ipv6static *state*
-sa6 *state*
-i6 *static_ipv6_ip_address*
-g6 *ipv6_gateway_address*
-p6 *length*
-vlan *state*
-vlanid *VLAN ID*

Example:

```
system> ifconfig eth0
-state    :   enabled
-c        :   dthens
-ghn      :   disabled
-i        :   192.168.70.125
-g        :   0.0.0.0
-s        :   255.255.255.0
-n        :   IMM00096B9E003A
-auto     :   true
-r        :   auto
-d        :   auto
-vlan     :   disabled
-vlanid   :   1
-m        :   1500
-b        :   00:09:6B:9E:00:3A
-l        :   00:00:00:00:00:00
-dn       :
-ipv6     :  enabled
-ipv6static :  disabled
-i6       :  ::
-p6       :  64
-g6       :  ::
-dhcp6    :  enabled
-sa6      :  enabled
-lla      :  fe80::6eae:8bff:fe23:91ae
-nic :  shared:nic3
      nic1: dedicate
      nic2: ext card slot #3
      nic3: ext card slot #5  [active]
-address_table    :

system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
```

keycfg command

Use this command to display, add, or delete activation keys.

Activation keys control access to optional IMM functionality.

Notes:

- When the **keycfg** command is run without any options, the list of installed activation keys is displayed. Key information displayed includes an index number for each activation key, the type of activation key, the date through which the key is valid, the number of uses remaining, the key status, and a key description.
- Add new activation keys through file transfer.
- Delete old keys by specifying the number of the key or the type of key. When deleting keys by type, only the first key of a given type is deleted.

The following table shows the arguments for the options.

Table 33. keycfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-add	Add activation key	Values for the -ip, -pn, -u, -pw, and -f command options
-ip	IP address of TFTP server with activation key to add	Valid IP address for TFTP server
-pn	Port number for TFTP/SFTP server with activation key to add	Valid port number for TFTP/SFTP server (default 69/22)
-u	User name for SFTP server with activation key to add	Valid user name for SFTP server
-pw	Password for SFTP server with activation key to add	Valid password for SFTP server
-f	File name for activation key to add	Valid file name for activation key file
-del	Delete activation key by index number	Valid activation key index number from **keycfg** listing
-deltype	Delete activation key by key type	Valid key type value

Syntax:

```
keycfg [options]
option:
  -add
     -ip tftp/sftp server ip address
     -pn pn port number of tftp/sftp server (default 69/22)
     -u  username for sftp server
     -pw password for sftp server
     -f  filename
     -del   n ( where n is a valid ID number from listing)
     -deltype x ( where x is a Type value)
```

Example:

```
system> keycfg
ID  Type  Valid            Uses            Status    Description
1   4     10/10/2010       5                "valid"   "IMM remote presence"
2   3     10/20/2010       2                "valid"   "IMM feature
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

Note: The **Description** field for ID number 3 is displayed on separate lines due to space limitations.

ldap command

Use this command to display and configure the LDAP protocol configuration parameters.

The following table shows the arguments for the options.

Table 34. ldap command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-a	User authentication method	local only, LDAP only, local first then LDAP, LDAP first then local
-aom	Authentication only mode	enabled, disabled
-b	Binding method	anonymous, bind with ClientDN and password, bind with Login Credential
-c	Client distinguished name	String of up to 127 characters for *client_dn*
-d	Search domain	String of up to 63 characters for *search_domain*
-f	Group filter	String of up to 127 characters for *group_filter*
-fn	Forest name	For active directory environments. String of up to 127 characters.
-g	Group search attribute	String of up to 63 characters for *group_search_attr*
-l	Login permission attribute	String of up to 63 characters for *string*
-p	Client password	String of up to 15 characters for *client_pw*
-pc	Confirm client password	String of up to 15 characters for *confirm_pw* Command usage is: ldap -p *client_pw* -pc *confirm_pw* This option is required when you change the client password. It compares the *confirm_pw* argument with the *client_pw* argument. The command will fail if the arguments do not match.
-ep	Encrypted password	Backup/restore password (internal use only)
-r	Root entry distinguished name (DN)	String of up to 127 characters for *root_dn*
-rbs	Enhanced Role-Based Security for active directory users	enabled, disabled
-s1ip	Server 1 host name/IP address	String up to 127 characters or an IP address for *host name/ip_addr*
-s2ip	Server 2 host name/IP address	String up to 127 characters or an IP address for *host name/ip_addr*
-s3ip	Server 3 host name/IP address	String up to 127 characters or an IP address for *host name/ip_addr*
-s4ip	Server 4 host name/IP address	String up to 127 characters or an IP address for *host name/ip_addr*
-s1pn	Server 1 port number	A numeric port number up to 5 digits for *port_number*

Table 34. ldap command (continued)

Option	Description	Values
-s2pn	Server 2 port number	A numeric port number up to 5 digits for *port_number*
-s3pn	Server 3 port number	A numeric port number up to 5 digits for *port_number*
-s4pn	Server 4 port number	A numeric port number up to 5 digits for *port_number*
-t	Server target name	When the rbs option is enabled, this field specifies a target name that can be associated with one or more roles on the Active Directory server through the Role-Based Security (RBS) Snap-In tool.
-u	UID search attribute	String of up to 63 characters for *search_attrib*
-v	Get LDAP server address through DNS	off, on
-h	Displays the command usage and options	

Syntax:

```
ldap [options]
options:
   -a loc|ldap|locld|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -ep encrypted_pw
   -r root_dn
   -rbs enable|disabled
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s4ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -s4pn port_number
   -t name
   -u search_attrib
   -v off|on
   -h
```

ntp command

Use this command to display and configure the Network Time Protocol (NTP).

The following table shows the arguments for the options.

Table 35. ntp command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 35. ntp command (continued)

Option	Description	Values
-en	Enables or disables the Network Time Protocol.	enabled, disabled
-i[1]	Name or IP address of the Network Time Protocol server. This is the index number of the Network Time Protocol server.	The name of the NTP server to be used for clock synchronization. The range of the index number of the NTP server is from -i1 through -i4.
-f	The frequency (in minutes) that the IMM clock is synchronized with the Network Time Protocol server.	3 - 1440 minutes
-synch	Requests an immediate synchronization with the Network Time Protocol server.	No values are used with this parameter.

1. -i is the same as i1.

Syntax:
```
ntp [options]
options:
-en state
-i  hostname/ip_addr
-f  frequency
-synch
```

Example:
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

portcfg command

Use this command to configure the IMM for the serial redirection feature.

The IMM must be configured to match the server internal serial port settings. To change the serial port configuration, type the options, followed by the values. To change the serial port configuration, you must have at least Adapter Networking and Security Configuration authority.

Note: The server external serial port can only be used by the IMM for IPMI functionality. The CLI is not supported through the serial port. The **serred** and **cliauth** options that were present in the Remote Supervisor Adapter II CLI are not supported.

Running the **portcfg** command with no options displays serial port configuration. The following table shows the arguments for the options.

Note: The number of data bits (8) is set in the hardware and cannot be changed.

Table 36. portcfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 36. portcfg command (continued)

Option	Description	Values
-b	Baud rate	9600, 19200, 38400, 57600, 115200
-p	Parity	none, odd, even
-s	Stop bits	1, 2
-climode	CLI mode	0, 1, 2 Where: • 0 = none: The CLI is disabled • 1 = cliems: The CLI is enabled with EMS-compatible keystroke sequences • 2 = cliuser: The CLI is enabled with user-defined keystroke sequences

Syntax:

```
portcfg [options]
 options:
   -b baud_rate
   -p parity
   -s stopbits
   -climode mode
```

Example:

```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

portcontrol command

Use this command to turn a network service port on or off.

Currently this command only supports control of the port for the IPMI protocol. Type **portcontrol** to display the IPMI port state. To enable or disable the IPMI network port, type the **-ipmi** option followed by the **on** or **off** values.

Table 37. portcontrol command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-all	Enable or disable all interfaces and discovery protocols	on, off
-cim	Enable or disable CIM discovery	on, off
-ipmi	Enable or disable the ipmi access via LAN	on, off

Table 37. portcontrol command (continued)

Option	Description	Values
-ipmi-kcs	Enable or disable ipmi access from server	on, off
-rest	Enable or disable REST discovery	on, off
-slp	Enable or disable SLP discovery	on, off
-snmp	Enable or disable SNMP discovery	on, off
-ssdp	Enable or disable SSDP discovery	on, off
-cli	Enable or disable CLI discovery	on, off
-web	Enable or disable WEB discovery	on, off

Syntax:

```
portcontrol [options]
 options:
   -ipmi on/off
```

Example:

```
system> portcontrol
cim : on
ipmi : on
ipmi-kcs : on
rest : on
slp : on
snmp : off
ssdp : on
cli : on
web : on
```

ports command

Use this command to display and configure IMM ports.

Running the **ports** command with no options displays information for all IMM ports. The following table shows the arguments for the options.

Table 38. ports command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-open	Display open ports	
-reset	Reset ports to default settings	
-httpp	HTTP port number	Default port number: 80

Table 38. ports command (continued)

Option	Description	Values
-httpsp	HTTPS port number	Default port number: 443
-sshp	SSH legacy CLI port number	Default port number: 22
-snmpap	SNMP agent port number	Default port number: 161
-snmptp	SNMP traps port number	Default port number: 162
-rpp	Remote presence port number	Default port number: 3900
-cimhp	CIM over HTTP port number	Default port number: 5988
-cimhsp	CIM over HTTPS port number	Default port number: 5989

Syntax:

```
ports [options]
option:
  -open
  -reset
  -httpp port_number
  -httpsp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

Example:

```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-cimhp 5988
-cimhsp 5989
system>
```

rdmount command

Use this command to mount remote disk images or network shares

The following table shows the arguments for the options.

Table 39. rdmount command

The following table is a multi-row two column table consisting of the options and option descriptions.

Notes:

- Up to two files can be uploaded in the XClarity Controller memory and mounted as virtual media using the XClarity Controller RDOC feature. The total size for both files must not exceed 50 MB. The uploaded images are read only unless the –rw option is used.
- When using the HTTP, SFTP, or FTP protocols to mount or map the images, the total size for all the images must not exceed 50 MB. There is no size limit if the NFS or SAMBA protocols are used.

Table 39. rdmount command (continued)

Option	Description
-r	rdoc operation (if used, must be first option) -r -map: mount the RDOC images -r -unmap<filename>: unmount the mounted RDOC images -r -maplist: shows the mounted RDOC images via the XClarity Controller web browser and the CLI interface
-map	-t <samba|nfs|http|sftp|ftp> filesystem type -ro read-only -rw read-write -u user -p password -l file location (URL format) -o option (extra option string for samba and nfs mounts) -d domain (domain for samba mount)
-maplist	shows the mapped images
-unmap <id|fname>	use id with network images, filename with rdoc
-mount	mount the mapped images
-unmount	unmount the mounted images

restore command

Use this command to restore system settings from a backup file.

The following table shows the arguments for the options.

Table 40. restore command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-f	Backup file name	Valid file name
-pp	Password or pass-phrase used to encrypt passwords inside the backup file	Valid password or quote-delimited pass-phrase
-ip	IP address of TFTP/SFTP server	Valid IP address
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22)
-u	Username for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password

Syntax:

```
restore [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
username
  -pw password
```

Example:

```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

restoredefaults command

Use this command to restore all IMM settings to the factory default.

- There are no options for the **restoredefaults** command.
- You will be asked to confirm the command before it is processed.

Syntax:

```
restoredefaults
```

Example:

```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

roles command

Use this command to display or configure roles.

The following table shows the arguments for the options.

Table 41. roles command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 41. roles command (continued)

Option	Description	Values
-n	Role to configure	Limited to 32 characters
-p	Set privileges	custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us • **am**: User account management access • **rce**: Remote console access • **rcvma**: Remote console and remote disk (virtual media) access • **pr**: Remote server power/restart access • **cel**: Ability to clear event logs • **bc**: Adapter Configuration (basic) • **nsc**: Adapter Configuration (network and security) • **ac**: Adapter Configuration (advanced) • **us**: UEFI Security **Note:** the above custom permission flags can be used in any combination
d	Delete a row	

Syntax

```
   roles [-options] - display/configure roles
   - role_account -role number[3-31]
options:
   -n        - role name (limited to 32 characters)
   -p        - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
      am     - User account management access
      rca    - Remote console access
      rcvma  - Remote console and remote disk (virtual media) access
      pr     - Remote server power/restart access
      cel    - Ability to clear event logs
      bc     - Adapter Configuration (basic)
      nsc    - Adapter Configuration (network and security)
      ac     - Adapter Configuration (advanced)
      us     - UEFI Security
      Note: the above custom permission flags can be used in any combination
   -d        - delete a row
```

Example

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok



system> roles
Account              Role                            Privilege                    Assigned To
------- ----------------------------------   -------------------------     -------------------------------
    0                    Administrator                    all                          USERID
    1                         ReadOnly                      none
    2                         Operator            custom:pr|cel|bc|nsc
    3                            test1             custom:am|rca|rcvma
```

seccfg command

Use this command to perform firmware rollback.

The following table shows the arguments for the options.

Table 42. seccfg command

The following table is a multi-row two column table consisting of the options and option descriptions.

Option	Description
-fwrb	Allows firmware rollback to previous versions (yes/no)
-rppen	Remote physical presence enable (read only)
-rppto	Remote physical presence timeout (read only)
-rpp <yes/no?	Physical presence (if enabled by BIOS)

set command

Use this command to change some IMM settings.

- Some IMM settings can be changed with a simple **set** command.
- Some of these settings, such as environment variables, are used by the CLI.

The following table shows the arguments for the options.

Table 43. set command

The following table is a single-row three column table consisting of the command description and associated information.

Option	Description	Values
value	Set value for specified path or setting	Appropriate value for specified path or setting.

Syntax:
```
set [options]
option:
  value
```

smtp command

Use this command to display and configure settings for the SMTP interface.

Running the **smtp** command with no options displays all SMTP interface information. The following table shows the arguments for the options.

Table 44. smtp command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 44. smtp command (continued)

Option	Description	Values
-auth	SMTP authentication support	enabled, disabled
-authepw	SMTP authentication encrypted password	Valid password string
-authmd	SMTP authentication method	CRAM-MD5, LOGIN
-authn	SMTP authentication user name	String (limited to 256 characters)
-authpw	SMTP authentication password	String (limited to 256 characters)
-pn	SMTP port number	Valid port number
-s	SMTP server IP address or host name	Valid IP address or host name (63 character limit)

Syntax:
```
smtp [options]
option:
  -auth enabled|disabled
  -authepw password
  -authmd CRAM-MD5|LOGIN
  -authn username
  -authpw password
  -s ip_address_or_hostname
  -pn port_number
```

Example:
```
system> smtp
-s test.com
-pn 25
system>
```

snmp command

Use this command to display and configure SNMP interface information.

Running the **snmp** command with no options displays all SNMP interface information. The following table shows the arguments for the options.

Table 45. snmp command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-a3	SNMPv3 agent	on, off **Notes:** To enable the SNMPv3 agent, the following criteria must be met: • IMM contact specified using the -cn command option. • IMM location specified using the -l command option.
-t1	SNMPv1 traps	on, off
-t	SNMPv3 traps	on, off

Table 45. snmp command (continued)

Option	Description	Values
-l	IMM location	String (limited to 47 characters). **Notes:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear the IMM location by specifying no argument or by specifying an empty string as the argument, such as "".
-cn	IMM contact name	String (limited to 47 characters). **Notes:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear the IMM contact name by specifying no argument or by specifying an empty string as the argument, such as "".
-c	SNMP community name	String (limited to 15 characters). **Notes:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear an SNMP community name by specifying no argument or by specifying an empty string as the argument, such as "".
-ci	SNMP community IP address/host name	Valid IP address or hostname (limited to 63 characters). **Notes:** • An IP address or host name can only contain dots, underscores, minus signs, letters and digits. No embedded spaces or consecutive periods are allowed. • Clear an SNMP community IP address or host name by specifying no argument.

Syntax:

```
snmp [options]
option:
 -a3 state
  -t state
  -l location
  -cn contact_name
  -t1 state
  -c community name
  -ci community IP address/hostname
```

Example:

```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
system>
```

snmpalerts command

Use this command to manage alerts sent via the SNMP.

Running **snmpalerts** with no options displays all SNMP alert settings. The following table shows the arguments for the options.

Table 46. snmpalerts command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-status	SNMP alert status	on, off
-crt	Sets critical events that send alerts	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Custom critical alert settings are specified using a pipe separated list of values of the form **snmpalerts -crt custom:te|vo**, where custom values are: • te: critical temperature threshold exceeded • vo: critical voltage threshold exceeded • po: critical power failure • di: hard disk drive failure • fa: fan failure • cp: microprocessor failure • me: memory failure • in: hardware incompatibility • re: power redundancy failure • ot: all other critical events
-crten	Send critical event alerts	enabled, disabled
-wrn	Sets warning events that send alerts	all, none, custom:rp|te|vo|po|fa|cp|me|ot Custom warning alert settings are specified using a pipe separated list of values of the form **snmpalerts -wrn custom:rp|te**, where custom values are: • rp: power redundancy warning • te: warning temperature threshold exceeded • vo: warning voltage threshold exceeded • po: warning power threshold exceeded • fa: non-critical fan event • cp: microprocessor in degraded state • me: memory warning • ot: all other warning events
-wrnen	Send warning event alerts	enabled, disabled

Table 46. snmpalerts command (continued)

Option	Description	Values
-sys	Sets routine events that send alerts	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Custom routine alert settings are specified using a pipe separated list of values of the form **snmpalerts -sys custom:lo|tio**, where custom values are: • lo: successful remote login • tio: operating system timeout • ot: all other informational and system events • po: system power on/off • bf: operating system boot failure • til: operating system loader watchdog timeout • pf: predicted failure (PFA) • el: event log 75% full • ne: network change
-sysen	Send routine event alerts	enabled, disabled

Syntax:

```
snmpalerts [options]
   options:
     -status status
     -crt event_type
     -crten state
     -wrn event_type
     -wrnen state
     -sys event_type
     -sysen state
```

srcfg command

Use this command to indicate the key sequence to enter the CLI from the serial redirection mode.

To change the serial redirect configuration, type the options, followed by the values. To change the serial redirect configuration, you must have at least Adapter Networking and Security Configuration authority.

Note: The IMM hardware does not provide for a serial port to serial port pass-through capability. Therefore the `-passthru` and `entercliseq` options which are present in the Remote Supervisor Adapter II CLI are not supported.

Running the **srcfg** command with no options displays the current serial redirection keystroke sequence. The following table shows the arguments for the `srcfg -entercliseq` command option.

Table 47. srcfg command

The following table is a single-row three column table consisting of the option, option description, and value information for the option.

Table 47. srcfg command (continued)

Option	Description	Values
-entercliseq	Enter a CLI keystroke sequence	User-defined keystroke sequence to enter the CLI. **Note:** This sequence must have at least one character and at most 15 characters. The caret symbol (^) has a special meaning in this sequence. It denotes Ctrl for keystrokes that map to Ctrl sequences (for example, ^[for the escape key and ^M for carriage return). All occurrences of ^ are interpreted as part of a Ctrl sequence. Refer to an ASCII-to-key conversion table for a complete list of Ctrl sequences. The default value for this field is ^[(which is Esc followed by (.

Syntax:
```
srcfg [options]
options:
-entercliseq entercli_keyseq
```

Example:
```
system> srcfg
-entercliseq ^[Q
system>
```

sshcfg command

Use this command to display and configure SSH parameters.

Running the **sshcfg** command with no options displays all SSH parameters. The following table shows the arguments for the options.

Table 48. sshcfg command

This following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-cstatus	State of SSH CLI	enabled, disabled
-hk gen	Generate SSH server private key	
-hk rsa	Display server RSA public key	

Syntax:
```
sshcfg [options]
option:
  -cstatus state
  -hk gen
  -hk rsa
```

Example:
```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

ssl command

Use this command to display and configure the SSL parameters.

To enable an SSL client, a client certificate must be installed. Running the **ssl** command with no options displays SSL parameters. The following table shows the arguments for the options.

Table 49. ssl command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-ce	Enables or disables an SSL client	on, off
-se	Enables or disables an SSL server	on, off
-cime	Enables or disables CIM over HTTPS on the SSL server	on, off

Syntax:

```
portcfg [options]
 options:
  -ce state
  -se state
  -cime state
```

Parameters: The following parameters are presented in the option status display for the **ssl** command and are output only from the CLI:

Server secure transport enable
This status display is read-only and cannot be set directly.

Server Web/CMD key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL server CSR key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client LDAP key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client CSR key status

This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

sslcfg command

Use this command to display and configure the SSL for the IMM and manage certificates.

Running the **sslcfg** command with no options displays all SSL configuration information. The **sslcfg** command is used to generate a new encryption key and self-signed certificate or certificate signing request (CSR). The following table shows the arguments for the options.

Table 50. sslcfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-server	SSL server status	enabled, disabled **Note:** The SSL server can be enabled only if a valid certificate is in place.
-client	SSL client status	enabled, disabled **Note:** The SSL client can be enabled only if a valid server or client certificate is in place.
-cim	CIM over HTTPS status	enabled, disabled **Note:** CIM over HTTPS can be enabled only if a valid server or client certificate is in place.
-cert	Generate self-signed certificate	server, client, sysdir, storekey **Notes:** • Values for the **-c**, **-sp**, **-cl**, **-on**, and **-hn** command options are required when generating a self-signed certificate. • Values for the **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, and **-dq** command options are optional when generating a self-signed certificate.
-csr	Generate a CSR	server, client, sysdir, storekey **Notes:** • Values for the **-c**, **-sp**, **-cl**, **-on**, and **-hn** command options are required when generating a CSR. • Values for the **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd**, and **-un** command options are optional when generating a CSR.

Table 50. sslcfg command (continued)

Option	Description	Values
-i	IP address for TFTP/SFTP server	Valid IP address **Note:** An IP address for the TFTP or SFTP server must be specified when uploading a certificate, or downloading a certificate or CSR.
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22)
-u	User name for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password
-l	Certificate filename	Valid filename **Note:** A filename is required when downloading or uploading a certificate or CSR. If no filename is specified for a download, the default name for the file is used and displayed.
-dnld	Download certificate file	This option takes no arguments; but, must also specify values for the **-cert** or **-csr** command option (depending on the certificate type being downloaded). This option takes no arguments; but, must also specify values for the **-i** command option, and **-l** (optional) command option.
-upld	Imports certificate file	This option takes no arguments, but must also specify values for the **-cert**, **-i**, and **-l** command options.
-tc*x*	Trusted certificate *x* for SSL client	import, download, remove **Note:** The trusted certificate number, *x*, is specified as an integer from 1 to 3 in the command option.
-c	Country	Country code (2 letters) **Note:** Required when generating a self-signed certificate or CSR.
-sp	State or province	Quote-delimited string (maximum 60 characters) **Note:** Required when generating a self-signed certificate or CSR.
-cl	City or locality	Quote-delimited string (maximum 50 characters) **Note:** Required when generating a self-signed certificate or CSR.
-on	Organization name	Quote-delimited string (maximum 60 characters) **Note:** Required when generating a self-signed certificate or CSR.
-hn	IMM host name	String (maximum 60 characters) **Note:** Required when generating a self-signed certificate or CSR.
-cp	Contact person	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-ea	Contact person email address	Valid email address (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-ou	Organizational unit	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-s	Surname	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-gn	Given name	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-in	Initials	Quote-delimited string (maximum 20 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-dq	Domain name qualifier	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.

Table 50. sslcfg command (continued)

Option	Description	Values
-cpwd	Challenge password	String (minimum 6 characters, maximum 30 characters) **Note:** Optional when generating a CSR.
-un	Unstructured name	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a CSR.

Syntax:

```
sslcfg [options]
option:
  -server state
  -client state
  -cim state
  -cert certificate_type
  -csr certificate_type
  -i ip_address
port number
username
  -pw password
  -l filename
  -dnld
  -upld
  -tc xaction
  -c country_code
  -sp state_or_province
  -cl city_or_locality
  -on organization_name
  -hn bmc_hostname
  -cp contact_person
  -ea email_address
  -ou organizational_unit
  -s surname
  -gn given_name
  -in initials
  -dq dn_qualifier
  -cpwd challenge_password
  -un unstructured_name
```

Examples:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

Client certificate examples:

- To generate a CSR for a storage key, enter the following command:
```
system> sslcfg
-csr storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
-cp Contact -ea "" -ou""
ok
```

The above example is displayed on multiple lines due to space limitations.

- To download a certificate from the IMM to another server, enter the following command:
```
system> sslcfg
-csr storekey -dnld -i 192.168.70.230 -l storekey.csr
ok
```
- To upload the certificate processed by the Certificate Authority (CA), enter the following command:
```
system> sslcfg
-cert storekey -upld -i 192.168.70.230 -l tklm.der
```
- To generate a self-signed certificate, enter the following command:
```
system> sslcfg
-cert storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
-cp Contact -ea "" -ou "
ok
```

  The above example is displayed on multiple lines due to space limitations.

SKLM Server certificate example:

- To import the SKLM server certificate, enter the following command:
```
system> storekeycfg
-add -ip 192.168.70.200 -f tklm-server.der
ok
```

storekeycfg command

Use this command to configure the host name or IP address and network port for a SKLM server.

You can configure up to four SKLM server targets. The **storekeycfg** command is also used to install and remove the certificates that are used by the IMM for authentication to the SKLM server.

The following table shows the arguments for the options.

Table 51. storekeycfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-add	Add the activation key	Values are -ip, -pn, -u, -pw, and -f command options
-ip	Host name or IP address for the TFTP/SFTP server	Valid host name or IP address for TFTP/SFTP server
-pn	Port number of the TFTP or SFTP server	Valid port number for TFTP/SFTP server (default value is 69/22)
-u	User name for SFTP server	Valid user name for SFTP server
-pw	Password for SFTP server	Valid password for SFTP server
-f	File name for activation key	Valid file name for activation key file name

Table 51. storekeycfg command (continued)

Option	Description	Values
-del	Use this command to delete the activation key by index number	Valid activation key index number from keycfg listing
-dgrp	Add the device group	Device group name
-sxip	Add the host name or IP address for the SKLM server	Valid host name or IP address for SKLM server. Numeric value of 1, 2, 3, or 4.
-sxpn	Add the port number of the SKLM server	Valid port number for SKLM server. Numeric value of 1, 2, 3, or 4.
-testx	Test the configuration and connection to the SKLM server	Numeric value of 1, 2, 3, or 4
-h	Display the command usage and options	

Syntax:

```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

Examples:

To import the SKLM server certificate, enter the following command:

```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

To configure the SKLM server address and port number, enter the following command:

```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

To set the device group name, enter the following command:

```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

syncrep command

Use this command to launch firmware sync from remote repository.

The following table shows the arguments for the options.

Table 52. syncrep command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-t	Protocol to connect repository	samba, nfs
-l	Location of remote repository	In URL format
-u	User	
-p	Password	
-o	Option	Extra option string for samba and nfs mounts
-d	Domain	Domain for samba mount
-q	Query current update status	
-c	Cancel the sync process	

Syntax

```
syncrep [options]  Launch firmware sync from remote repository
options:
     -t <samba|nfs> protocol to connect repository
     -l location of remote repository (URL format)
     -u User
     -p Password
     -o option (extra option string for samba and nfs mounts)
     -d domain (domain for samba mount)
     -q query current update status
     -c cancel the sync process
```

Example

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

thermal command

Use this command to display and configure the thermal mode policy of the host system.

Running the **thermal** command with no options displays the thermal mode policy. The following table shows the arguments for the options.

Table 53. thermal command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-mode	Thermal mode selection	normal, performance, minimal, efficiency, custom
-table	Vendor, device identification (ID) and alternate thermal table	

Syntax:
```
thermal [options]
option:
  -mode thermal_mode
  -table vendorID_devicetable_number
```

Example:
```
system> thermal
-mode normal
-table 80860126 1 1ODE0DFA 3
system>
```

timeouts command

Use this command to display or change the timeout values.

- To display the timeouts, type `timeouts`.
- To change timeout values, type the options followed by the values.
- To change timeout values, you must have at least Adapter Configuration authority.

The following table shows the arguments for the timeout values. These values match the graduated scale pull-down options for server timeouts on the web interface.

Table 54. timeouts command

The following table is a multi-row four column table consisting of the options, option descriptions, and associated values for the options.

Option	Timeout	Units	Values
-f	Power off delay	minutes	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-l	Loader timeout	minutes	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-o	Operating system timeout	minutes	disabled, 2.5, 3, 3.5, 4

Syntax:
```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
```

Example:
```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

tls command

Use this command to set the minimum TLS level.

The following table shows the arguments for the options.

Table 55. tls command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-min	Select the minimum TLS level	1.0, 1.1, 1.2 [1]
-h	List the usage and options	
Notes: 1. When the cryptography mode is set to the NIST-800-131A Compliance mode, the TLS version must be set to 1.2.		

Syntax:
```
tls [options]
option:
  -min 1.0|1.1|1.2
  -h
```

Examples:

To get the usage for the tls command, issue the following command:
```
system> tls
-h
system>
```

To obtain the current tls version, issue the following command:
```
system> tls
-min 1.0
system>
```

To change the current tls version to 1.2, issue the following command:
```
system> tls
-min 1.2
ok
system>
```

trespass command

Use this command to configure and display the trespass messages.

The **trespass** command can be used to configure and display the trespass messages. The trespass messages will be displayed to any user logging in through the WEB or CLI interface.

The following table shows the arguments for the options.

Table 56. uefipw command

The following table is a multi-row two column table consisting of the options and option descriptions.

Option	Description
-s	Configure trespass messages
-h	Lists usage and options

Syntax:

```
usage:
   trespass display the trespass message
   -s <trespass message> configure trespass message
   -h - Lists usage and options
```

uefipw command

Use this command to configure UEFI admin passwords. The password is write-only.

The **uefipw** command can be used with the “-p” option to configure the UEFI admin password for XCC or with the “-ep” option for LXCA to configure the UEFI admin password by CLI interface. The password is write-only.

The following table shows the arguments for the options.

Table 57. uefipw command

The following table is a multi-row two column table consisting of the options and option descriptions.

Option	Description
-cp	Current password (limited to 20 characters)
-p	New password (limited to 20 characters)
-cep	Current password encrypted
-ep	New password encrypted

Syntax:

```
usage:
   uefipw [-options] - Configure the UEFI admin password
options:
   -cp      - current password (limited to 20 characters)
   -p       - new password (limited to 20 characters)
   -cep     - current password encrypted
   -ep      - new password encrypted
```

usbeth command

Use this command to enable or disable the in-band LAN over USB interface.

Syntax:

```
usbeth [options]
options:
-en <enabled|disabled>
```

Example:

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

usbfp command

Use this command to control the BMC use of the front panel USB port

The following table shows the arguments for the options.

Table 58. usbfp command

The following table is a multi-row two column table consisting of the options and option descriptions.

Option	Description
-mode <bmc | server | shared>	Set usage mode to BMC, server, or shared
-it <minutes>	Inactivity timeout in minutes (shared mode
-btn <on | off>	Enable using id button to toggle owner (shared mode)
-own <bmc | server >	Set owner to bmc or server (shared mode)

users command

Use this command to access all user accounts and their authority levels.

The **users** command is also used to create new user accounts and modify existing accounts. Running the **users** command with no options displays a list of users and some basic user information. The following table shows the arguments for the options.

Table 59. users command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-user_index	User account index number	1 through 12, inclusive, or `all` for all users.
-n	User account name	Unique string containing only numbers, letters, periods, and underscores. Minimum of 4 characters and maximum of 16 characters.
-p	User account password	String that contains at least one alphabetic and one non-alphabetic character. Minimum of 6 characters and maximum of 20 characters. Null creates an account without a password that the user must set during their first login.
-r	Role name	As listed in “roles command” on page 131 command
-ep	Encryption password (for backup/restore)	Valid password
-clear	Erase specified user account If you are authorized, you can remove your own account or the account of other users, even if they are currently logged in, unless it is the only account remaining with User Account Management privileges. Sessions that are already in progress when user accounts are deleted will not be automatically terminated.	User account index number to erase must be specified, following the form: `users -clear -`*user_index*

Table 59. users command (continued)

Option	Description	Values
-curr	Display users currently logged in	
-sauth	SNMPv3 authentication protocol	HMAC-MD5, HMAC-SHA, none
-spriv	SNMPv3 privacy protocol	CBC-DES, AES, none
-spw	SNMPv3 privacy password	Valid password
-sepw	SNMPv3 privacy password (encrypted)	Valid password
-sacc	SNMPv3 access type	get, set
-strap	SNMPv3 trap host name	Valid host name
-pk	Display SSH public key for user	User account index number. **Notes:** • Each SSH key assigned to the user is displayed, along with an identifying key index number. • When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk`. • All keys are in OpenSSH format.
-e	Display entire SSH key in OpenSSH format *(SSH public key option)*	This option takes no arguments and must be used exclusive of all other `users -pk` options. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -e`.
-remove	Remove SSH public key from user *(SSH public key option)*	Public key index number to remove must be given as a specific *-key_index* or `-all` for all keys assigned to the user. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -remove -1`.
-add	Add SSH public key for user *(SSH public key option)*	Quote-delimited key in OpenSSH format **Notes:** • The `-add` option is used exclusive of all other `users -pk` command options. • When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/ aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/ qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="`

Table 59. users command (continued)

Option	Description	Values
-upld	Upload an SSH public key *(SSH public key option)*	Requires the `-i` and `-l` options to specify key location. **Notes:** • The `-upld` option is used exclusive of all other `users -pk` command options (except for `-i` and `-l`). • To replace a key with a new key, you must specify a *-key_index*. To add a key to the end of the list of current keys, do not specify a key index. • When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`.
-dnld	Download the specified SSH public key *(SSH public key option)*	Requires a *-key_index* to specify the key to download and the `-i` and `-l` options to specify the download location on another computer running a TFTP server. **Notes:** • The `-dnld` option is used exclusive of all other `users -pk` command options (except for `-i`, `-l`, and *-key_index*). • When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.
-i	IP address of TFTP/SFTP server for uploading or downloading a key file *(SSH public key option)*	Valid IP address **Note:** The `-i` option is required by the `users -pk -upld` and `users -pk -dnld` command options.
-pn	Port number of TFTP/SFTP server *(SSH public key option)*	Valid port number (default 69/22) **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-u	User name for SFTP server *(SSH public key option)*	Valid user name **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-pw	Password for SFTP server *(SSH public key option)*	Valid password **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-l	File name for uploading or downloading a key file via TFTP or SFTP *(SSH public key option)*	Valid file name **Note:** The `-l` option is required by the `users -pk -upld` and `users -pk -dnld` command options.
-af	Accept connections from host *(SSH public key option)*	A comma-separated list of hostnames and IP addresses, limited to 511 characters. Valid characters include: alphanumeric, comma, asterisk, question mark, exclamation point, period, hyphen, colon and percent sign.
-cm	Comment *(SSH public key option)*	Quote-delimited string of up to 255 characters. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -cm "This is my comment."`.

Syntax:

```
users [-options] - display/configure user accounts
options:
   -[1-12]  - user account number
```

```
  -l       - display password expiration days
  -n       - username (limited to 16 characters)
  -p       - password (limited to 32 characters)
  -shp     - set hashpassword (total 64 characters)
  -ssalt   - set salt (limited to 64 characters)
  -ghp     - get hashpassword
  -gsalt   - get salt
  -ep      - encrypted password (used with backup/restore )
  -r       - role name as listed in roles command
  -clear   - clear user account
  -curr    - display current users
  -sauth   (none|HMAC-SHA)           - snmpv3 authentication protocol
  -spriv   (none|CBC-DES|AES)        - snmpv3 privacy protocol
  -spw     password                    - snmpv3 privacy password
  -sepw    encryptedpassword          - snmpv3 privacy password (encrypted)
  -sacc    (Get)                  - snmpv3 Access type
  -strap   hostname                    - snmpv3 trap hostname

  -pk      - SSH public keys options:
      -e       - Displays the entire key in OpenSSH format
      -remove  - Removes the specified key for the specified user
      -add     - Adds a public key for the specified user
      -upld    - Used to upload a public key in OpenSSH/RFC4716 format
      -dnld    - Used to download the specified public key to a TFTP/SFTP server
      -i       - IP address of the TFTP/SFTP
      -pn      - port number of tftp/sftp server (default 69/22)
      -u       - username for sftp server
      -pw      - password for sftp server
      -l       - Filename of the key file when uploading or downloading via TFTP/SFTP
      -af      - accept connections from host, in the format: from="<list>", where
                 <list> is a comma-separated list of hostnames and IP addresses
                 (limited to 511 characters)
      -cm      - comment (limited to 255 characters, must be quote-delimited)
```

Example:

```
system> users
 Account      Login ID      Advanced Attribute              Role             Password Expires
 -------      --------       ------------------             ------             ----------------
    1           USERID                  Native                 Administrator                    89 day(s)
system> users -2 -n sptest -p PasswOrd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account      Login ID      Advanced Attribute            Role               Password Expires
 -------      --------       ------------------           ------              ----------------
    1           USERID                  Native           Administrator                   90 day(s)
2           sptest                  Native                 Administrator            Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -r  Administr
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
```

IMM control commands

This topic provides an alphabetic list of IMM control CLI commands.

There are currently 7 IMM control commands:

alertentries command

Use this command to manage alert recipients.

- **alertentries** with no options display all alert entry settings.
- **alertentries -number -test** generates a test alert to the given recipient index number.
- **alertentries -number** (where number is 0 - 12) display alert entry settings for the specified recipient index number or allow you to modify the alert settings for that recipient.

The following table shows the arguments for the options.

Table 60. alertentries command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-number	Alert recipient index number to display, add, modify, or delete	1 through 12
-status	Alert recipient status	on, off
-type	Alert type	email, syslog
-log	Include event log in alert email	on, off
-n	Alert recipient name	String
-e	Alert recipient email address	Valid email address
-ip	Syslog IP address or host name	Valid IP address or host name
-pn	Syslog port number	Valid port number
-del	Delete specified recipient index number	
-test	Generate a test alert to specified recipient index number	
-crt	Sets critical events that send alerts	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Custom critical alert settings are specified using a pipe separated list of values of the form **alertentries -crt custom:te|vo**, where custom values are: • te: critical temperature threshold exceeded • vo: critical voltage threshold exceeded • po: critical power failure • di: hard disk drive failure • fa: fan failure • cp: microprocessor failure • me: memory failure • in: hardware incompatibility • re: power redundancy failure • ot: all other critical events

Table 60. alertentries command (continued)

Option	Description	Values
-crten	Send critical event alerts	enabled, disabled
-wrn	Sets warning events that send alerts	all, none, custom:rp|te|vo|po|fa|cp|me|ot Custom warning alert settings are specified using a pipe separated list of values of the form **alertentries -wrn custom:rp|te**, where custom values are: • rp: power redundancy warning • te: warning temperature threshold exceeded • vo: warning voltage threshold exceeded • po: warning power threshold exceeded • fa: non-critical fan event • cp: microprocessor in degraded state • me: memory warning • ot: all other warning events
-wrnen	Send warning event alerts	enabled, disabled
-sys	Sets routine events that send alerts	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Custom routine alert settings are specified using a pipe separated list of values of the form **alertentries -sys custom:lo|tio**, where custom values are: • lo: successful remote login • tio: operating system timeout • ot: all other informational and system events • po: system power on/off • bf: operating system boot failure • til: operating system loader watchdog timeout • pf: predicted failure (PFA) • el: event log 75% full • ne: network change
-sysen	Send routine event alerts	enabled, disabled

Syntax:

```
alertentries [options]
   options:
   -number recipient_number
      -status status
      -type alert_type
      -log include_log_state
      -n recipient_name
      -e email_address
      -ip ip_addr_or_hostname
      -pn port_number
      -del
      -test
      -crt event_type
      -crten state
      -wrn event_type
      -wrnen state
      -sys event_type
```

```
-sysen state
```

Example:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

batch command

Use this command to execute one or more CLI commands that are contained in a file.

- Comment lines in the batch file begin with a #.
- When running a batch file, commands that fail are returned along with a failure return code.
- Batch file commands that contain unrecognized command options might generate warnings.

The following table shows the arguments for the options.

Table 61. batch command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-f	Batch file name	Valid file name
-ip	IP address of TFTP/SFTP server	Valid IP address
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22)
-u	Username for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password

Syntax:

```
batch [options]
option:
  -f filename
  -ip ip_address
  -pn port_number
```

username
-pw *password*

Example:
```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

clearcfg command

Use this command to set the IMM configuration to its factory defaults.

You must have at least Advanced Adapter Configuration authority to issue this command. After the configuration of the IMM is cleared, the IMM is restarted.

clock command

Use this command to display the current date and time. You can set the UTC offset and daylight saving time settings

The BMC obtains the time from the host server or NTP server.

The time obtained from the host may be local time or UTC time. The host option should be set to UTC if NTP is not used and the host uses UTC format. UTC offset can be in the format of +0200, +2:00, +2, or 2, for positive offsets, and -0500, -5:00 or -5, for negative offsets. UTC offset and daylight savings times are used with NTP or when the host mode is UTC.

For a UTC offset of +2, -7, -6, -5, -4 and -3 special daylight saving time settings are required.

- For +2, the daylight saving time options are as follows: off, ee (Eastern Europe), tky (Turkey), bei (Beirut), amm (Amman), jem (Jerusalem).
- For -7, the daylight saving time settings are as follows: off, mtn (Mountain), maz (Mazatlan).
- For -6, the daylight saving time settings are as follows: off, mex (Mexico), cna (Central North America).
- For -5, the daylight saving time settings are as follows: off, cub (Cuba), ena (Eastern North America).
- For -4, the daylight saving time settings are as follows: off, asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantic).
- For -3, the daylight saving time settings are as follows: off, gtb (Godthab), bre (Brazil - East).

Syntax:
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

Example:
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

identify command

Use this command to turn the chassis identification LED on or off, or to have it flash.

The **-d** option can be used with the **-s on** option to turn the LED on for only the number of seconds specified with the **-d** option. The LED turns off after the number of seconds elapses.

Syntax:
```
identify [options]
options:
-s on/off/blink
-d seconds
```

Example:
```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

info command

Use this command to display and configure information about the IMM.

Running the **info** command with no options displays all IMM location and contact information. The following table shows the arguments for the options.

Table 62. info command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-name	IMM name	String
-contact	Name of IMM contact person	String
-location	IMM location	String
-room[1]	IMM room identifier	String
-rack[1]	IMM rack identifier	String
-rup[1]	Position of IMM in rack	String
-ruh	Rack unit height	Read only
-bbay	Blade bay location	Read only

1. Value is read only and cannot be reset if the IMM resides in a Flex System.

Syntax:
```
info [options]
option:
  -name xcc_name
  -contact contact_name
  -location xcc_location
  -room room_id
  -rack rack_id
  -rup rack_unit_position
  -ruh rack_unit_height
  -bbay blade_bay
```

spreset command

Use this command to restart the IMM.

You must have at least Advanced Adapter Configuration authority to issue this command.

Service advisor commands

This topic provides an alphabetic list of service advisor CLI commands.

There are currently 3 service advisor commands:

chconfig command

Use this command to display and configure the Service Advisor settings.

- The Service Advisor Terms and Conditions must be accepted, using the **chconfig -li** command option, before configuring any other parameters.
- All contact information fields, as well as the **Service Support Center** field (using chconfig -sc command option), are required before the Support of Service Advisor can be enabled.
- All HTTP Proxy fields must be set, if an HTTP proxy is required.

The following table shows the arguments for the options.

Table 63. chconfig command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-li	View or accept the Service Advisor Terms and Conditions **Note:** Terms and Conditions must be accepted before configuring any other parameters.	view, accept
-sa	Support status of the Service Advisor **Notes:** To enable Service Advisor, the following criteria must be met: • The country code is required. • All options in the Service Advisor Contact Information are required.	enabled, disabled
-sc	Country code for the Service Support Center	Two-character ISO country code
Service Advisor contact information options:		
-cn	Name of primary contact person	Quote-delimited string (30 characters maximum)
-cph	Phone number of primary contact person	Quote-delimited string (5 - 30 characters)
-ce	Email address of primary contact person **Note:** Alphanumeric characters '.', '-' or '_' are acceptable as userid or hostname. Email address must contain at least two domain items and the last domain item should be 2–4 alphabetic characters.	Valid email address of the form `userid@hostname` (30 characters maximum)

Table 63. chconfig command (continued)

Option	Description	Values
-co	Organization or company name of primary contact person	Quote-delimited string (30 characters maximum)
-ca	Address of the machine location	Quote-delimited string (30 characters maximum)
-cci	City of the machine location	Quote-delimited string (30 characters maximum)
-cs	State of the machine location	Quote-delimited string (30 characters maximum)
-cz	Postal code of the machine location	Quote-delimited string (9 characters maximum)
Alternate Service Advisor contact information options:		
-an	Name of alternate contact person	Quote-delimited string (30 characters maximum)
-aph	Phone number of alternate contact person	Quote-delimited string (5 - 30 characters)
-ae	Email address of alternate contact person **Note:** Alphanumeric characters '.', '-' or '_' are acceptable as userid or hostname. Email address must contain at least two domain items and the last domain item should be 2–4 alphabetic characters.	Valid email address of the form `userid@hostname` (30 characters maximum)
-ao	Organization or company name of alternate contact person	Quote-delimited string (30 characters maximum)
-aa	Address of the alternate machine location	Quote-delimited string (30 characters maximum)
-aci	City of the alternate machine location	Quote-delimited string (30 characters maximum)
-as	State of the alternate machine location	Quote-delimited string (30 characters maximum)
-az	Postal code of the alternate machine location	Quote-delimited string (9 characters maximum)
HTTP proxy settings options:		
-loc	HTTP proxy location	Fully qualified host name or IP address for HTTP proxy (63 characters maximum)
-po	HTTP proxy port	Valid port number (1 - 65535)
-ps	HTTP proxy status	enabled, disabled
-pw	HTTP proxy password	Valid password, quote-delimited (15 characters maximum)
-epw	HTTP proxy encrypted password	Valid password, quote-delimited (15 characters maximum)
-u	HTTP proxy user name	Valid user name, quote-delimited (30 characters maximum)
-test	Test http proxy	

Syntax:

```
chconfig [options]
option:
  -li view|accept
  -sa enable|disable
  -sc service_country_code
```

-ce *contact_email*
-cn *contact_name*
-co *company_name*
-cph *contact_phone*
-cpx *contact_extension_phone*
-an *alternate_contact_name*
-ae *alternate_contact_email*
-aph *alternate_contact_phone*
-apx *alternate_contact_extension_phone*
-mp *machine_phone_number*
-loc *hostname/ip_address*
-po *proxy_port*
-ps *proxy_status*
-pw *proxy_pw*
-ccl *machine_country_code*
-u *proxy_user_name*

chmanual command

Use this command to generate a manual call home request.

Note: Call home message recipients are configured using the **chconfig** command.

- The **chmanual -test** command generates a call home test message.

The following table shows the arguments for the options.

Table 64. chmanual command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options..

Option	Description	Values
-test	Generates a test message to call home recipients	

Syntax:

```
chmanual [options]
Generates a manual Call Home or a Test Call Home
  -test: Generate a test Call Home.
```

chlog command

Use this command to display the last five call home events and cancel the case associated with the event by caseNumber..

The **chlog** command displays the last five entries from the call-home activity log that were generated by the server or the user. The most recent call home entry is shown first. The server will not send duplicate events if they are not acknowledged as corrected in the activity log.

The following table shows the arguments for the options.

Table 65. chconfig command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options..

Table 65. chconfig command (continued)

Option	Description	Values
-c	cancel the case associated with the event by caseNumber	

Syntax:

```
chlog[-options]
      Displays the last five call home events that were generated either by
      the system or the user (most recent call home entry first.)

      -c: cancel the case associated with the event by caseNumber
```

Agent-less commands

This topic provides an alphabetic list of Agent-less commands.

There are currently 3 Agent-less commands:

storage command

Use this command to display and configure (if supported by the platform) information about the server's storage devices that are managed by the IMM.

The following table shows the arguments for the options.

Table 66. storage command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-list	List the storage targets managed by the IMM.	*controllers*|*pools*|*volumes*|*drives* Where *target* is: • *controllers*: list the supported RAID controllers[1] • *pools*: list the storage pools associated with the RAID controller[1] • *volumes*: list the storage volumes associated with the RAID controller[1] • *drives*: list the storage drives associated with the RAID controller[1]
-list -target *target_id*	List the storage *targets* managed by the IMM according to the *target_id*.	*pools*|*volumes*|*drives ctrl[x]*|*pool[x]* Where *target* and *target_id* are: • *pools ctrl[x]*: list the storage pools associated with the RAID controller, based on the target_id[1] • *volumes ctrl[x]*|*pool[x]*: list the storage volumes associated with the RAID controller, based on the target_id[1] • *drives ctrl[x]*|*pool[x]*: list the storage drives associated with the RAID controller, based on the target_id[1]

Table 66. storage command (continued)

Option	Description	Values
-list flashdimms	List the Flash DIMMs managed by the IMM.	
-list devices	Display the status of all disks and Flash DIMMS managed by the IMM.	
-show *target_id*	Display information for the selected target that is managed by the IMM.	Where *target_id* is: *ctrl[x]|vol[x]|disk[x]|pool[x]* *|flashdimm[x]* [3]
-show *target_id* info	Display detailed information for the selected target that is managed by the IMM.	Where *target_id* is: *ctrl[x]|vol[x]|disk[x]|pool[x]* *|flashdimm[x]* [3]
-show *target_id firmware*[3]	Display the firmware information for the selected target that is managed by the IMM.	Where *target_id* is: *ctrl[x]|disk[x]|flashdimm[x]*[2]
-showlog *target_id<m:n|all>*[3]	Display the event logs of the selected target that is managed by the IMM.	Where *target_id* is: *ctrl[x]*[4] *m:n|all* Where *m:n* is one to the maximum number of event logs Where *all* are all of the event logs
-config ctrl -scanforgn -target *target_id*[3]	Detect the foreign RAID configuration.	Where *target_id* is: *ctrl[x]*[5]
-config ctrl -imptforgn -target *target_id*[3]	Import the foreign RAID configuration.	Where *target_id* is: *ctrl[x]*[5]
-config ctrl -clrforgn -target *target_id*[3]	Clear the foreign RAID configuration.	Where *target_id* is: *ctrl[x]*[5]
-config ctrl -clrcfg -target *target_id*[3]	Clear the RAID configuration.	Where *target_id* is: *ctrl[x]*[5]
-config drv -mkoffline -target *target_id*[3]	Change the drive state from online to offline.	Where *target_id* is: *disk[x]*[5]
-config drv -mkonline -target *target_id*[3]	Change the drive state from offline to online.	Where *target_id* is: *disk[x]*[5]
-config drv -mkmissing -target *target_id*[3]	Mark the offline drive as an unconfigured good drive.	Where *target_id* is: *disk[x]*[5]
-config drv -prprm -target *target_id*[3]	Prepare an unconfigured good drive for removal.	Where *target_id* is: *disk[x]*[5]
-config drv -undoprprm -target *target_id*[3]	Cancel the prepare an unconfigured good drive for removal operation.	Where *target_id* is: *disk[x]*[5]
-config drv -mkbad -target *target_id*[3]	Change the unconfigured good drive to a unconfigured bad drive.	Where *target_id* is: *disk[x]*[5]

Table 66. storage command (continued)

Option	Description	Values
-config drv -mkgood -target *target_id*[3]	Change an unconfigured bad drive to a unconfigured good drive. or Convert the just a bunch of disks (JBOD) drive to an unconfigured good drive.	Where *target_id* is: *disk[x]*[5]
-config drv -addhsp *-[dedicated pools]* -target *target_id*[3]	Assign the selected drive as a hot spare to one controller or to existing storage pools.	Where *target_id* is: *disk[x]*[5]
-config drv -rmhsp -target *target_id*[3]	Remove the hot spare.	Where *target_id* is: *disk[x]*[5]
-config vol -remove -target *target_id*[3]	Remove one volume.	Where *target_id* is: *vol[x]*[5]
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target *target_id*[3]	Modify the properties of one volume.	• [-N *volume_name*] is the name of the volume • [-w <*0*|*1*|*2*>] is the cache write policy: – Type *0* for the Write Through policy – Type *1* for the Write Back policy – Type *2* for the Write With Battery Backup Unit (BBU) policy • [-r <*0*|*1*|*2*>] is the cache read policy: – Type *0* for the No Read Ahead policy – Type *1* for the Read Ahead Policy – Type *2* for the Adaptive Read Ahead policy • [-i <*0*|*1*>] is the cache I/O policy: – Type *0* for the Direct I/O policy – Type *1* for the Cached I/O policy • [-a <*0*|*2*|*3*>] is the access policy: – Type *0* for the Read Write policy – Type *2* for the Read Only policy – Type *3* for the Blocked policy • [-d <*0*|*1*|*2*>] is the disk cache policy: – Type *0* if the policy is unchanged – Type *1* to enable policy[6] – Type *2* to disable policy • [-b <*0*|*1*>] is the background initialization: – Type *0* to enable initialization – Type *1* to disable initialization • *-target_id* is *vol[x]*[5]

Table 66. storage command (continued)

Option	Description	Values
-config vol -add<[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3],[7]	Create one volume for a new storage pool when the target is a controller. or Create one volume with an existing storage pool when the target is a storage pool.	• [-R <*0*|*1*|*5*|*1E*|*6*|*10*|*50*|*60*|*00*|*1ERLQ0*|*1E0RLQ0*>] This option defines the RAID level and is only used with a new storage pool • [-D disk *[id11]:disk[id12]:..disk[id21]:disk[id22]:..*] This option defines the drive group (including spans) and is only used with a new storage pool • [-H disk *[id1]:disk[id2]:..*]This option defines the hot spare group and is only used with a new storage pool • [-1 hole] This option defines the index number of the free hole space for an existing storage pool • [-N *volume_name*] is the name of the volume • [-w <*0*|*1*|*2*>] is the cache write policy: – Type *0* for the Write Through policy – Type *1* for the Write Back policy – Type *2* for the Write With Battery Backup Unit (BBU) policy • [-r <*0*|*1*|*2*>] is the cache read policy: – Type *0* for the No Read Ahead policy – Type *1* for the Read Ahead policy – Type *2* for the Adaptive Read Ahead policy
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target *target_id*[3]	Create one volume for a new storage pool when the target is a controller. or Create one volume with an existing storage pool when the target is a storage pool.	• [-i <*0*|*1*>] is the cache I/O policy: – Type *0* for the Direct I/O policy – Type *1* for the Cached I/O policy • [-a <*0*|*2*|*3*>] is the access policy: – Type *0* for the Read Write policy – Type *2* for the Read Only policy – Type *3* for the Blocked policy • [-d <*0*|*1*|*2*>] is the disk cache policy: – Type *0* if the policy remains unchanged – Type *1* to enable the policy[6] – Type *2* to disable the policy • [-f <*0/1/2*>] is the type of initialization: – Type *0* for no initialization – Type *1* for quick initialization – Type *2* for full initialization • [-S *volume_size*] is the size of the new volume in MB • [-P *strip_size*] is the volume strip size for example, 128K or 1M • -target *target_id* is: – *ctrl[x]* (new storage pool)[5] – *pool[x]* (existing storage pool)[5]

Table 66. storage command (continued)

Option	Description	Values
-config vol -getfreecap [-R] [-D disk] [-H disk] -target *target_id*[3]	Get the free capacity amount of the drive group.	• [-R <*0*|*1*|*5*|*1E*|*6*|*10*|*50*|*60*|*00*|*1ERLQ0*|*1E0RLQ0*>] This option defines the RAID level and is only used with a new storage pool • [-D disk *[id11]:[id12]:..[id21]:[id22]:..*] This option defines the drive group (including spans) and is only used with a new storage pool • [-H disk *[id1]:[id2]:..*]This option defines the hot spare group and is only used with a new storage pool • -target *target_id* is: – *ctrl[x]*[5]
-help	Display the command usage and options	

Notes:
1. This command is only supported on servers where the IMM can access the RAID controller.
2. Firmware information is displayed only for associated controllers, disks, and Flash DIMMs. Firmware information for associated pools and volumes are not displayed.
3. Information is displayed on multiple lines due to space limitations.
4. This command is only supported on servers that support RAID logs.
5. This command is only supported on servers that support RAID configurations.
6. The *Enable* value does not support RAID level 1 configurations.
7. A partial list of available options are listed here. The remaining options for the **storage -config vol -add** command are listed in the following row.

Syntax:
```
storage [options]
option:
  -config ctrl|drv|vol -option [-options] -target target_id
  -list controllers|pools|volumes|drives
  -list pools -target ctrl[x]
  -list volumes -target ctrl[x]|pool[x]
  -list drives -target ctrl[x]|pool[x]
  -list devices
  -list flashdimms
  -show target_id
  -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
  -show {ctrl[x]|disk[x]|flashdimm[x]}firmware
  -showlog ctrl[x]m:n|all
  -h help
```

Examples:
```
system> storage
-config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage
-config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -imptforgn -target ctrl[0]
ok
system>
```

```
system> storage
-config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage
-config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage
-config drv -addhsp -target disk[0-0]
ok
system>
system> storage
-config drv -mkbad -target disk[0-0]
ok
system>
system> storage
-config drv -mkgood -target disk[0-0]
ok
system>
system> storage
-config drv -mkmissing -target disk[0-0]
ok
system>
system> storage
-config drv -mkoffline -target disk[0-0]
ok
system>
system> storage
-config drv -mkonline -target disk[0-0]
ok
system>
system> storage
-config drv -prprm -target disk[0-0]
ok
system>
system> storage
-config drv -rmhsp -target disk[0-0]
ok
system>
system> storage
-config drv -undoprprm -target disk[0-0]
ok
system>
system> storage
-config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage
-config vol -add -R 1 -D disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage
-config vol -getfreecap -R 1 -D disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage
-config vol -remove -target vol[0-1]
ok
system>
```

```
system> storage
-config vol -set -N LD_volume -w 0 -target vol[0-0]
ok
system>
system> storage
-list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage
-list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage
-list volumes
system>storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage
-list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage
-list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
system> storage
-list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show ctrl[0] firmware
Total Firmware number: 2
```

```
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 1234567890
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUDOXTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
Storage Pool 0
Storage Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
```

```
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage
-show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
```

```
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

adapter command

This command is used to display PCIe adapter inventory information.

If the **adapter** command is not supported, the server responds with the following message when the command is issued:
`Your platform does not support this command.`
If you remove, replace, or configure any adapters, you must restart the server (at least once) to view the updated adapter information.

The following table shows the arguments for the options.

Table 67. adapter command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-list	List all PCIe adapters in the server	
-show *target_id*	Show the detailed information for the target PCIe adapter	*target_id [info|firmware|ports|chips]* Where: • *info*: display the hardware information for the adapter • *firmware*: display all firmware information for the adapter • *ports*: display all Ethernet port information for the adapter • *chips*: display all GPU chip information for the adapter
-h	Display the command usage and options	

Syntax:

```
adapter [options]
option:
  -list
  -show target_id [info|firmware|ports|chips]
  -h help
```

Examples:

```
system> adapter
list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
slot-2   Adapter 01:02:03
system> adapter
```

```
show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
```

```
Package Type: dici
```

mvstor command

Use this command to get M.2 related inventory information and manage the virtual volumes.

The following table shows the arguments for the options.

Table 68. mvstor command

The following table is a multi-row two column table consisting of the options and option descriptions.

Option	Description
-h/?	Print the help info for this command
-version	Display the controller firmware information
-disks	Display the media disks information
-volumes	Display the virtual volumes information
-create	Create a virtual volume, the VD_Name, RaidLevel and StripeSize can be specified
-delete	Delete a virtual volume
-import	Import a foreign virtual volume. After importing the virtual volume, a system reboot will rebuild the virtual volume automatically.

Usage

```
   mvstor [-options] - raid configuration for SATA/NVMe RAID boot solution.
options:
   -version                    - displays controller firmware version.
   -disks                      - displays information of media disks.
   -volumes                    - displays information of virtual disks
   -create -slot <slot_no> -name <vd name> -level <0|1> -stripe <32|64|128|256|512> - create virtual volume.
       Marvell SATA RAID: stripe size can only be 32k or 64k
       Marvell NVMe RAID: vd name is unapplicable. The name will always be VD_0.
   -delete -slot <slot_no> -id <0|1>          - delete the virtual volume
   -import -slot <slot_no> -id <0|1>          - import a foreign virtual volume
```

Example

```
system> mvstor -version
    Controller Slot      Device Name                                              Version
1                ThinkSystem M.2 SATA 2-Bay RAID Enablement Kit        2.3.20.1203


system> mvstor -disks
  Controller Slot 1    M.2 Bay0         128GB M.2 SATA SSD     LEN
  Controller Slot 1    M.2 Bay1         128GB M.2 SATA SSD     LEN

system> mvstor -volumes
Controller Slot 1:
    VD_ID:         0
    VD_Name:       VD_Test
    PD_Member:     0,1
    RaidLevel:     1
    StripSize:     64k
    VD_Capacity:   117 GB
    VD_Status:     Optimal
       1             64k          29 GB           Optimal
```

```
system> mvstor -delete –slot 1 -id 0
VD_ID 0 is deleted

system> mvstor -create –slot 1 -name M2RAID -level 1 -strip 64
New volume is created

system> mvstor -import –slot 1 -id 0
VD_ID 0 is imported
```

Support commands

This topic provides an alphabetic list of Support commands.

There is only one support command: the “dbgshimm command” on page 173.

dbgshimm command

Use this command to unlock network access to the secure debug shell.

Note: This command is intended only for support personnel use.

The following table shows the arguments for the options.

Table 69. dbgshimm command

The following table is a multi-row two column table consisting of the options and option descriptions.

Option	Description
status	Display status
enable	Enable debug access (default if no option specified)
disable	Disable debug access

Chapter 11. IPMI interface

This chapter describes the IPMI interface supported by the XClarity Controller.

For details of the standard IPMI commands, refer to the Intelligent Platform Management Interface (IPMI) Specification document (version 2.0 or above). This document provides descriptions on the OEM parameters used with the standard IPMI and OEM IPMI commands supported by the XClarity Controller firmware.

Managing the XClarity Controller with IPMI

Use the information in this topic to manage the XClarity Controller using the Intelligent Platform Management Interface (IPMI).

The XClarity Controller comes with a user ID set initially to a user name of USERID and password of PASSW0RD (with a zero, not the letter O). This user has Supervisor access.

Important: Change this user name and password during your initial configuration for enhanced security.

In a Flex System, a user can configure a Flex System CMM to centrally manage the XClarity Controller IPMI user accounts. In this circumstance, you might not be able to access the XClarity Controller using the IPMI until the CMM has configured the IPMI user IDs.

Note: The user ID credentials configured by the CMM might be different than the USERID/PASSW0RD combination described above. If no IPMI user IDs have been configured by the CMM, the network port associated with the IPMI protocol will be closed.

The XClarity Controller also provides the following IPMI remote server management capabilities:

IPMI Command-line interfaces
The IPMI command line interface provides direct access to server-management functions through the IPMI 2.0 protocol. You can use the IPMItool to issue commands to control server power, view server information, and identify the server. For more information about the IPMItool, see “Using IPMItool” on page 175.

Serial over LAN
To manage servers from a remote location, use the IPMItool to establish a Serial over LAN (SOL) connection. For more information about the IPMItool, see “Using IPMItool” on page 175.

Using IPMItool

Use the information in this topic to access information about the IPMItool.

The IPMItool provides various tools that you can use to manage and configure an IPMI system. You can use the IPMItool in-band or out-of-band to manage and configure the XClarity Controller.

For more information about the IPMItool, or to download the IPMItool, go to https://github.com/ipmitool/ipmitool.

© Copyright Lenovo 2017, 2020

IPMI Commands with OEM Parameters

Get / Set LAN Configuration Parameters

In order to reflect the capabilities provided by the XCC for some of the network settings, the values for some of the parameter data is defined as shown below.

DHCP

In addition to the usual methods of obtaining an IP address, the XCC provides a mode where it attempts to obtain an IP address from a DHCP server for a given period of time and if unsuccessful fails over to using a static IP address.

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Parameter	#	Parameter Data
IP Address Source	4	data 1 [7:4] – reserved [3:0] – address source 0h = unspecified 1h = static address (manually configured) 2h = address obtained by XCC running DHCP 3h = address obtained by BIOS or system software 4h = address obtained by XCC running other address assignment protocol. The XCC uses the value 4h to indicate the address mode of DHCP with failover to static.

Ethernet Interface Selection

The XCC hardware contains dual 10/100 Ethernet MACs with RMII interfaces. The XCC hardware also contains dual 1Gbps Ethernet MACs with RGMII interfaces. One of the MACs is usually connected to the shared server NIC and the other MAC is used as a dedicated system management port. Only one Ethernet port on a server is active at a given time. Both ports will not be simultaneously enabled.

On some servers, the system designers may choose to connect up only one or the other of these Ethernet interfaces on the system planar. In those systems, only the Ethernet interface that is connected on the planar is supported by the XCC. A request to use the unconnected port returns a CCh completion code.

The package IDS for all optional network cards are numbered as follows:

- optional card #1, package ID = 03h (eth2),
- optional card #2, package ID = 04h (eth3),

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Parameter	#	Parameter Data
OEM Parameter This parameter number is used by the XCC to indicate which of the possible Ethernet ports (logical packages) should be used. This parameter in the Get/Set LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The response data will return 3 bytes, or optionally 4 bytes if the device is in an NCSI package. Byte 1 = completion code Byte 2 = revision Byte 3 = 00h for eth0, or 01h for eth1, etc… Byte 4 = (optional) channel number, if the device is an NCSI package	C0h	data1 00h = eth0 01h = eth1 02h = eth2 etc… FFh = disable all external network ports) XCC supports a 2nd optional data byte to specify which channel in a package is used data2 00h = channel 0 01h = channel 1 etc… If data2 is not specified in the request, channel 0 is assumed

The data1 byte is used to specify the logical package. It may be a dedicated systems management NIC or an NCSI interface into the NIC shared with the server.

The data2 byte is used to specify the channel for logical package, if the package is an NCSI device. If the data2 is not specified in the request and the logical package is an NCSI device, channel, 0 is assumed. I data2 is specified in the request but the logical package is not an NCSI device, the channel information is ignored.

Examples:

Appendix A. If channel 2 of the shared NIC on the planar (package ID = 0, eth0) is to be used as the management port , the input data would be: 0xC0 0x00 0x02

Appendix B: If the first channel of the first network mezzanine card is to be used, the input would be: 0xC0 0x02 0x0

Ethernet over USB Enable/Disable

The parameter below is used to enable or disable the XCC inband interface.

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Parameter	#	Parameter Data
OEM Parameter (This parameter number is used by the XCC to enable or disable the Ethernet over USB interface.) This parameter in the Get LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (disabled), or 01h (enabled)	C1h	data 1 0x00 = disabled 0x01 = enabled

The data1 byte is used to specify the logical package. It may be a dedicated systems management NIC or an NCSI interface into the NIC shared with the server.

The data2 byte is used to specify the channel for logical package, if the package is an NCSI device. If the data2 is not specified in the request and the logical package is an NCSI device, channel, 0 is assumed. I data2 is specified in the request but the logical package is not an NCSI device, the channel information is ignored.

Examples:

Appendix A. If channel 2 of the shared NIC on the planar (package ID = 0, eth0) is to be used as the management port , the input data would be: 0xC0 0x00 0x02

Appendix B: If the first channel of the first network mezzanine card is to be used, the input would be: 0xC0 0x02 0x0

IPMI option for getting the DUID-LLT

An additional read-only value that needs to be exposed via IPMI is the DUID. According to RFC3315, this format of DUID is based on the Link Layer Address Plus Time.

Parameter	#	Parameter Data
OEM Parameter (This parameter number is used by the XCC to enable or disable the Ethernet over USB interface.) This parameter in the Get LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The response data will return 3 bytes: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec) Byte 3 = length of following data bytes (16 bytes currently) Byte 4-n DUID_LLT	C2h	

Ethernet configuration parameters

The parameters below may be used to configure specific Ethernet settings.

Parameter	#	Parameter Data
OEM Parameter (This parameter number is used by the XCC to enable or disable Auto-negotiation setting for Ethernet Interface.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (disabled), or 01h (enabled)	C3h	data 1 0x00 = disabled 0x01 = enabled Note: On Flex and Stark systems the auto-negotiation setting is not changeable because it could break the network communication path via the CMM and SMM.
OEM Parameter (This parameter number is used by the XCC to get or set the Data rate of Ethernet Interface.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (10Mb), or 01h (100Mb)	C4h	data 1 0x00 = 10Mbit 0x01 = 100Mbit

Parameter	#	Parameter Data
OEM Parameter (This parameter number is used by the XCC to get or set the Duplex setting of the Ethernet interface.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (Half Duplex), or 01h (Full Duplex)	C5h	data 1 0x00 = Half Duplex 0x01 = Full Duplex
OEM Parameter (This parameter number is used by the XCC to get or set the Maximum transmission unit (MTU) of the Ethernet interface.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3-4 = size of MTU	C6h	data 1 Size of MTU
OEM Parameter (This parameter number is used by the XCC to get or set Locally administered MAC address.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 – 8 = Mac Address	C7h	data 1 - 6 Mac Address

IPMI option for getting the Link-Local Address

This is a read-only parameter to retrieve the IPV6 Link-Local Address.

Parameter	#	Parameter Data
OEM Parameter This parameter is used to obtain the Link-Local address of the XCC: The response data will return the following: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec) Byte 3 = IPV6 address prefix length Byte 4-19 Local Link address in binary format	C8h	

IPMI option for enabling/disabling IPv6

This is a read/write parameter to enable/disable IPV6 in the XCC.

Parameter	#	Parameter Data
OEM Parameter This parameter is used to enable/ disable IPv6 in the XCC The response data will return the following: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec) Byte 3 = 00h (disabled), or 01h (enabled)	C9h	data 1 0x00 = disabled 0x01 = enabled

Ethernet-over-USB Pass-through to external network

The parameter below is used to configure the Ethernet-over-USB to external Ethernet pass-through.

Parameter	#	Parameter Data
OEM Parameter This parameter in the Get/Set LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The Get response data will return the following: Byte 1 = completion code Byte 2 = revision Byte 3 = reserved (00h) Bytes 4:5 = Ethernet-over-USB Port number (LSByte first) Bytes 6:7 = External Ethernet Port number (LSByte first) The number of bytes to follow can vary (1, 4, or 16 bytes) depending upon the addressing mode: • Byte 8 = pre-defined modes: 00h = the pass-through is disabled 01h = the CMM's IP address is used Bytes 8:11 = IPv4 external network IP address in binary form Bytes 8:23 = IPv6 external network IP address in binary form Completion codes: 00h – success 80h – parameter not supported C1h – command not supported C7h – request data length invalid	CAh	Set LAN Configuration Parameters: data 1 reserved (= 00h) data 2:3 Ethernet over USB Port number, LSByte first data 4:5 External Ethernet Port number, LSByte first The number of bytes to follow can vary (1, 4, or 16 bytes) depending upon the addressing mode: data 6 00h = disable the pass-through 01h = use the CMM's IP address data 6:9 IPv4 external network IP address in binary form data 6:21 IPv6 external network IP address in binary form
OEM Parameter This parameter is used to set and get the lan over usb ip address and netmask of the XCC: The response data will return the following: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec)	CBh	Data 1:4 IP address of XCC -side lan over usb interface. Data 5:8 Netmask of XCC -side lan over usb interface

Parameter	#	Parameter Data
Byte 3:10 = IP address and Netmask value (MS-byte) first		
OEM Parameter This parameter is used to set and get the lan over usb ip address of the Host OS: The response data will return the following: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec) Byte 3:6 = IP address (MS-byte) first	CCh	Data 1:4 IP address of Host-side lan over usb interface.

Query Logical Package Inventory

The parameter below is used to query NCSI package inventory.

Parameter	#	Parameter Data
OEM Parameter This parameter in the Get/Set LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. Query package inventory operation The query package information operation is performed by issuing the request with two 0x00 data bytes besides the D3h parameter number. Query package inventory : --> 0x0C 0x02 0x00 0xD3 0x00 0x00 The XCC response includes a byte of information for each package that is present: bits 7:4 = number of NCSI channels in the package bits 3:0 = the logical package number Response --> 0x00 0x00 0x40 0x01 0x32 indicates that 3 logical packages are present: package 0 has 4 NCSI channels package 1 is not an NCSI NIC , so it does not support NCSI channels package 2 has 3 NCSI channels	D3h	Get/Set LAN Configuration Parameters:

Get/Set Logical Package Data

The parameter below is used to read and to set the priority assigned to each package.

Parameter	#	Parameter Data
OEM Parameter This parameter in the Get/Set LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The command supports 2 operations: • Read package priority • Set package priority Read package priority operation The read package priority operation is performed by issuing the request with two 0x00 data bytes besides the D4h parameter number. Read package priority: --> 0x0C 0x02 0x01 0xD4 0x00 0x00 Response --> 0x00 0x00 0x00 0x12 0x23 logical package 0 = priority 0 logical package 2 = priority 1 logical package 3 = priority 2 Set package priority operation The set package priority operation is performed by issuing the request with one or more parameters in addition to the D4h parameter number. Set package priority: --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 set logical package 0 = priority 0 set logical package 2 = priority 1 set logical package 3 = priority 2 Response:	D4	Get/Set LAN Configuration Parameters: Bit [7-4] = priority of the logical package (1 = highest, 15 = lowest) Bit [3-0] = logical package number

Parameter	#	Parameter Data
completion code only, no additional data		

Get/Set XCC networking synchronization status

Parameter	#	Parameter Data
OEM Parameter The byte is used to config to synchronize networking setting between dedicated and shared nic mode This parameter in the Get LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (enabled) , or 01h (disabled)	D5h	data 1 0x00 = Synchronization 0x01 = Independence

The byte is used to config to synchronize networking setting between dedicated and shared nic mode , the default value was 0h here, it mean XCC will automatically update networking setting between mode change and use shared nic (on board) as major reference , if set as 1h , each networking setting will be independent here , which is we can configure different networking setting between mode, such as VLAN enable on Dedicated and set VLAN disable on Shared NIC mode.

Get/Set XCC networking mode

Parameter	#	Parameter Data
OEM Parameter This parameter is used to get/set network mode of XCC management NIC. The response data will return 4 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = applied/specified netmode Byte 4 = package id of applied netmode Byte 5 = channel id of applied netmode	D6h	Set LAN Configuration Parameters: data 1 Netmode to set Get LAN Configuration Parameters: data 1 Netmode to get, This is an optional data, defaults to query current netmode

OEM IPMI Commands

The XCC supports the following IPMI OEM commands. Each command requires a different level of privilege as listed as below.

Code	Netfn 0x2E Commands	Privilege
0xCC	Reset XCC to Default	PRIV_USR

Code	Netfn 0x3A Commands	Privilege
0x00	Query Firmware version	PRIV_USR
0x0D	Board Information	PRIV_USR
0x1E	Chassis Power Restore Delay Options	PRIV_USR
0x38	NMI and Reset	PRIV_USR
0x49	Initiate Data Collection	PRIV_USR
0x4A	Push File	PRIV_USR
0x4D	Data Collection Status	PRIV_USR
0x50	Get Build Information	PRIV_USR
0x55	Get/Set Host Name	PRIV_USR
0x6B	Query FPGA Firmware Revision Level	PRIV_USR
0x6C	Query Board Hardware Revision Level	PRIV_USR

Code	Netfn 0x3A Commands	Privilege
0x6D	Query PSoC Firmware Revision Level	PRIV_USR
0x98	FP USB Port Control	PRIV_USR
0xC7	Native NM IPMI Switch	PRIV_ADM

Reset XCC to Default Command

This command resets the XCC configuration setting to the default values.

Net Function = 0x2E			
Code	**Command**	**Request, Response Data**	**Description**
0xCC	Reset XCC to Default	**Request:** Byte 1 – 0x5EByte 2 – 0x2B Byte 3 – 0x00 Byte 4 – 0x0AByte 5 – 0x01 Byte 6 – 0xFF Byte 7 – 0x00Byte 8 – 0x00 Byte 9 – 0x00 **Response:** Byte 1 – Completion CodeByte 2 – 0x5EByte 3 – 0x2B Byte 4 – 0x00 Byte 5 – 0x0AByte 6 – 0x01 Byte 7 – Response Data 0 = Success non-zero = Failure	This command resets the XCC configuration settings to the default values.

Board / Firmware Information Commands

This section lists the commands for querying the board and firmware information.

Net Function = 0x3A			
Code	**Command**	**Request, Response Data**	**Description**
0x00	Query Firmware Version	**Request**: No data on request **Response**: Byte 1 – Completion Code Byte 2 – Major version Byte 3 – Minor version	This command returns the major and minor version numbers of the firmware. If the command is made with the optional 1 byte of request data, the XCC response also returns the third field (Revision) of the version. (Major.Minor.Revision)
0x0D	Query Board Information	**Request**: N/A **Response**: Byte 1 – System ID Byte 2 – Board Revision	This command returns the Board ID and planar revision.
0x50	Query Build Information	**Request**: N/A **Response**: Byte 1 – Completion Code. Bytes 2:10 – ASCIIZ Build Name Bytes 11:23 – ASCIIZ Build Date Bytes 24:31 – ASCII Build Time	This command returns the build name, build date, and build time. The build name and build date strings have a zero termination. The format of the build date is YYYY-MM-DD. e.g. “ZUBT99A ” “2005-03-07” “23:59:59”

Net Function = 0x3A			
Code	**Command**	**Request, Response Data**	**Description**
0x6B	Query FPGA Firmware Revision Level	**Request**: Byte 1 – FPGA Device Type* FPGA Device Type 0 = Local (Active level) 1 = CPU Card 1 (Active level) 2 = CPU Card 2 (Active level) 3 = CPU Card 3 (Active level) 4 = CPU Card 4 (Active level) 5 = Local Primary ROM 6 = Local Recovery ROM **Response**: Byte 1 – Completion Code Byte 2 – Major revision level Byte 3 – Minor revision level Byte 4 – Sub-Minor revision level (Test Byte on XCC platforms)	This command returns the revision level of the FPGA firmware. If Byte 1 is omitted then Local (Active level) will be selected
0x6C	Query Board Hardware Revision Level	**Request**: No Data. **Response**: Byte 1 – Completion Code Byte 2 – Revision level	This command returns the revision level of the board hardware where the FPGA resides.
0x6D	Query PSoC Firmware Revision Level	**Request**: None **Response**: Byte 1 – Completion Code Byte 2 – bin# Byte 3 – APID Byte 4 – Rev Byte 5-6 – FRU ID	This command returns the revision level of all of the detected PSoC devices. Note: bin# represents a physical location. Consult the system specification for details.

Net Function = 0x3A			
Code	**Command**	**Request, Response Data**	**Description**
		Bytes 6:N – repeat of Bytes 2-6 for each detected PSoC	

System Control Commands

The IPMI specification provides basic power and reset control. Lenovo adds additional control functions.

<table>
<tr><th colspan="4">Net Function = 0x2E</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr><td>0x1E</td><td>Chassis Power Restore Delay Options</td><td>Request:<table><tr><td>Byte 1</td><td>Request Type:

0x00 = Set Delay Options

0x01 = Query Delay Options</td></tr><tr><td>Byte 2</td><td>(if byte 1 = 0x00)

0x00 = Disabled (default)

0x01 = Random

0x02 - 0xFF Reserved</td></tr></table>Response:

Byte 1 – Completion Code

Byte 2 – Delay Options (for Query request only)</td><td>This setting is used, when the chassis power restore policy is set to always power-on or restore to power-on (if previously powered-on), after AC is applied/returns. There are 2 choices: Disabled (the default setting, no delay when powered-on), and Random. The random delay setting, provides a random delay between 1 and 15 seconds, from the time AC is applied/returns and when the server is automatically powered-on.

The command is supported by XCC only on Rack servers.</td></tr>
<tr><td>0x38</td><td>NMI and reset</td><td>Request:

Byte 1 – Number of seconds
0 = NMI Only

Byte 2 – Reset type
0 = soft reset
1 = power cycle

Response :

Byte 1 – Completion code</td><td>This command is used to perform a system NMI. Optionally the system can be reset (rebooted) or power cycled after the NMI.

If the “Number of Seconds” field is not 0, then the system will be reset or power cycled after the specified number of seconds.

Byte 2 of the request is optional. If byte 2 is not provided, or if it has a value of 0x00, a soft reset is performed. If byte 2 is 0x01, the system is power cycled.</td></tr>
</table>

Miscellaneous Commands

This section is for commands that do not fit into any other section.

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr><td>0x55</td><td>Get/Set Hostname</td><td>Request Length = 0:

Empty Request Data

Response:

<table><tr><td>Byte 1</td><td>Completion Code</td></tr><tr><td>Bytes 2-65</td><td>Current Hostname.

ASCIIZ, Null terminated string.</td></tr></table>
Request Length 1-64:

<table><tr><td>Bytes 1-64</td><td>DHCP Hostname

ASCIIZ Terminate with 00h</td></tr></table></td><td>Use this command to Get/Set the Hostname.

When setting the Hostname, the desired value must be terminated by a 00h. The hostname is limited to 63 characters plus the null.</td></tr>
<tr><td>0x98</td><td>FP USB Port Control</td><td>Request:

Byte 1

<table><tr><td>01h:</td><td>Get current owner of front panel USB port</td></tr></table>
Response:

Byte 1 – Completion Code

Byte 2

<table><tr><td>00h:</td><td>Owned by host</td></tr><tr><td>01h:</td><td>Owned by BMC</td></tr></table>
Request:

Byte 1

<table><tr><td>02h:</td><td>Get the configuration of front panel USB port</td></tr></table></td><td>This command is used for query status/configuration of FP USB port, configure mode/timeout of FP USB port and switch USB port owner between host and BMC

In configuration, FP USB can has 3 modes – dedicated to host, solely owned by BMC or shared mode that allows owner switch between host and BMC.

If shared mode is enabled, the USB port is connected to BMC when server is powered off and connected to the server when the server power is on.

When shared mode is enabled and server power is on, the BMC will return USB port back to the server after inactivity timeout in configuration occurs.

If the server has identification button, users can enable/disable the ID button to switch owner of FP USB port by holding the ID button for more than 3 seconds.

Hysteresis in seconds will be set when automatically switching the</td></tr>
</table>

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr><td></td><td></td><td>Response:

Byte 1 – Completion Code

Byte 2

<table><tr><td>00h:</td><td>Dedicated to host</td></tr><tr><td>01h:</td><td>Dedicated to BMC</td></tr><tr><td>02h:</td><td>Shared mode</td></tr></table>
Byte 3:4 – Inactivity timeout in minutes(MSB first)

Byte 5 – Enable ID button

<table><tr><td>00h:</td><td>Disabled</td></tr><tr><td>01h:</td><td>Enabled</td></tr></table>
Byte 6 – Hysteresis (optional) in seconds

Request:

Byte 1

03h: set the configuration of front panel USB port

Byte 2

<table><tr><td>00h:</td><td>Dedicated to host</td></tr><tr><td>01h:</td><td>Dedicated to BMC</td></tr><tr><td>02h:</td><td>Shared mode</td></tr></table>
Byte 3:4 – Inactivity timeout in minutes(MSB first)

Byte 5 – Enable ID button

<table><tr><td>00h:</td><td>Disabled</td></tr><tr><td>01h:</td><td>Enabled</td></tr></table>
Byte 6 – Hysteresis (optional) in seconds

Response:

Byte 1 – Completion CodeByte 2</td><td>port during the power cycle. This is an optional parameter.

SD530 Servers

On the SD530 platform the port is optional and if present is wired directly to the XCC, and only to the XCC. Switching the port to the Host in not available.

• When the command is issued with byte 1 = 1, the XCC will always respond that the port is owned by the BMC.
• When the command is issued with byte 1 = 2, the XCC will always respond that the port is dedicated to the BMC.
• When the command is issued with byte 1 = 3 or byte 1 =4, the XCC will respond with completion code D6h.

Non-SD530 Servers

On the non-SD530 platform the XCC’s use of the front panel USB port can be disabled by switching to the “Host Only” mode.

When the command is issued with byte 1 = 5 or byte 1 =6, the XCC will respond with completion code D6h.</td></tr>
</table>

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>00h:</td><td>Switch to host</td></tr>
<tr><td>01h:</td><td>Switch to BMC</td></tr>
</table>
Response:

Byte 1 – Completion Code

Byte 1
<table>
<tr><td>05h:</td><td>Enable/ Disable the front panel USB port</td></tr>
</table>
Byte 2
<table>
<tr><td>00h:</td><td>Disable</td></tr>
<tr><td>01h:</td><td>Enable</td></tr>
</table>
Response:

Byte 1 – Completion Code

Request:

Byte 1
<table>
<tr><td>06h:</td><td>Read the Enable/ Disable state of the front panel USB port</td></tr>
</table>
Response:

Byte 1 - Completion Code

Byte 2</td><td></td></tr>
<tr><td>0xC7</td><td>Native NM IPMI Switch</td><td>Request Length = 0:

Empty request data

Response:
<table>
<tr><td>Byte 1</td><td>Completion Code</td></tr>
<tr><td>Bytes 2</td><td>Current Enable/ Disable Status</td></tr>
</table></td><td>This command is used to enable/ disable the bridging function of XCC for Native Intel IPMI commands.</td></tr>
</table>

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr><td></td><td></td><td>Request Length= 1:
<table><tr><td>Byte 1</td><td>Native NM IPMI Interface Enable/ Disable attribute

00h – Disable

01h – Enable</td></tr></table>Response:
<table><tr><td>Byte 1</td><td>Completion Code</td></tr></table></td><td></td></tr>
</table>

Chapter 12. Edge servers

This topic describes specific functions for Edge servers.

Notes:

1. The system requires you to change the XCC password on you first login.
2. The IPMI-over-LAN is disabled by default.
3. The IPMI-over-KCS is disabled by default.

System Lockdown Mode

When **System Lockdown Mode** is in active state, it means that system is under lockdown mode. You could activate the system and unlock it, otherwise the host system will not be allowed to boot.

Click **Security** under **BMC Configuration** and scroll to **System Lockdown Mode**.

System Lockdown Mode

To activate the system and exit **System Lockdown Mode**, complete the following steps.

1. Click **Inactive** button and a **Key Vault Activation** window will pop-up to show the **Challenge Text**.
2. Contact your IT administrator and provide **Challenge Text**.
3. Obtain **Challenge Response** from your IT administrator and enter it in **Key Vault Activation** window.
4. Click **OK** button and then Click **Apply**.
5. If all setting works correctly, you will see **System Lockdown Mode** changes to **Inactive**.

Note: When System Lockdown Mode is in active state, any access to system secrets is **denied.** such as SED keys.

To force the system to enter System Lockdown Mode, complete the following steps.

1. Click **Active** button.
2. Click **OK** button and then Click **Apply**.

Motion Detection

You can enable this function to protect your server by detecting any physical movement of your server. If Motion Detection is enabled, you can set the following items depending on your preference and configuration.

- **Sensitivity Level**: Select the sensitivity level from **Low**, **Medium** and **High** according to your preference
- **Orientation**: Select your configuration from **Stand Desktop**, **Wall Mount (Horizontal)**, **Wall Mount (Vertical)**, **Bookshelf** and **Ceiling Mount**.

Note: Motion Detection would be disabled automatically when the system entering the lockdown mode.

Chassis Intrusion Detection

You can enable this function to protect your server by detecting any physical movement of the top cover.

Additional Configurations

If the Wireless enabled LOM Package is installed, there are three settings you can choose for a detected tamper event.

© Copyright Lenovo 2017, 2020

Under some unusual circumstances, **Challenge Text** may fail to be verified by ThinkShield Key Vault Portal, it might be necessary to reset the device internal counter prior to activate the device under your IT administrator's request.

SED Authentication Key (AK) Manager

To the system installed with SED (self-encrypting drive), this feature controls BMC to deploy SED key. You can use SED key to encrypt boot and data drives and boot the system without manual intervention

Note: This operation is not allowed when the system is not activated (System Lockdown Mode is asserted) or current user does not have the authority to manage SED key.

Click **Security** under **BMC Configuration** and scroll to **SED Authentication Key (AK) Manager**.

Change the SED AK

Generate SED AK from Passphrase: Set the password and reenter it for the confirmation. Click **Re-generate** to get the new SED AK.
Generate a Random SED AK: Click **Re-generate** to get a Random SED AK.
Backup the SED AK: Set the password and re-enter it for the confirmation. Click **Start Backup** to back the SED AK; then, download the SED AK file and store it safely for future use.

Note: If you use the backup SED AK file to restore a configuration, the system will ask for the password that you set here.

Recover the SED AK: You can only perform this task while the SED is not functioning properly. There are two ways to recover the SED AK:

- **Recover SED AK using Passphrase**: Use the password that set in **Generate SED AK from Passphrase** mode to recover the SED AK.
- **Recover SED AK from Backup file**: Upload the backup file generated in **Backup the SED AK** mode and enter the corresponding backup file password to recover the SED AK.

Edge Networking

This function page only supported while the Wireless enabled LOM Package is installed.

For the network topology preset tables, please see https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html for more details.

Wi-Fi Connectivity

Click **Enabled** and you can configure settings according to your Wi-Fi configuration.

LTE Connectivity

This allows you to control LTE connectivity for the Edgenetwork board.

Edge Network Board Address

IPv4 or IPv6 status	**DHCP Server** status	**Method**
Disabled	**Disabled**	**Obtain IP from DHCP**
Enabled	**Enabled**	**Use static IP address**
Enabled	**Disabled**	**Obtain IP from DHCP** or **Use static IP address** depending on your usage.

BMC Network Bridge

You can access the BMC via **Down Link Ports**, **Wi-Fi Ports**, **Up Link Ports** or **None**.

Note: Select **None** refers that this function is disabled.

Edge Network Board Troubleshooting

Restart Immediately: You can restart the network board by this button.
Reset To Factory Defaults: You can reset the network board to default setting by this button.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support are available at:

http://datacentersupport.lenovo.com

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for ThinkSystem.

Before you call

Before you call, there are several steps that you can take to try and solve the problem yourself. If you decide that you do need to call for assistance, gather the information that will be needed by the service technician to more quickly resolve your problem.

Attempt to resolve the problem yourself

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

You can find the product documentation for your ThinkSystem products at the following location:

http://thinksystem.lenovofiles.com/help/index.jsp

You can take these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.lenovo.com/serverproven/ to make sure that the hardware and software is supported by your product.
- Go to http://datacentersupport.lenovo.com and check for information to help you solve the problem.
  - Check the Lenovo forums at https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg to see if someone else has encountered a similar problem.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error

© Copyright Lenovo 2017, 2020

messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Gathering information needed to call Support

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call. You can also see http://datacentersupport.lenovo.com/warrantylookup for more information about your product warranty.

Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.

- Hardware and Software Maintenance agreement contract numbers, if applicable
- Machine type number (Lenovo 4-digit machine identifier)
- Model number
- Serial number
- Current system UEFI and firmware levels
- Other pertinent information such as error messages and logs

As an alternative to calling Lenovo Support, you can go to https://www-947.ibm.com/support/servicerequest/Home.action to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The Lenovo service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

Collecting service data

To clearly identify the root cause of a server issue or at the request of Lenovo Support, you might need collect service data that can be used for further analysis. Service data includes information such as event logs and hardware inventory.

Service data can be collected through the following tools:

- **Lenovo XClarity Controller**

  You can use the Lenovo XClarity Controller web interface or the CLI to collect service data for the server. The file can be saved and sent to Lenovo Support.

  - For more information about using the web interface to collect service data, see http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_servicesandsupport.html.
  - For more information about using the CLI to collect service data, see http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator can be set up to collect and send diagnostic files automatically to Lenovo Support when certain serviceable events occur in Lenovo XClarity Administrator and the managed endpoints. You can choose to send diagnostic files to Lenovo Support using Call Home or to another service provider using SFTP. You can also manually collect diagnostic files, open a problem record, and send diagnostic files to the Lenovo Support Center.

  You can find more information about setting up automatic problem notification within the Lenovo XClarity Administrator at http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html.

- **Lenovo XClarity Provisioning Manager**

Use the Collect Service Data function of Lenovo XClarity Provisioning Manager to collect system service data. You can collect existing system log data or run a new diagnostic to collect new data.

- **Lenovo XClarity Essentials**

  Lenovo XClarity Essentials can be run in-band from the operating system. In addition to the hardware service data, Lenovo XClarity Essentials can collect information about the operating system, such as the operating system event log.

  To obtain service data, you can run the **getinfor** command. For more information about running the **getinfor**, see http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_getinfor_command.html.

Contacting Support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/us/en/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/us/en/supportphonelist for your region support details.

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2017, 2020

Trademarks

Lenovo, the Lenovo logo, ThinkSystem, Flex System, System x, NeXtScale System, and x Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 70. Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Additional electronic emissions notices are available at:

http://thinksystem.lenovofiles.com/help/index.jsp

Taiwan BSMI RoHS declaration

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1. ˋ超出0.1 wt％″ 及 ˋ超出0.01 wt％″ 係指限用物質之百分比含量超出百分比含量基準值。

Note1 : "exceeding 0.1wt%" and "exceeding 0.01 wt%" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. ˋ○″ 係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : " ○ "indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. ˋ - ″ 係指該項限用物質為排除項目。

Note3 : The "-" indicates that the restricted substance corresponds to the exemption.

Taiwan import and export contact information

Contacts are available for Taiwan import and export information.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Index

A

absolute mouse control 64
accseccfg command 107
activation key
  export 86
  install 85, 122
  manage 122
  remove 86, 122
Active Directory Users
  LDAP 149
active system events
  overview 47
adapter command 170
adapter information
  Server Configuration 55
advanced Ethernet
  settings 29, 176
advanced management module 1
Agent-less commands 161
alertcfg command 109
alertentries command 153
alphabetical command list 91
asu command 109
audit log 51
autonegotiation
  set 120

B

backup command 112
baseboard management controller (BMC) 1
batch command 155
binding method
  LDAP server 124
BIOS (basic input/output system) 1
block list and time restriction
  settings 34
blue screen capture 63
BMC
  certificate signing request 40
BMC management
  BMC configuration
    back up BMC configuration 45
    backup and restore BMC configuration 45
    restore BMC configuration 46
    restore to factory default 46
browser requirements 6

C

CA-signed
  certificate 40
call home
  configuring 43
centralized management
  encryption keys 39
certificate classifications
  CA-signed 40
  self-assigned 40
certificate management
  CIM over HTTPS 139–140
  client 40
  Drive Access 143
  HTTPS server 139–140
  LDAP 139–140
  server 43
  SSH server 138
certificate signing request
  BMC 40
chconfig command 158
chlog command 160
chmanual command 160
CIM over HTTP port
  set 128
CIM over HTTPS
  certificate management 139–140
  security 139–140
CIM over HTTPS port
  set 128
clearcfg command 156
clearlog command 94
CLI key sequence
  set 126
client
  certificate management 40
client certificate management
  CA-signed 40
  self-assigned 40
client distinguished name
  LDAP server 124
clock command 156
collecting service data 75, 202
command-line interface (CLI)
  accessing 89
  command syntax 90
  description 89
  features and limitations 90
  logging in 89
commands
  accseccfg 107
  adapter 170
  alertcfg 109
  alertentries 153
  asu 109
  backup 112
  batch 155
  chconfig 158
  chlog 160
  chmanual 160
  clearcfg 156
  clearlog 94
  clock 156
  console 107
  dbgshimm 173
  dhcpinfo 113
  dns 114
  encaps 116
  ethtousb 116
  exit 93
  fans 95
  ffdc 95
  firewall 117
  fuelg 105
  gprofile 118
  hashpw 119
  help 93
  history 93
  hreport 96
  identify 156
  ifconfig 120
  info 157
  keycfg 122
  ldap 124
  led 97

© Copyright Lenovo 2017, 2020

mhlog 97
mvstor 172
ntp 125
portcfg 126
portcontrol 127
ports 128
power 103
pxeboot 106
rdmount 129
readlog 99
reset 105
restore 130
restoredefaults 131
roles 131
seccfg 133
set 133
smtp 133
snmp 134
snmpalerts 136
spreset 158
srcfg 137
sshcfg 138
ssl 139
sslcfg 140
storage 161
storekeycfg 143
syncrep 144
syshealth 100
temps 101
thermal 145
timeouts 146
TLS 146
trespass 147
uefipw 148
usbeth 148
usbfp 148
users 149
volts 101
vpd 102
commands, alphabetical list 91
commands, types of
Agent-less 161
configuration 107
IMM control 152
monitor 94
serial redirect 107
server power and restart 103
service advisor 158
Support 173
utility 93
configuration commands 107
configuration restore
IMM 130
configure
block list and time restriction 34
DDNS 114
DDNS settings 31
DNS 114
DNS settings 31
Ethernet 120
Ethernet over USB 116
Ethernet over USB settings 32
Ethernet settings 29, 176
IPMI 33
IPMI over KCS Access 38
IPv4 120
IPv6 120
LDAP 124
LDAP server 124
LDAP settings 24
network protocols 29
network service port 127
port assignments 33
ports 128
prevent system firmware down-level 38
security settings 36
serial port 126
SKLM device group 40
SKLM key repository servers 40
SMTP 133
SNMPv1 134
SNMPv1 traps 134
SNMPv3 alert settings 32
SNMPv3 user accounts 149
SSH server 38
USB 116
user account security levels 107
configuring
front panel USB port to management 35
global login settings 22
serial-to-SSH redirection 89
configuring the server
options to configure
the server 55
configuring the storage
options to configure
the storage 79
configuring the XClarity Controller
options to configure
the XClarity Controller 17
console command 107
contamination, particulate and gaseous 206
create
user account 149
creating a personalized support web page 201
custom support web page 201

D

date
set 156
date and time, XClarity Controller
setting 77
dbgshimm command 173
dcmi
functions and commands 60
power management 60
DDNS
configure 114
custom domain name 114
DHCP server specified domain name 114
domain name source 114
manage 114
default configuration
IMM 131
default static IP address 10
delete
user 149
delete group
enable, disable 118
device group
drive access page 40
dhcpinfo command 113
distinguished name, client
LDAP server 124
distinguished name, root
LDAP server 124
DNS
configure 114
IPv4 addressing 114
IPv6 addressing 114
LDAP server 124
server addressing 114
dns command 114
domain name source
DDNS 114
domain name, custom
DDNS 114

domain name, DHCP server specified
DDNS 114
Drive Access
certificate management 143
security 143
drive access page
configure 40
device group 40
SKLM certificate management 40
SKLM key repository servers 40
Drive Access tab
security option 39–40

E

email and syslog notifications 52
encaps command 116
encryption keys
centralized management 39
enhanced role-based security
LDAP 149
enterprise level features 5
Ethernet
configure 120
Ethernet over USB
configure 116
port forwarding 116
ethtousb command 116
event log 50
event window
log 50–51
exit command 93
exiting the remote console session 75
export
activation key 86
Extended Audit Log
extended audit log 43

F

fans command 95
features of XClarity Controller 2
Features on Demand
install feature 122
manage 122
remove feature 122
ffdc command 95
firewall command 117
firmware
view server 102
firmware, server
updating 83–84
Flex servers 1
Flex System 1
FoD
install feature 122
manage 122
remove feature 122
fuelg command 105
functions and commands
dcmi 60
node manager 59

G

gaseous contamination 206
Getting help 201
global login
settings 22
global login settings
account security policy settings 23
gprofile command 118
group filter
LDAP 124
group search attribute
LDAP 124

H

hardware health 47
hardware service and support telephone numbers 203
hash password 20
hashpw command 119
help 201
help command 93
history command 93
host name
LDAP server 124
set 120
SMTP server 133
hreport command 96
HTTP port
set 128
HTTPS port
set 128
HTTPS server
certificate management 139–140
security 139–140

I

identify command 156
ifconfig command 120
IMM
configuration restore 130
default configuration 131
reset 158
reset configuration 131
restore configuration 130
spreset 158
IMM control commands 152
important notices 206
info command 157
install
activation key 85, 122
install feature
Features on Demand 122
FoD 122
IP address
configuring 9
IPv4 9
IPv6 9
LDAP server 124
SMTP server 133
IP address, default static 10
IPMI
configure 33
remote server management 175
ipmi bridging
power management 59
through XClarity Controller 59
ipmi commands
power consumption 59
IPMI interface
description 175
IPMI over KCS Access
configure 38
IPMItool 175
IPv4
configure 120
IPv4 addressing
DNS 114

© Copyright Lenovo 2017, 2020

IPv6 9
  configure 120
IPv6 addressing
  DNS 114

K

keyboard support in remote console 63
keycfg command 122

L

LDAP
  Active Directory Users 149
  certificate management 139–140
  configure 124
  configuring 17
  enhanced role-based security 149
  group filter 124
  group search attribute 124
  login permission attribute 124
  role-based security, enhanced 149
  security 139–140
  server target name 124
ldap command 124
LDAP server
  binding method 124
  client distinguished name 124
  configure 124
  DNS 124
  host name 124
  IP address 124
  password 124
  port number 124
  pre-configured 124
  root distinguished name 124
  search domain 124
  UID search attribute 124
LDAP server port
  set 124
led command 97
License Management 85
logging in to the XClarity Controller 12
login attempt authentication 17
login permission attribute
  LDAP 124

M

MAC address
  manage 120
maintenance history 51
manage
  activation key 122
  DDNS 114
  Features on Demand 122
  FoD 122
  MAC address 120
  SNMPv1 communities 134
  user 149
management
  server certificate 43
  SKLM certificate 40
managing power
  using IPMI commands 59
maximum transmission unit
  set 120
media mount error issues 73
media mount methods 65
mhlog command 97
MIBs Introduction 7
minimum, levels
  TLS 146
monitor commands 94
monitoring power
  using IPMI commands 59
monitoring the server status 47
mouse control
  absolute 64
  relative 64
  relative with default Linux acceleration 64
mouse support in remote console 63
MTU
  set 120
multiple language support 7
mvstor command 172

N

network connection 10
  default static IP address 10
  IP address, default static 10
  static IP address, default 10
network protocol properties
  assert physical presence 39
  block list and time restriction 34
  DDNS 31
  DNS 31
  Ethernet over USB 32
  Ethernet settings 29, 176
  IPMI 33
  IPMI over KCS Access 38
  port assignments 33
  prevent system firmware down-level 38
  SNMPv3 alert settings 32
network service port
  configure 127
network settings
  IPMI commands 33
new local account
  creating 17
node manager
  functions and commands 59
notes, important 206
notices 205
notices and statements 8
ntp command 125

O

OEM IPMI Commands 187
one-time
  setting up 56
OneCLI 1
online publications
  documentation update information 1
  error code information 1
  firmware update information 1
operating-system requirements 6
operating-system screen capture 63
option
  SKLM 39
OS failure screen data
  capture 54
overview 47
  ssl 36

P

particulate contamination 206

password
  LDAP server 124
  user 149
port assignments
  configure 33
  settings 33
port forwarding
  Ethernet over USB 116
port number
  LDAP server 124
  SMTP server 133
port numbers
  set 128
portcfg command 126
portcontrol command 127
ports
  configure 128
  set numbers 128
  view open 128
ports command 128
power
  managing using IPMI commands 59
  monitoring using IPMI commands 59
power command 103
power consumption
  ipmi commands 59
power management
  dcmi 60
  ipmi bridging 59
power management option
  power actions 58
  power capping policy 57
  power redundancy 57
  power restore policy 58
  Server Management tab 56
pre-configured
  LDAP server 124
prevent system firmware down-level
  configure 38
pxeboot command 106

R

RAID detail
  Server Configuration 79
RAID setup
  Server Configuration 79
rdmount command 129
readlog command 99
relative mouse control 64
relative mouse control for Linux (default Linux acceleration) 64
remote access 2
remote console
  absolute mouse control 64
  keyboard support 63
  mouse support 63
  power and restart commands 62
  relative mouse control 64
  relative mouse control for Linux (default Linux acceleration) 64
  screen capture 63
  video viewer 61
  virtual media session 61
remote console feature 61
remote console functionality 61
  enabling 62
remote console mouse support 63
remote console port
  set 128
remote console screen modes 64
remote power control 62
remove
  activation key 86, 122
remove feature
  Features on Demand 122
  FoD 122
requirements
  operating system 6
  web browser 6
reset
  IMM 158
reset command 105
reset configuration
  IMM 131
restart XClarity Controller 46
restore command 130
restore configuration
  IMM 130
restoredefaults command 131
role-based levels
  operator 118
  rbs 118
  supervisor 118
role-based security, enhanced
  LDAP 149
roles command 131
root distinguished name
  LDAP server 124

S

screen video record/replay
  server management 64
search domain
  LDAP server 124
seccfg command 133
security
  CIM over HTTPS 139–140
  Drive Access 143
  HTTPS server 139–140
  LDAP 139–140
  SSH server 38, 138
  ssl certificate handling 37
  SSL certificate management 37
  ssl overview 36
security option
  Drive Access tab 39–40
Security option
  Drive Access tab 40
self-assigned
  certificate 40
Serial over LAN 175
serial port
  configure 126
serial redirect command 107
serial-to-SSH redirection 89
server
  certificate management 43
  configuration options 55
server addressing
  DNS 114
server certificate
  management 43
server configuration
  server properties 75
Server Configuration
  adapter information 55
  RAID detail 79
  RAID setup 79
server firmware
  updating 83–84
server management
  one-time 56
  OS failure screen data 54
  screen video record/replay 64
  server firmware 83–84

© Copyright Lenovo 2017, 2020

server timeouts, setting 76
system boot mode 55
system boot order 55
Server Management tab
power management option 56
server power and restart
commands 103
server properties
server configuration 75
setting location and contact 75
server status
monitoring 47
server target name
LDAP 124
server timeout
selections 76
service advisor commands 158
service and support
before you call 201
hardware 203
software 203
service data 202
collecting 75
downloading 75
set
autonegotiation 120
CIM over HTTP port 128
CIM over HTTPS port 128
CLI key sequence 126
date 156
host name 120
HTTP port 128
HTTPS port 128
LDAP server port 124
maximum transmission unit 120
MTU 120
remote console port 128
SNMP agent port 128
SNMP Traps port 128
SNMPv1 contact 134
SNMPv3 contact 134
SSH CLI port 128
time 156
user authentication method 107
web inactivity timeout 107
set command 133
set port numbers 128
setting
the XClarity Controller date and time 77
setting location and contact 75
setting server timeouts 76
settings
advanced 29, 176
block list and time restriction 34
DDNS 31
DNS 31
Ethernet 29, 176
Ethernet over USB 32
global login 22
account security policy settings 23
LDAP 24
port assignments 33
security 36
SNMPv3 alert 32
SSH server 38
SKLM
key repository servers 40
option 39
SKLM certificate
management 40
SKLM certificate management
drive access page 40
SKLM device group
configuration 40
SKLM key repository servers
configure 40
drive access page 40
SMTP
configure 133
server host name 133
server IP address 133
server port number 133
smtp command 133
SNMP agent port
set 128
snmp command 134
SNMP TRAP recipients 52
SNMP Traps port
set 128
snmpalerts command 136
SNMPv1
configure 134
SNMPv1 communities
manage 134
SNMPv1 contact
set 134
SNMPv1 traps
configure 134
SNMPv3 contact
set 134
SNMPv3 settings
user 149
SNMPv3 user accounts
configure 149
software service and support telephone numbers 203
spreset command 158
srcfg command 137
SSH CLI port
set 128
SSH keys
user 149
SSH server
certificate management 138
security 138
sshcfg command 138
SSL
certificate handling 37
certificate management 37
ssl command 139
sslcfg command 140
standard level features 2
static IP address, default 10
storage
configuration options 79
storage command 161
storage devices 161
storage devices
storage command 161
storage inventory 80
storekeycfg command 143
Support commands 173
support for multiple languages 7
support web page, custom 201
syncrep command 144
syshealth command 100
system information 48
system utilization 50

T

Taiwan BSMI RoHS declaration 208
Taiwan import and export contact information 208
target name, server
LDAP 124
telecommunication regulatory statement 207
telephone numbers 203
temps command 101
the system information

viewing 48
the system utilization
viewing 50
thermal command 145
ThinkSystem Server Firmware
description 1
time
set 156
timeouts command 146
TLS
minimum level 146
TLS command 146
tools
IPMItool 175
trademarks 206
trespass command 147
trespass message option 76

U

uefipw command 148
UID search attribute
LDAP server 124
USB
configure 116
usbeth command 148
usbfp command 148
user
delete 149
manage 149
password 149
SNMPv3 settings 149
SSH keys 149
user account
create 149
deleting 20
user account security levels
configure 107
user authentication method 17
set 107
users
view current 149
users command 149
using
remote console feature 61
remote console function 61
utility commands 93

V

Video Viewer
absolute mouse control 64
mouse support 63
power and restart commands 62
relative mouse control 64
relative mouse control for Linux (default Linux acceleration) 64
screen capture 63
video color mode 63
view and configure the virtual drives 79
view current
users 149
view firmware information
server 102
view open ports 128
volts command 101
vpd command 102

W

Web browser requirements 6
web inactivity session timeout 22
web inactivity timeout
set 107
web interface
logging in to web interface 12
web interface, opening and using 9
working with
events in the audit log 51
events in the event log 50

X

XClarity Controller
configuration options 17
configure network protocol 29
description 1
features 2
ipmi bridging 59
network connection 10
new functions 1
serial redirection 89
web interface 9
XClarity Controller advanced level 2
XClarity Controller enterprise level 2
XClarity Controller standard level 2
XClarity Controller configuration
configuring call home 43
XClarity Controller features
enterprise level 5
standard level 2
XClarity Controller features advanced level features
advanced level 5
XClarity Controller functions
on web interface 13
XClarity Controller management
configuring LDAP 17
configuring user accounts 17
creating a new local user 17
deleting a user account 20
security settings 36
XClarity Controller properties
date and time 77
XClarity Provisioning Manager
Setup utility 10

© Copyright Lenovo 2017, 2020

Lenovo

Part Number: SP47A30085

Printed in China

(1P) P/N: SP47A30085



Lenovo ThinkSystem SR530 Server (Xeon SP Gen 2)

Product Guide

Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.

Featuring the second generation of the Intel Xeon Processor Scalable Family (Xeon SP Gen 2), the SR530 server offers a balance of performance, capacity and value. The SR530 server supports up to two processors, up to 768 GB of 2933 MHz TruDDR4 memory, 8x 2.5-inch or 4x 3.5-inch drive bays with an extensive choice of SAS/SATA SSDs and SAS/SATA HDDs, and flexible I/O expansion options with a LOM slot and up to 3x PCIe slots.

The SR530 server offers basic software RAID or advanced hardware RAID protection and a wide range of networking options, including embedded LOM, selectable LOM, ML2, and PCIe network adapters. The next-generation Lenovo XClarity Controller, which is built into the SR530 server, provides advanced service processor control, monitoring, and alerting functions.

The following figure shows the ThinkSystem SR530 server with 3.5-inch front hot-swap drives. Other drive configurations are also available.



Figure 1. Lenovo ThinkSystem SR530 with 3.5-inch hot-swap drives

Did you know?

The SR530 server delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies that can deliver 96% (Titanium) or 94% (Platinum) efficiency at 50% load when connected to a 200 - 240 V AC power source.

The SR530 server is designed to meet ASHRAE A4 standards (up to 45 °C) in select configurations, which enable customers to lower energy costs, while still maintaining world-class reliability.

Key features

The SR530 server offers a balance of processing power, expandability, and cost for small and medium businesses up to the large enterprise. Ease of use and comprehensive systems management tools help make deployment easier and efficient design improves your business environment and helps save operational costs.

Scalability and performance

The SR530 server offers numerous features to boost performance, improve scalability, and reduce costs:

- Improves productivity by offering superior system performance with the second generation of the Intel Xeon Processor Scalable Family with up to 22-core processors, up to 30.25 MB of last level cache (LLC), up to 2933 MHz memory speeds, and up to 10.4 GT/s Ultra Path Interconnect (UPI) links.
    - Support for up to two processors, 44 cores, and 88 threads allows to maximize the concurrent execution of multithreaded applications.
    - Intelligent and adaptive system performance with energy efficient Intel Turbo Boost 2.0 Technology allows CPU cores to run at maximum speeds during peak workloads by temporarily going beyond processor thermal design power (TDP).
    - Intel Hyper-Threading Technology boosts performance for multithreaded applications by enabling simultaneous multithreading within each processor core, up to two threads per core.
    - Intel Virtualization Technology integrates hardware-level virtualization hooks that allow operating system vendors to better utilize the hardware for virtualization workloads.
    - Intel Speed Select Technology provides improvements in server utilization and guaranteed per-core performance service levels with more granular control over processor performance.
    - Intel Deep Learning Boost (Vector Neural Network Instruction set [VNNI]) is designed to deliver significant, more efficient Deep Learning (Inference) acceleration for high-performance Artificial Intelligence (AI) workloads.
    - Intel Advanced Vector Extensions 512 (AVX-512) enable acceleration of enterprise-class and high performance computing (HPC) workloads.
- Helps maximize system performance for data intensive applications with up to 2933 MHz memory speeds and up to 768 GB of memory capacity.
- Offers flexible and scalable internal storage in a 1U rack form factor with up to 8x 2.5-inch drives for performance-optimized configurations or up to 4x 3.5-inch drives for capacity-optimized configurations, providing a wide selection of SAS/SATA HDDs/SSDs.
- Provides I/O scalability with a LOM slot and up to three PCI Express (PCIe) 3.0 I/O expansion slots in a 1U rack form factor.
- Reduces I/O latency and increases overall system performance with Intel Integrated I/O Technology that embeds the PCI Express 3.0 controller into the Intel Xeon Processor Scalable Family.

Availability and serviceability

The SR530 server provides many features to simplify serviceability and increase system uptime:

- Offers protection in the event of a non-correctable memory failure with Single Device Data Correction (SDDC, also known as Chipkill, requires x4-based DIMMs), Adaptive Double Device Data Correction (ADDDC, also known as Redundant Bit Steering [RBS], requires x4-based DIMMs and Intel Xeon Gold or Platinum processors), memory mirroring, and memory rank sparing.
- Provides easy access to upgrades and serviceable parts (such as processors, memory DIMMs, and adapter cards) with tool-less cover removal.
- Offers affordable data protection with software RAID and Simple Swap drives and advanced hardware RAID data redundancy with hot-swap drives.
- Provides availability for applications with redundant hot-swap power supplies and redundant non-hot-swap fans.
- Speeds up troubleshooting tasks to reduce service time with diagnostics built into the XClarity Provisioning Manager.

- Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
- Continuously monitors system parameters, triggers alerts, and performs recovery actions in case of failure to minimize downtime with Built-in XClarity Controller (XCC).
- Provides quick access to system status, firmware, network, health, and alerts information via Virtual Operator Panel from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access.

Manageability and security

Powerful systems management features simplify local and remote management of the SR530 server and deliver enterprise-class data protection:

- Provides advanced service processor control, monitoring, and alerting functions with XClarity Controller, a next generation service processor.
- Improves Unified Extensible Firmware Interface (UEFI) system setup, configuration, updates, simplified error handling, and operating system deployment with the embedded XClarity Provisioning Manager.
- Offers XClarity Essentials software tools that can help you set up, use, and maintain the server.
- Increases uptime, reduces costs, and improves productivity through advanced server management capabilities with Lenovo XClarity Administrator that provides comprehensive hardware management.
- Provides on-the-go monitoring and management of devices in XClarity Administrator from anywhere with the Lenovo XClarity mobile app, which can help improve efficiency and reduce downtime risks.
- Centralizes infrastructure resource management with Lenovo XClarity Integrators for VMware vCenter and Microsoft System Center, extending XClarity Administrator features to virtualization management software tools and enabling users to deploy and manage infrastructure end-to-end.
- Offers advanced cryptographic functionality (such as digital signatures and remote attestation) with an integrated Trusted Platform Module (TPM) or optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC).
- Keeps user data safe with Lenovo Business Vantage, a security software tool suite designed to work with the Trusted Cryptographic Module (available only in PRC).
- Offers enterprise-class data protection with advanced RAID and optional self-encrypting drives.
- Provides faster, stronger encryption with industry-standard AES NI support.
- Helps prevent certain classes of malicious buffer overflow attacks with Intel Execute Disable Bit functionality, when combined with a supporting operating system.
- Enhances security through hardware-based resistance to malicious software attacks with Intel Trusted Execution Technology, allowing an application to run in its own isolated space, protected from all other software running on a system.

Energy efficiency

The SR530 server offers the following energy-efficiency features to save energy, reduce operational costs, increase energy availability, and contribute to the green environment:

- Delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies.
- Enables customers to lower energy costs with design to meet ASHRAE A4 standards in select configurations.
- Reduces power drawn with Intel Intelligent Power Capability that powers individual processor elements on and off as needed.
- Helps reduce power consumption with variable speed fans.
- Helps achieve lower heat output and reduced cooling needs with Lenovo XClarity Energy Manager that provides advanced data center power notification, analysis, and policy-based management.

Components and connectors

The following figure shows the front of the SR530 server with four 3.5-inch drive bays.

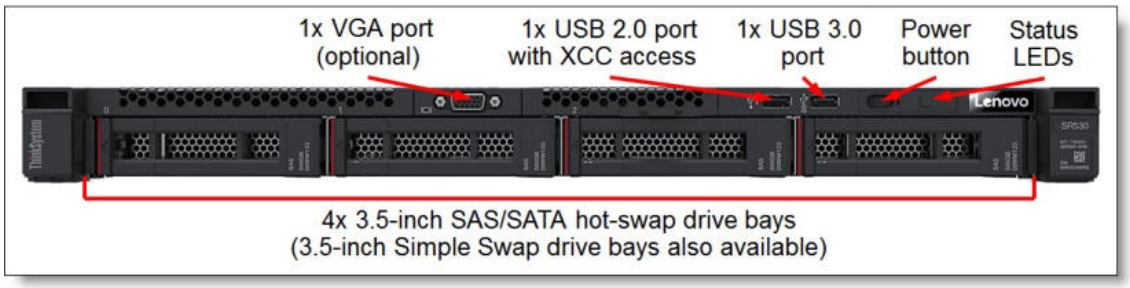


Figure 2. Front view of the SR530: 4x 3.5-inch drive bays

The following figure shows the front of the SR530 server with eight 2.5-inch drive bays.

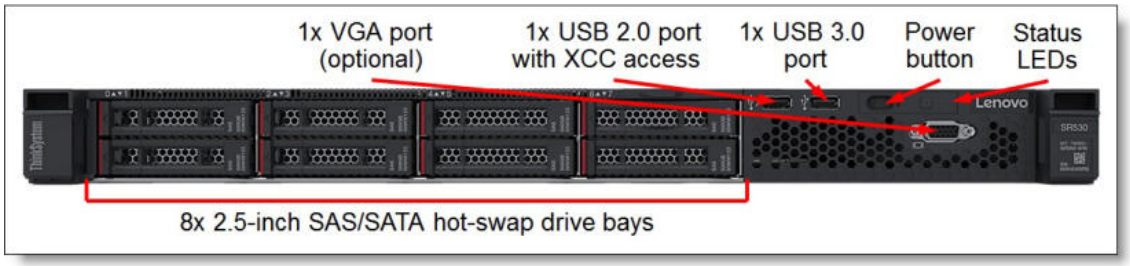


Figure 3. Front view of the SR530: 8x 2.5-inch drive bays

The front of the SR530 server includes the following components:

- Up to 8x 2.5-inch or 4x 3.5-inch hot-swap drive bays, or 4x 3.5-inch Simple Swap drive bays.
- One VGA port (optional).
- One USB 3.0 port.
- One USB 2.0 port with XClarity Controller access.
- Power button.
- Status LEDs.

The following figure shows the rear of the SR530 server with three PCIe low profile slots.

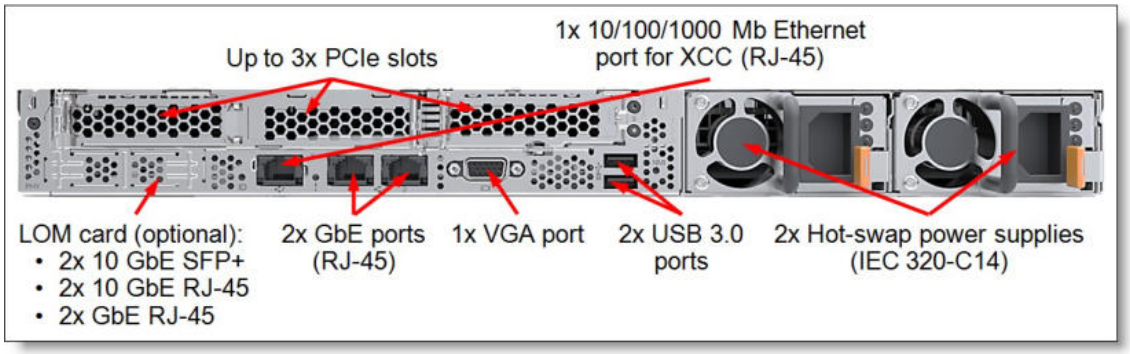


Figure 4. Rear view of the SR530

The rear of the SR530 server includes the following components:

- Up to three PCIe expansion slots (depending on the riser cards selected).
- One LOM card slot.
- One 1 GbE port for XClarity Controller.
- One VGA port.
- Two USB 3.0 ports.
- Up to two hot-swap power supplies.

The following figure shows the locations of key components inside the SR530 server.

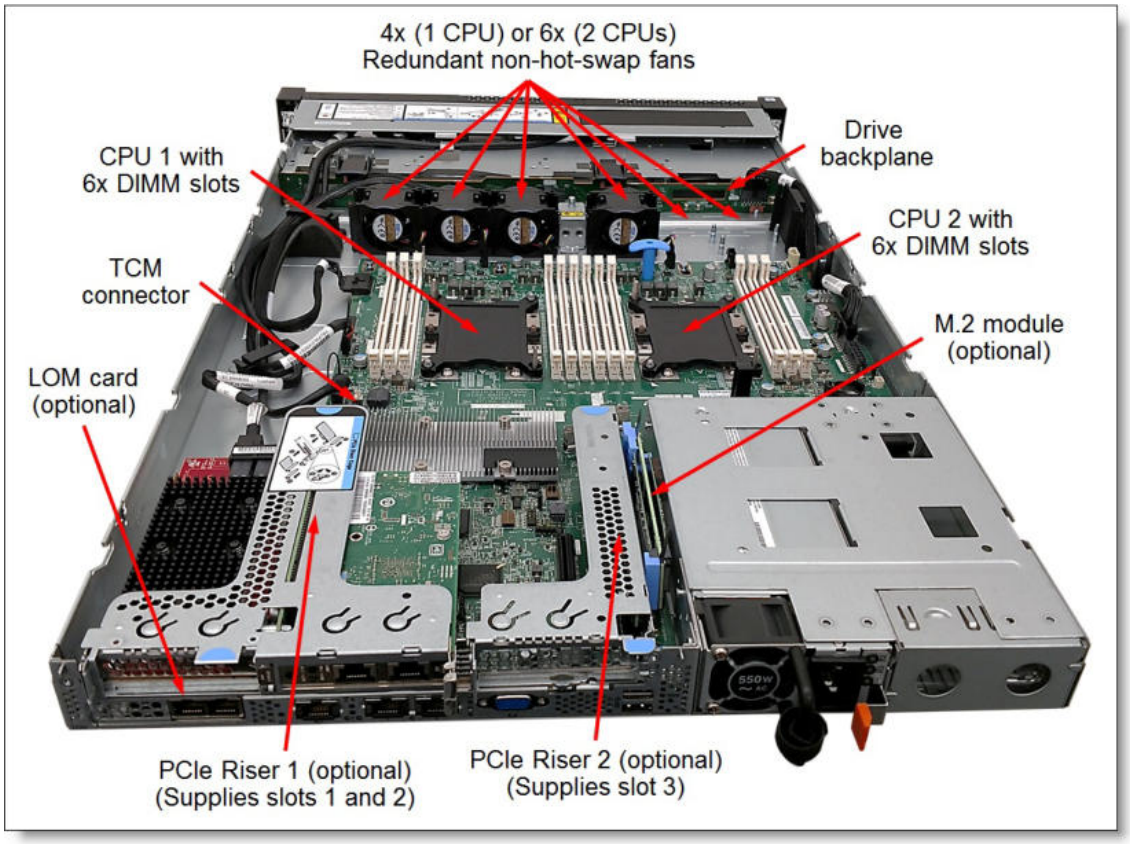


Figure 5. Internal view of the SR530

The following key components are located inside the SR530 server:

- Up to two processors.
- 12 DIMM slots (6 DIMM slots per processor).
- Drive backplanes.
- One M.2 module connector.
- One LOM card connector.
- Two slots for PCIe riser cards.
- One TCM connector.
- Four (one processor) or six (two processors) non-hot-swap system fans.

System specifications

The following table lists the system specifications for the SR530 server.

Table 1. SR530 system specifications

Attribute	Specification
Machine types	7X07 - 1 year warranty 7X08 - 3 year warranty
Form factor	1U rack-mount.
Processor	Up to two Intel Xeon Gen 2 Bronze, Silver, Gold, or Platinum processors: • Up to 22 cores (1.9 GHz core speeds) • Up to 3.8 GHz core speeds (4 cores) • Two UPI links up to 10.4 GT/s each • Up to 30.25 MB cache • Up to 2933 MHz memory speed

Attribute	Specification
Chipset	Intel C622.
Memory	Up to 12 DIMM sockets (6 DIMMs per processor; six memory channels per processor with one DIMM per channel) with support for the following TruDDR4 RDIMM types and capacities: • 8 GB, 16 GB, 32 GB, and 64 GB 2933 MHz. • 16 GB and 32 GB 2666 MHz.
Memory protection	Error correction code (ECC), SDDC (for x4-based memory DIMMs), ADDDC (for x4-based memory DIMMs, requires Intel Xeon Gold or Platinum processors), memory mirroring, memory rank sparing, patrol scrubbing, and demand scrubbing.
Memory capacity	Up to 768 GB with 12x 64 GB RDIMMs (Up to 384 GB per processor).
Drive bays	• 4 LFF SATA Simple Swap drive bays • 4 LFF SAS/SATA hot-swap drive bays • 8 SFF SAS/SATA hot-swap drive bays

Internal storage capacity	• 2.5-inch drives:
	  ◦ 122.88TB using 8x 15.36TB 2.5-inch SAS/SATA SSDs
	  ◦ 19.2TB using 8x 2.4TB 2.5-inch HDDs
	• 3.5-inch drives:
	  ◦ 72TB using 4x 18TB 3.5-inch HDDs
	  ◦ 30.72TB using 4x 7.68TB 3.5-inch SAS/SATA SSDs

Storage controller	6 Gbps SATA
	• Non-RAID: Onboard SATA AHCI
	• RAID 0/1/10/5: Onboard SATA RAID (Intel RSTe)
	
	12 Gbps SAS/6 Gbps SATA RAID
	• RAID 0/1/10/5/50:
	  ◦ RAID 530-8i
	  ◦ RAID 730-8i 1GB Cache
	• RAID 0/1/10/5/50/6/60:
	  ◦ RAID 730-8i 2GB Flash
	  ◦ RAID 930-8i 2GB Flash
	  ◦ RAID 930-16i 4GB or 8GB Flash
	
	12 Gbps SAS/6 Gbps SATA non-RAID: 430-8i HBA

Optical drive bays	None. Support for an external USB DVD RW Optical Disk Drive (SeeOptical drives).

Network interfaces	• 2x Integrated 1 GbE RJ-45 ports (no 10/100 Mb support)
	• Onboard LOM slot for up to two additional 1/10 Gb Ethernet ports:
	  ◦ 2x 1 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE SFP+ ports (no 10/100 Mb support)
	• Optional Mezzanine LOM (ML2) slot for dual-port 10 GbE cards with SFP+ or RJ-45 connectors.
	• 1x RJ-45 10/100/1000 Mb Ethernet systems management port.

I/O expansion slots	Up to three slots depending on the riser cards installed. The slots are as follows: • Slot 1: PCIe 3.0 x8; low profile • Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length • Slot 3: PCIe 3.0 x8 or x16; low profile PCIe x16 slot 3 requires the second processor to be installed.
Ports	• Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. • Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
Cooling	Four (one processor) or six (two processors) non-hot-swap system fans with N+1 redundancy.
Power supply	Up to two redundant hot-swap 550 W or 750 W (100 - 240 V) High Efficiency Platinum or 750 W (200 - 240 V) High Efficiency Titanium AC power supplies. HVDC support (PRC only).

Attribute	Specification
Video	Matrox G200 with 16 MB memory integrated into the XClarity Controller. Maximum resolution is 1920x1200 at 60 Hz with 32 bits per pixel.
Hot-swap parts	Drives (select models) and power supplies.
Systems management	XClarity Controller (XCC) Standard, Advanced, or Enterprise (Pilot 4 chip), proactive platform alerts, XClarity Provisioning Manager, XClarity Essentials, XClarity Administrator, XClarity Integrators for VMware vCenter and Microsoft System Center, XClarity Energy Manager, Capacity Planner.
Security features	Power-on password, administrator's password, secure firmware updates, Trusted Platform Module (TPM) 1.2 or 2.0 (configurable UEFI setting). Optional lockable front bezel. Optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC). Optional Lenovo Business Vantage security software (available only in PRC).
Operating systems	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. See the Operating systems section for specifics.
Warranty	One-year (7X07) or three-year (7X08) customer-replaceable unit (CRU) and onsite limited warranty with 9x5 Next Business Day Parts Delivered.
Service and support	Optional service upgrades are available through Lenovo Services: 2-hour or 4-hour response time, 6-hour or 24-hour committed service repair, warranty extension up to 5 years, 1-year or 2-year post-warranty extensions, YourDrive Your Data, Enterprise Software Support, and Basic Hardware Installation Services.
Dimensions	Width: 435 mm (17.1 in.), height: 43 mm (1.7 in.), depth: 750 mm (29.5 in.). See Physical specifications for details.
Weight	Minimum configuration: 10.2 kg (22.5 lb), maximum: 16 kg (35.3 lb)

Models

ThinkSystem SR530 models can be configured by using the Lenovo Data Center Solution Configurator (DCSC).

Configure-to-order (CTO) models are used to create models with factory-integrated server customizations. For CTO models, two base CTO models are available for the SR530 as listed in the following table, CTO1WW and CTOLWW:

- The CTO1WW base CTO model is for general business and is selectable by choosing **General Purpose** mode in DCSC.
- The CTOLWW base model is intended for High Performance Computing (HPC) and Artificial Intelligence (AI) configurations and solutions, including configurations for Lenovo Scalable Infrastructure (LeSI), and is enabled using either the **HPC & AI LeSI Solutions** mode or **HPC & AI ThinkSystem Hardware** mode in DCSC. CTOLWW configurations can also be built using System x and Cluster Solutions Configurator (x-config).

Preconfigured server models may also be available for the SR530, however these are region-specific; that is, each region may define their own server models, and not all server models are available in every region.

The following table lists the base CTO models of the ThinkSystem SR530 server.

Table 2. Base CTO models

Description	Machine Type/Model General purpose	Machine Type/Model for HPC and AI
ThinkSystem SR530 - 3 year Warranty	7X08CTO1WW	7X08CTOLWW
ThinkSystem SR530 - 1 year Warranty	7X07CTO1WW	7X07CTOLWW

The following table lists the base chassis for CTO models of the SR530 server.

Table 3. Base chassis for CTO models

Feature code	Description
AV0T	ThinkSystem SR530 3.5" Chassis with 4 Bays
AV0S	ThinkSystem SR530 2.5" Chassis with 8 Bays

All models of the SR530 server are shipped with the following items:

- *Rack Installation Guide*
- *Electronic Publications Flyer*

Models table conventions: The model tables shown in this section use the following conventions:

- XClarity Controller: "S" = Standard, "A" = Advanced, "E" = Enterprise.
- Front VGA port: "Y" = Included; "N" = Not included, optional.
- Tool-less Rail Kit: "Y" = Included; "N" = Not included, optional.
- Cable Management Arm (CMA): "Y" = Included; "N" = Not included, optional.
- Power cord:
  - "R1" = 1.5 m C13-C14 rack power cable.
  - "R2" = 2.8 m C13-C14 rack power cable.
  - "L2" = 2.8 m line cord.
  - "N" = Not included; see Power supplies and cables for the ordering information.

The following tables list the models of the SR530 server for the following regions:

- Brazil
- Latin America (except Brazil)
- Europe, Middle East, and Africa (EMEA)
- India
- Hong Kong, Taiwan, Korea
- Japan
- Association of Southeast Asian Nations (ASEAN)
- Australia and New Zealand

Table 4. SR530 server models: Brazil

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Brazil													
7X08A0A1BR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
TopSeller models - Brazil													
7X08100QBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x SATA AHCI	4 / 4 SS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A0A2BR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
7X08A09YBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09ZBR	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0APBR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 5. SR530 server models: Latin America (except Brazil)

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
TopSeller models - Latin America (except Brazil)													
7X08A09WLA	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09XLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0AQLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	Y	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 6. SR530 server models: EMEA

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - EMEA													
7X08A0ACEA	1x 3206R 8C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	R2
7X08A075EA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AZEA	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	None	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	N	R2
7X08A0ADEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AHEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A078EA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A06WEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A07FEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AEEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AJEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A07CEA	1x 4214 12C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AKEA	1x 4214R 12C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A070EA	1x 4216 16C 100W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0ALEA	1x 5218R 20C 125W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 7. SR530 server models: India

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - India													
7X08A08TSG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07USG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A07WSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A084SG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07YSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A079SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06VSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07SSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07JSG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ASG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08PSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A098SG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A077SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A095SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07RSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08VSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08WSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06USG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A094SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A089SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ESG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08KSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 8. SR530 server models: Hong Kong, Taiwan, Korea

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Hong Kong, Taiwan, Korea													
7X08A09CCN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085CN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08100VCN	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	Y	N	Y
7X08A071CN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YCN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09BCN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080CN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CCN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A082CN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09DCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07NCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A088CN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GCN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A087CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08MCN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092CN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06XCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07KCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 9. SR530 server models: Japan

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Japan													
7X08A0AWJP	1x 5218R 20C 125W 2.1GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
TopSeller models - Japan													
7X08A08AJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08DJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08EJP	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07HJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08SJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08QJP	1x 4214 12C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07QJP	1x 4215 8C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07LJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07MJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08HJP	1x 5215 10C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08FJP	1x 5217 8C 115W 3.0GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08YJP	1x 5218 16C 125W 2.3GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A090JP	1x 5220 18C 125W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08UJP	1x 5222 4C 105W 3.8GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A096JP	1x 6230 20C 125W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A0AXJP	1x 3206R 8C 85W 1.9GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AYJP	1x 4210R 10C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AVJP	1x 4214R 12C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 10. SR530 server models: ASEAN

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - ASEAN													
7X08A099SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A086SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A081SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ZSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A083SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A093SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07VSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ESG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RSG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A073SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A097SG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07PSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07TSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09FSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A091SG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 11. SR530 server models: Australia and New Zealand

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Australia and New Zealand (1-year warranty)													
7X07A00VAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	None	No bays / 8 HS SFF	Open bay	Open slot	None	1x 550W	S	Y	Y	N	R2
Relationship models - Australia and New Zealand (3-year warranty)													
7X08A099AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A071AU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YAU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XAU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080AU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A0B0AU	1x 4216 16C 100W 2.1GHz	1x 32GB(x4) 2933MHz	1x RAID 930-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W Platinum	E	Y	Y	N	Y
7X08A07VAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07EAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076AU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BAU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LAU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092AU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A06XAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
TopSeller models - Australia and New Zealand (3-year warranty)													
7X08A09GAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09HAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09LAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09KAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09NAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09MAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09JAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Processors

The SR530 server supports one or two Intel Xeon Bronze, Silver, Gold, or Platinum processors of up to 125 W TDP. The following table lists the specifications of the processors for the SR530 server.

Processor specifications table abbreviations:

- UPI: Ultra Path Interconnect
- TDP: Thermal Design Power
- HT: Hyper-Threading
- TB: Turbo Boost 2.0
- VT-x: Virtualization Technology
- VT-d: Virtualization Technology for Directed I/O
- SST-PP: Speed Select Technology - Performance Profile
- FMA: Fused-Multiply Add (AVX-512)
- RAS: Reliability, Availability, and Serviceability
    - Std: Standard RAS
    - Adv: Advanced RAS

Table 12. Processor specifications

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
Intel Xeon Bronze processors														
3204	6 / 6	1.9 / 1.9 GHz	8.25 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	Std

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
3206R	8 / 8	1.9 / 1.9 GHz	11 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	
Intel Xeon Silver processors														
4208	8 / 16	2.1 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4209T	8 / 16	2.2 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	70 W	Y	Y	Y	Y	N	1	Std
4210	10 / 20	2.2 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4210R	10 / 20	2.4 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4214R	12 / 24	2.4 / 3.5 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214Y	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	Y	1	Std
	10 / 20	2.3 / 3.2 GHz												
	8 / 16	2.4 / 3.2 GHz												
4215	8 / 16	2.5 / 3.5 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4216	16 / 32	2.1 / 3.2 GHz	22 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
Intel Xeon Gold processors														
5215	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	1 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5215L	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	4.5 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5217	8 / 16	3.0 / 3.7 GHz	11 MB	2666 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	1	Adv
5218	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218B	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218R	20 / 40	2.1 / 4.0 GHz	27.5 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218T	16 / 32	2.1 / 3.8 GHz	22 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5220	18 / 36	2.2 / 3.9 GHz	24.75 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220S	18 / 36	2.7 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220T	18 / 36	1.9 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5222	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv
6209U	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	N/A	125 W	Y	Y	Y	Y	N	2	Adv
6222V	20 / 40	1.8 / 3.6 GHz	27.5 MB	2400 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	2	Adv
6226	12 / 24	2.7 / 3.7 GHz	19.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230N	20 / 40	2.3 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230T	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6238T	22 / 44	1.9 / 3.7 GHz	30.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
Intel Xeon Platinum processors														
8253	16 / 32	2.2 / 3.0 GHz	22 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
8256	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv

Configuration notes:

- The Intel Xeon Gold 5218 and 5218B processors have similar specifications; however, they use different silicon designs and cannot be mixed in the same system.
- The processors that support SST-PP offer three distinct operating points that are defined by a core count with a base speed associated with that core count. The operating point is static, it is selected during the boot process and cannot be changed at runtime.

For the SR530 server models that come with one processor, the second processor can be ordered, if required (see the following table for ordering information). The second processor must be of the same model as the first processor. The second processor option includes a processor and a heatsink; two additional system fans are not included and need to be purchased with the second processor (see Cooling for details).

Table 13. Processor options

Description	Part number	Feature code*
Intel Xeon Bronze processors		
SR530/SR570/SR630 Intel Xeon Bronze 3204 6C 85W 1.9GHz Processor w/o FAN	4XG7A37939	B4HU
SR530/SR570/SR630 Intel Xeon Bronze 3206R 8C 85W 1.9GHz Processor w/o FAN	4XG7A37990	B7N3
Intel Xeon Silver processors		
SR530/SR570/SR630 Intel Xeon Silver 4208 8C 85W 2.1GHz Processor w/o FAN	4XG7A37936	B4HT
SR530/SR570/SR630 Intel Xeon Silver 4209T 8C 70W 2.2GHz Processor w/o FAN	4XG7A37945	B4P4
SR530/SR570/SR630 Intel Xeon Silver 4210 10C 85W 2.2GHz Processor w/o FAN	4XG7A37933	B4HS
SR530/SR570/SR630 Intel Xeon Silver 4210R 10C 100W 2.4GHz Processor w/o FAN	4XG7A37988	B7N5
SR530/SR570/SR630 Intel Xeon Silver 4214 12C 85W 2.2GHz Processor w/o FAN	4XG7A37930	B4HR
SR530/SR570/SR630 Intel Xeon Silver 4214R 12C 100W 2.4GHz Processor w/o FAN	4XG7A37987	B7N6
SR530/SR570/SR630 Intel Xeon Silver 4214Y 12/10/8C 85W 2.2GHz Processor w/o FAN	4XG7A37942	B4NW
SR530/SR570/SR630 Intel Xeon Silver 4215 8C 85W 2.5GHz Processor w/o FAN	4XG7A37927	B4HQ
SR530/SR570/SR630 Intel Xeon Silver 4216 16C 100W 2.1GHz Processor w/o FAN	4XG7A37924	B4HP
Intel Xeon Gold processors		
SR530/SR570/SR630 Intel Xeon Gold 5215 10C 85W 2.5GHz Processor w/o FAN	4XG7A37917	B4HN
SR530/SR570/SR630 Intel Xeon Gold 5215L 10C 85W 2.5GHz Processor w/o FAN	4XG7A37911	B4P9
SR530/SR570 Intel Xeon Gold 5217 8C 115W 3.0GHz Processor w/o FAN	4XG7A37921	B4HM
SR530/SR570/SR630 Intel Xeon Gold 5218 16C 125W 2.3GHz Processor w/o FAN	4XG7A37896	B4HL
SR530/SR570/SR630 Intel Xeon Gold 5218B 16C 125W 2.3GHz Processor w/o FAN	4XG7A37959	B6BS
SR530/SR570/SR630 Intel Xeon Gold 5218R 20C 125W 2.1GHz Processor w/o FAN	4XG7A63296	BAZS
SR530/SR570 Intel Xeon Gold 5218T 16C 105W 2.1GHz Processor w/o FAN	4XG7A38017	B4P3
SR530/SR570/SR630 Intel Xeon Gold 5220 18C 125W 2.2GHz Processor w/o FAN	4XG7A37893	B4HK
SR530/SR570/SR630 Intel Xeon Gold 5220S 18C 125W 2.7GHz Processor w/o FAN	4XG7A38018	B6CW
SR530/SR570 Intel Xeon Gold 5220T 18C 105W 1.9GHz Processor w/o FAN	4XG7A38004	B6CQ
SR530/SR570 Intel Xeon Gold 5222 4C 105W 3.8GHz Processor w/o FAN	4XG7A37953	B5S1
Intel Xeon Gold 6209U 20C 125W 2.1GHz Processor	None**	B6CX
SR530/SR570/SR630 Intel Xeon Gold 6222V 20C 115W 1.8GHz Processor w/o FAN	4XG7A38022	B6CV
SR530/SR570/SR630 Intel Xeon Gold 6226 12C 125W 2.7GHz Processor w/o FAN	4XG7A38020	B6CL
SR530/SR570/SR630 Intel Xeon Gold 6230 20C 125W 2.1GHz Processor w/o FAN	4XG7A37890	B4HJ
SR530/SR570 Intel Xeon Gold 6230N 20C 125W 2.3GHz Processor w/o FAN	4XG7A38029	B5RY
SR530/SR570 Intel Xeon Gold 6230T 20C 125W 2.1GHz Processor w/o FAN	4XG7A38007	B6CP
SR530/SR570 Intel Xeon Gold 6238T 22C 125W 1.9GHz Processor w/o FAN	4XG7A37908	B4P2
Intel Xeon Platinum processors		
SR530/SR570/SR630 Intel Xeon Platinum 8253 16C 125W 2.2GHz Processor w/o FAN	4XG7A37899	B5RZ
SR530/SR570 Intel Xeon Platinum 8256 4C 105W 3.8GHz Processor w/o FAN	4XG7A37949	B5S2

* For CTO configurations, the feature code represents a processor, and fans and heatsinks are derived by the configuration tool.
** Factory-installed only; no field upgrade. Supported in the uniprocessor configurations only.

Memory

The SR530 server supports up to 6 TruDDR4 memory RDIMMs when one processor is installed and up to 12 RDIMMs when two processors are installed for a total of up to 768 GB of memory capacity (up to 384 TB per processor). Each processor has six memory channels, and there is a one DIMM per channel.

Lenovo TruDDR4 memory uses the highest-quality components sourced from Tier 1 DRAM suppliers and only memory that meets strict requirements is selected. It is compatibility tested and tuned on every ThinkSystem server to maximize performance and reliability.

TruDDR4 memory has a unique signature programmed into the DIMM, which enables Lenovo servers to verify whether the memory installed is qualified and supported. Lenovo qualified and supported TruDDR4 memory is covered by Lenovo warranty, and service and support provided worldwide.

The following memory protection technologies are supported by the processor's integrated memory controllers:

- ECC
- SDDC (for x4-based memory DIMMs)
- ADDDC (for x4-based memory DIMMs; Gold and Platinum processors only)
- Memory mirroring
- Memory rank sparing
- Patrol scrubbing
- Demand scrubbing

The following table lists memory options available for the SR530 server.

Table 14. Memory options

Description	Part number	Feature code	Maximum quantity*
RDIMMs - 2933 MHz			
ThinkSystem 8GB TruDDR4 2933MHz (1Rx8 1.2V) RDIMM	4ZC7A08706	B4H1	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (1Rx4 1.2V) RDIMM	4ZC7A08707	B4LY	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (2Rx8 1.2V) RDIMM	4ZC7A08708	B4H2	6 / 12
ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08709	B4H3	6 / 12
ThinkSystem 64GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08710	B4H4	6 / 12
RDIMMs - 2666 MHz			
ThinkSystem 16GB TruDDR4 2666 MHz (1Rx4 1.2V) RDIMM	7X77A01302	AUNB	6 / 12
ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM	7X77A01303	AUNC	6 / 12
ThinkSystem 32GB TruDDR4 2666 MHz (2Rx4 1.2V) RDIMM	7X77A01304	AUND	6 / 12

* The maximum quantity shown is with one processor / two processors.

Configuration notes:

- All RDIMMs in the server operate at the same speed, which is determined as the lowest value of:
  - RDIMM rated speed (2666 MHz or 2933 MHz).
  - Memory speed supported by the specific processor (2133 MHz, 2400 MHz, 2666 MHz, or 2933 MHz).

  Note: Maximum memory speed can be achieved when Max performance mode is enabled in UEFI.
- Mixing RDIMMs of different ranks (single- or dual-rank), DRAM chip types (x4 or x8), speeds (2666 MHz or 2933 MHz), and capacities (8 GB, 16 GB, 32 GB, or 64 GB) is supported in the independent channel mode (the default operational mode).
- For server configurations with memory protection, the following rules apply:
  - Single Device Data Correction (SDDC) works only in the independent channel mode and supports only x4-based memory DIMMs.
  - Adaptive Double Device Data Correction (ADDDC) works with x4-based memory DIMMs and requires two DIMM ranks per channel, Intel Xeon Gold or Platinum processors, and the Closed Page memory access mode.
  - If memory mirroring is used, then DIMMs must be installed in quantities of 2 or 4 per processor for mirroring across two memory channels, or in quantities of 3 or 6 per processor for mirroring across three memory channels. Mixing two- and three-channel mirroring in the server is allowed (one processor uses two-channel mirroring, and another processor uses three-channel mirroring). All DIMMs in the server must be identical in type and size.
  - If memory rank sparing is used, then a minimum of two ranks must be installed per populated channel (a least one dual-rank or quad-rank DIMM; single-rank DIMMs are not supported). With rank sparing, one rank in each populated channel is reserved as spare memory for other ranks on the same channel. All DIMMs in the server must be identical in type and size.
  - SDDC, memory mirroring, and memory rank sparing modes are mutually exclusive. Only one operational memory mode can be enabled on the server.

Internal storage

The SR530 server supports the following internal drive bay configurations:

1. 4 LFF SATA Simple Swap drive bays
2. 4 LFF SAS/SATA hot-swap drive bays
3. 8 SFF SAS/SATA hot-swap drive bays

In addition, the SR530 server models can be configured with one or two internal M.2 SATA SSDs. The server also supports configurations without drive bays.

The following figure shows the internal drive bay configurations.

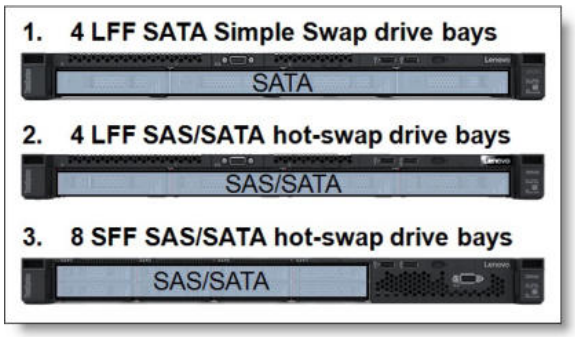


Figure 6. Internal drive bay configurations

The following table lists the internal storage options for the SR530 server.

Table 15. Internal storage options

Description	Part number	Feature code	Maximum quantity
Factory-installed backplane kits			
ThinkSystem 1U 3.5" SATA/SAS 4-Bay Backplane	None*	AUW8	1
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane	None*	AUWB	1
Backplane kit field upgrade options			
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane Kit	7XH7A05896	None**	1
M.2 enablement kits			
ThinkSystem M.2 Enablement Kit	7Y37A01092	AUMU	1
ThinkSystem M.2 with Mirroring Enablement Kit	7Y37A01093	AUMV	1

* These backplane kits can be factory-installed in standard or custom (CTO or Special Bid) models, and they might not have an option part number assigned.
** Field upgrade only; used for upgrading models without any drive bays to 8x 2.5" SAS/SATA hot-swap drive bays.

M.2 Enablement Kit configuration notes:

- The M.2 Enablement Kit (7Y37A01092) supports one M.2 SATA SSD which is connected to the SATA port on the Intel Platform Controller Hub (PCH).
- The M.2 with Mirroring Enablement Kit (7Y37A01093) is connected to the Intel PCH via the PCIe link, and the kit supports two M.2 SATA SSDs that can be configured in a RAID-1 or RAID-0 drive group, or they can operate as two separate drives.

The following tables list supported internal storage configurations with the SAS/SATA backplanes.

Table 16. Internal storage configurations

Drive bay configuration	Backplane kit type and quantity		Storage controller type and quantity*
	4x 3.5" SATA/SAS	8x 2.5" SATA/SAS	
4x 3.5" chassis (Feature code AV0T)			
4x 3.5-in. SATA Simple Swap	0	0	Onboard AHCI (non-RAID) / Intel RSTe (RAID) (4)
4x 3.5-in. SAS/SATA hot-swap	1	0	1x RAID 530-8i/730-8i 1GB (4)
			1x RAID 730-8i 2GB/930-8i (4)
			1x 430-8i HBA (4)
8x 2.5" chassis (Feature code AV0S)			
8x 2.5-in. SAS/SATA hot-swap	0	1	1x RAID 530-8i/730-8i 1GB (8)
			1x RAID 730-8i 2GB/930-8i/930-16i (8)
			1x 430-8i HBA (8)

* The number in brackets (x) specifies the quantity of drive bays connected to each of the controllers.

Configuration note: Models without any drive bays are based on the 8x 2.5" chassis (feature code AV0S), and they support adding drive bays by using the 2.5" 8-drive backplane kit (7XH7A05896).

Controllers for internal storage

The following table lists the storage controllers and options for internal storage of the SR530 server.

Table 17. RAID controllers and HBAs for internal storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
6 Gbps SATA controllers				
Onboard AHCI (non-RAID) / Intel RSTe (RAID)	Onboard*	Onboard*	1	-
12 Gb SAS/SATA RAID controllers				
ThinkSystem RAID 530-8i PCIe 12Gb Adapter	7Y37A01082	AUNG	1	1
ThinkSystem RAID 730-8i 1GB Cache PCIe 12Gb Adapter	7Y37A01083	AUNH	1	1
ThinkSystem RAID 730-8i 2GB Flash PCIe 12Gb Adapter	4Y37A09722	B4RQ	1	1
ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter	7Y37A01084	AUNJ	1	1
ThinkSystem RAID 930-16i 4GB Flash PCIe 12Gb Adapter	7Y37A01085	AUNK	1	1
ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter	4Y37A09721	B31E	1	1
12 Gb SAS/SATA non-RAID HBAs				
ThinkSystem 430-8i SAS/SATA 12Gb HBA	7Y37A01088	AUNL	1	1

* The onboard SATA controller integrated into the Intel C622 Platform Controller Hub (PCH) supports non-RAID (JBOD) AHCI mode or a hardware-assist, software RAID feature (Intel Rapid Storage Technology Enterprise [RSTe]).

Configuration note: Low profile SAS RAID controllers and HBAs for internal storage are supported in the PCIe x8 slot 1 supplied by the riser card 1.

The following table summarizes features of supported SAS/SATA storage controllers.

Table 18. Storage controller features and specifications (LP = Low profile, FHHL = Full-height half-length)

Feature	Intel RSTe	RAID 530-8i	RAID 730-8i 1GB	RAID 730-8i 2GB	RAID 930-8i	RAID 930-16i	430-8i HBA
Form factor	Onboard	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP
SAS controller	None	SAS3408	SAS3108	SAS3108	SAS3508	SAS3516	SAS3408
Host interface	PCH	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	6 Gb SATA	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	8	8	8	16	8
Connector type	SATA x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4
Number of connectors	2	2	2	2	2	4	2
Drive interface	SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD	HDD, SSD, SED	HDD, SSD	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED*
Hot-swap drive support	No	Yes	Yes	Yes	Yes	Yes	Yes
Number of drives	8	8	8	8	8	16^	8
RAID levels	0/1/10/5	0/1/10/5/50	0/1/10/5/50	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	None
JBOD mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cache	None	None	1 GB	2 GB	2 GB	4 GB; 8 GB	None
Cache protection	None	None	None	Flash backup (Included)	Flash backup (Included)	Flash backup (Included)	None
SED key management (SafeStore)	No	Yes	No	Yes	Yes	Yes	No
SSD I/O acceleration (FastPath)	No	Yes	No	Yes	Yes	Yes	No
SSD Caching (CacheCade Pro 2.0)	No	No	No	No	No**	No**	No
Consistency check	Yes	Yes	Yes	Yes	Yes	Yes	No
Patrol read	Yes	Yes	Yes	Yes	Yes	Yes	No
Online capacity expansion	Yes	Yes	Yes	Yes	Yes	Yes	No
Online RAID level migration	Yes	Yes	Yes	Yes	Yes	Yes	No
Global Hot Spare	Yes	Yes	Yes	Yes	Yes	Yes	No
Auto-rebuild	Yes	Yes	Yes	Yes	Yes	Yes	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
^ Up to 8 drives is supported by the RAID 930-16i in the SR530 server.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

Important: The onboard Intel RSTe is not supported by virtualization hypervisors, including VMware vSphere (ESXi), Linux KVM, Xen, and Microsoft Hyper-V.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Drives for internal storage

The following tables list the hard disk drive and solid-state drive options for the internal disk storage of the server.

2.5-inch hot-swap drives:

- 2.5-inch hot-swap 12 Gb SAS HDDs
- 2.5-inch hot-swap 6 Gb SATA HDDs
- 2.5-inch hot-swap 12 Gb SAS SSDs
- 2.5-inch hot-swap 6 Gb SATA SSDs

3.5-inch hot-swap drives:

- 3.5-inch hot-swap 12 Gb SAS HDDs
- 3.5-inch hot-swap 6 Gb SATA HDDs
- 3.5-inch hot-swap 12 Gb SAS SSDs
- 3.5-inch hot-swap 6 Gb SATA SSDs

Simple-swap drives:

- 3.5-inch simple-swap 6 Gb SATA HDDs

M.2 drives:

- M.2 SATA drives

M.2 drive support: The use of M.2 drives requires an additional adapter as described in the Internal storage section.

Table 19. 2.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00024	AULY	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00025	AULZ	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00026	AUM0	ThinkSystem 2.5" 900GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00027	AUM1	ThinkSystem 2.5" 1.2TB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00028	AUM2	ThinkSystem 2.5" 1.8TB 10K SAS 12Gb Hot Swap 512e HDD	8
7XB7A00069	B0YS	ThinkSystem 2.5" 2.4TB 10K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00021	AULV	ThinkSystem 2.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00022	AULW	ThinkSystem 2.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00023	AULX	ThinkSystem 2.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00034	AUM6	ThinkSystem 2.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00035	AUM7	ThinkSystem 2.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
2.5-inch hot-swap SED HDDs - 12 Gb SAS 10K			
7XB7A00030	AUM4	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD SED	8
7XB7A00031	AUM5	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD SED	8

Table 20. 2.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00036	AUUE	ThinkSystem 2.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	8
7XB7A00037	AUUJ	ThinkSystem 2.5" 2TB 7.2K SATA 6Gb Hot Swap 512e HDD	8

Table 21. 2.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17062	B8HU	ThinkSystem 2.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17063	B8J4	ThinkSystem 2.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17064	B8JD	ThinkSystem 2.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17065	B8JA	ThinkSystem 2.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13654	B4A1	ThinkSystem 2.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13655	B4A2	ThinkSystem 2.5" PM1645 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A38175	B91A	ThinkSystem 2.5" PM1643a 960GB Entry SAS 12Gb Hot Swap SSD	8
4XB7A38176	B91B	ThinkSystem 2.5" PM1643a 1.92TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17054	B91C	ThinkSystem 2.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17055	B91D	ThinkSystem 2.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17056	BC4R	ThinkSystem 2.5" PM1643a 15.36TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A13645	B4A7	ThinkSystem 2.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	8

Table 22. 2.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17087	B8J1	ThinkSystem 2.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17088	B8HY	ThinkSystem 2.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17089	B8J6	ThinkSystem 2.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17090	B8JE	ThinkSystem 2.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17091	B8J7	ThinkSystem 2.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13633	B49L	ThinkSystem 2.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13634	B49M	ThinkSystem 2.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13635	B49N	ThinkSystem 2.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13636	B49P	ThinkSystem 2.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13637	B49Q	ThinkSystem 2.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10237	B488	ThinkSystem 2.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10239	B48A	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10240	B48B	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10241	B48C	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			

Part number	Feature	Description	Maximum supported
4XB7A38271	BCTC	ThinkSystem 2.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38272	BCTD	ThinkSystem 2.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38273	BCTE	ThinkSystem 2.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38274	BCTF	ThinkSystem 2.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38275	BCTG	ThinkSystem 2.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17075	B8HV	ThinkSystem 2.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17076	B8JM	ThinkSystem 2.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17077	B8HP	ThinkSystem 2.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17078	B8J5	ThinkSystem 2.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17079	B8JP	ThinkSystem 2.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17080	B8J2	ThinkSystem 2.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38185	B9AC	ThinkSystem 2.5" 5210 960GB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38144	B7EW	ThinkSystem 2.5" 5210 1.92TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38145	B7EX	ThinkSystem 2.5" 5210 3.84TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38146	B7EY	ThinkSystem 2.5" 5210 7.68TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A10247	B498	ThinkSystem 2.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10248	B499	ThinkSystem 2.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10249	B49A	ThinkSystem 2.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13622	B49B	ThinkSystem 2.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13623	B49C	ThinkSystem 2.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10195	B34H	ThinkSystem 2.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10196	B34J	ThinkSystem 2.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10197	B34K	ThinkSystem 2.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10198	B34L	ThinkSystem 2.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10199	B34M	ThinkSystem 2.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10200	B4D2	ThinkSystem 2.5" PM883 7.68TB Entry SATA 6Gb Hot Swap SSD	8
7SD7A05740	B0Z0	ThinkSystem 2.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10155	B2X4	ThinkSystem 2.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10157	B2X6	ThinkSystem 2.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	8

Table 23. 3.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00063	B1JJ	ThinkSystem 3.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	4
3.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00038	AUU2	ThinkSystem 3.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00039	AUU3	ThinkSystem 3.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00040	AUUC	ThinkSystem 3.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00041	AUU4	ThinkSystem 3.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00042	AUU5	ThinkSystem 3.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00043	AUU6	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00044	AUU7	ThinkSystem 3.5" 6TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00045	B0YR	ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00046	AUUG	ThinkSystem 3.5" 10TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00067	B117	ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13906	B496	ThinkSystem 3.5" 14TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13911	B7EZ	ThinkSystem 3.5" 16TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A38266	BCFP	ThinkSystem 3.5" 18TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap SED HDDs - 12 Gb NL SAS			
7XB7A00047	AUUH	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD FIPS	4

Table 24. 3.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00049	AUUF	ThinkSystem 3.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00050	AUUD	ThinkSystem 3.5" 2TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00051	AUU8	ThinkSystem 3.5" 4TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00052	AUUA	ThinkSystem 3.5" 6TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00053	AUU9	ThinkSystem 3.5" 8TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00054	AUUB	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00068	B118	ThinkSystem 3.5" 12TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13907	B497	ThinkSystem 3.5" 14TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13914	B7F0	ThinkSystem 3.5" 16TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A38130	BCFH	ThinkSystem 3.5" 18TB 7.2K SATA 6Gb Hot Swap 512e HDD	4

Table 25. 3.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17066	B8HT	ThinkSystem 3.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17043	B8JN	ThinkSystem 3.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17067	B8JK	ThinkSystem 3.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17068	B8JG	ThinkSystem 3.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A13658	B4A4	ThinkSystem 3.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A17058	B91E	ThinkSystem 3.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A17059	BEVK	ThinkSystem 3.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A13649	B4A8	ThinkSystem 3.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	4

Table 26. 3.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17096	B8JL	ThinkSystem 3.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17097	B8JF	ThinkSystem 3.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17098	B8J0	ThinkSystem 3.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17099	B8HR	ThinkSystem 3.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17100	B8HX	ThinkSystem 3.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13639	B49R	ThinkSystem 3.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13640	B49S	ThinkSystem 3.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13641	B49T	ThinkSystem 3.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13642	B49U	ThinkSystem 3.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13643	B49V	ThinkSystem 3.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10242	B48D	ThinkSystem 3.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10244	B48F	ThinkSystem 3.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10245	B48G	ThinkSystem 3.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10246	B48H	ThinkSystem 3.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			
4XB7A38276	BCTH	ThinkSystem 3.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38277	BCTJ	ThinkSystem 3.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38278	BCTK	ThinkSystem 3.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38279	BCTL	ThinkSystem 3.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38281	BCTM	ThinkSystem 3.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17081	B8JB	ThinkSystem 3.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17082	B8J9	ThinkSystem 3.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17083	B8JC	ThinkSystem 3.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17084	B8HZ	ThinkSystem 3.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17085	B8HQ	ThinkSystem 3.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17086	B8J3	ThinkSystem 3.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Part number	Feature	Description	Maximum supported
4XB7A13625	B49D	ThinkSystem 3.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13626	B49E	ThinkSystem 3.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13627	B49F	ThinkSystem 3.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13628	B49G	ThinkSystem 3.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13629	B49H	ThinkSystem 3.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17176	B6TM	ThinkSystem 3.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17177	B6TN	ThinkSystem 3.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17178	B6TP	ThinkSystem 3.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17179	B6JY	ThinkSystem 3.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17180	B6JZ	ThinkSystem 3.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	4
7SD7A05735	B0Z5	ThinkSystem 3.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10160	B2X9	ThinkSystem 3.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10162	B2XB	ThinkSystem 3.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Table 27. 3.5-inch simple-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch simple-swap HDDs - 6 Gb NL SATA			
7XB7A00055	AUZS	ThinkSystem 1TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00056	AUZT	ThinkSystem 2TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00057	AUZU	ThinkSystem 4TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00058	AXC7	ThinkSystem 6TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00059	AXC6	ThinkSystem 8TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00060	AXC8	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Simple Swap 512e HDD	4

Table 29. M.2 SATA drives

Part number	Feature	Description	Maximum supported
M.2 SSDs - 6 Gb SATA - Entry (<3 DWPD)			
7N47A00129	AUUL	ThinkSystem M.2 32GB SATA 6Gbps Non-Hot Swap SSD	2
7N47A00130	AUUV	ThinkSystem M.2 128GB SATA 6Gbps Non-Hot Swap SSD	2
7SD7A05703	B11V	ThinkSystem M.2 5100 480GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17071	B8HS	ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17073	B919	ThinkSystem M.2 5300 480GB SATA 6Gbps Non-Hot Swap SSD	2

Optical drives

The server supports the external USB optical drive listed in the following table.

Table 30. External optical drive

Part number	Feature code	Description
7XA7A05926	AVV8	ThinkSystem External USB DVD RW Optical Disk Drive

The drive is based on the Lenovo Slim DVD Burner DB65 drive and supports the following formats: DVD-RAM, DVD-RW, DVD+RW, DVD+R, DVD-R, DVD-ROM, CD-RW, CD-R, CD-ROM.

I/O expansion

The SR530 server supports one LOM card slot and up to three PCIe slots with different riser cards installed into two riser sockets on the system planar (one riser socket supports installation of one riser card).

The slot form factors are as follows:

- LOM card slot
- Slot 1: PCIe 3.0 x8; low profile
- Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length
- Slot 3: PCIe 3.0 x8 or x16; low profile

Configuration notes:

- PCIe x16 slot 3 requires the second processor to be installed.
- The COM Port Upgrade Kit is installed in place of one of the PCIe slots 1, 2, or 3.

The locations of the PCIe slots are shown in the following figure.

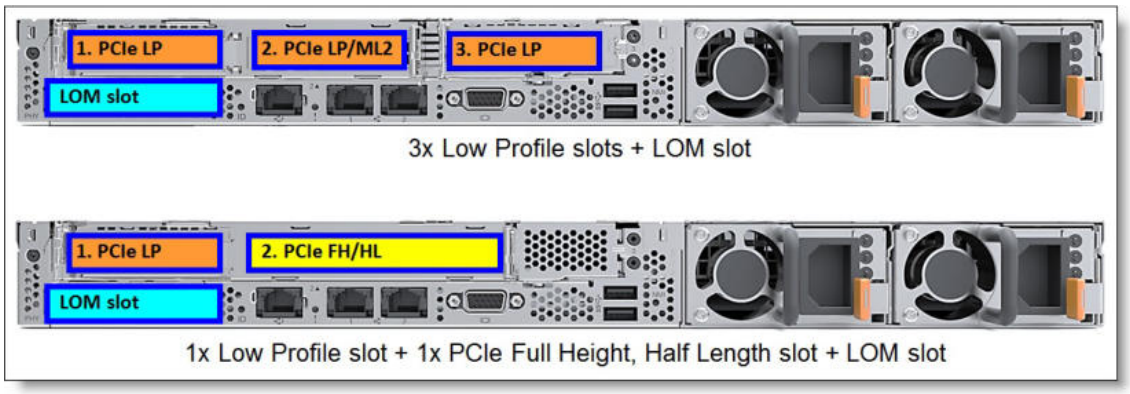


Figure 7. Slot locations

Riser 1 supplies slots 1 and 2, and Riser 2 supplies slot 3. The slots that are available for use depend on the number of riser cards that are installed and whether the second processor is installed, as shown in the following table.

Table 31. Slots available for use

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
None	None	LOM	-
None	PCIe x8	LOM, 3	-
None	PCIe x16	LOM	3
PCIe x8/x16 or PCIe x8/x8ML2	None	LOM, 1, 2	-
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x8	LOM, 1, 2, 3	-

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x16	LOM, 1, 2	3

The following table lists available PCIe riser card options.

Table 32. PCIe riser cards and miscellaneous options

Description	Part number	Feature code	Maximum quantity
x8 Riser Card 1 options (Riser card 1 supplies slots 1 and 2)			
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+LP Riser 1 Kit	7XH7A02682	AUWC	1
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+FH Riser 1 Kit	7XH7A05893	None*	1
ThinkSystem SR530/SR570 x8/x8ML2 PCIe LP+LP Riser 1 Kit	7XH7A05892	AV0X	1
Riser Card 2 option (Riser card 2 supplies slot 3)			
ThinkSystem SR530/SR570/SR630 x16 PCIe LP Riser 2 Kit	7XH7A02685	AUWA	1
ThinkSystem SR530/SR570 x8 PCIe LP Riser 2 Kit	7XH7A05891	AV0W	1
Serial port upgrade kit			
ThinkSystem COM Port Upgrade Kit	7Z17A02577	AUSL	1

* The LP+FH Riser 1 can be factory-installed by selecting the feature codes AUWC (LP+LP Riser 1) and AUWS (LP+FH Bracket).

The COM Port Upgrade Kit, part number 7Z17A02577, is used for mounting the external serial port on the rear of the SR530. This option includes the bracket and the cable. The COM Port option is mounted in place of one of the PCIe slots 1, 2, or 3.

Network adapters

The SR530 server has two onboard 1 GbE ports (no 10/100 Mb support) and up to two additional onboard 1/10 GbE network ports (no 10/100 Mb support) with optional LOM cards. Onboard ports and LOM cards use the Intel Ethernet Connection X722 1/10 GbE technology integrated into the Intel C622 Platform Controller Hub (PCH). The server also supports ML2 adapters that are installed in the custom ML2 slot provided by an ML2 riser card. The LOM cards support direct connectivity to the XClarity Controller via the Network Controller Sideband Interface (NSCI) for out-of-band systems management.

Note: ML2 network adapters do not support NSCI when used in the SR530 server.

The integrated Intel Ethernet Connection X722 has the following features:

- Two 1 Gb Ethernet ports (no 10/100 Mb Ethernet support)
- Two 1/10 Gb Ethernet capable ports (no 10/100 Mb Ethernet support)
- NIC Teaming (load balancing and failover)
- Data Center Bridging
- iWARP (RDMA over IP)
- VMDq and SR-IOV virtualization (10 Gb speeds only, 4 PFs, 128 VFs per device)
- IEEE 802.1q Virtual Local Area Networks (VLANs)
- NVGRE, VXLAN, IPinGRE, and MACinUDP network virtualization
- IEEE 802.1Qbg Edge Virtual Bridging
- TCP, IP, and UDP checksum offload
- Large Send Offload (LSO) and Generic Send Offload (GSO)
- Receive Side Scaling (RSS) for TCP and UDP traffic
- Jumbo frames up to 9.5 Kbytes

The following table lists the network adapters that are supported with the SR530 server.

Table 33. Network adapters

Description	Part number	Feature code	Max qty	I/O slots supported
LOM cards - 1 Gb Ethernet				
ThinkSystem 1Gb 2-port RJ45 LOM	7ZT7A00544	AUKG	1	LOM slot
LOM cards - 10 Gb Ethernet				
ThinkSystem 10Gb 2-port Base-T LOM	7ZT7A00548	AUKL	1	LOM slot
ThinkSystem 10Gb 2-port SFP+ LOM	7ZT7A00546	AUKJ	1*	LOM slot
ML2 adapters - 10 Gb Ethernet				
Broadcom NX-E ML2 10Gb 2-Port Base-T Ethernet Adapter	7ZT7A00497	AUKQ	1	2 (ML2)
Emulex VFA5.2 ML2 Dual Port 10GbE SFP+ Adapter	00AG560	AT7U	1*	2 (ML2)
Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	01CV770	AU7Z	1*	2 (ML2)
Intel X710-DA2 ML2 2x10GbE SFP+ Adapter	00JY940	ATRH	1*	2 (ML2)
PCIe Low Profile adapters - 1 Gb Ethernet				
Broadcom 5720 1GbE RJ45 2-Port PCIe Ethernet Adapter	7ZT7A00482	AUZX	3	1, 2, 3
Broadcom 5719 1GbE RJ45 4-Port PCIe Ethernet Adapter	7ZT7A00484	AUZV	3	1, 2, 3
ThinkSystem I350-F1 PCIe 1Gb 1-Port SFP Ethernet Adapter	7ZT7A00533	AUZZ	3	1, 2, 3
ThinkSystem I350-T2 PCIe 1Gb 2-Port RJ45 Ethernet Adapter	7ZT7A00534	AUZY	3	1, 2, 3
ThinkSystem I350-T4 PCIe 1Gb 4-Port RJ45 Ethernet Adapter	7ZT7A00535	AUZW	3	1, 2, 3
PCIe Low Profile adapters - 10 Gb Ethernet				
Broadcom 57416 10GBASE-T 2-Port PCIe Ethernet Adapter	7ZT7A00496	AUKP	3	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ PCIe Adapter	00AG570	AT7S	3*	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	00AG580	AT7T	3*	1, 2, 3
Intel X550-T2 Dual Port 10GBase-T Adapter	00MM860	ATPX	3	1, 2, 3
Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter	7ZT7A00537	AUKX	3*	1, 2, 3
QLogic QL41134 PCIe 10Gb 4-Port Base-T Ethernet Adapter	4XC7A08225	B31G	3	1, 2, 3
PCIe Full Height adapters - 10 Gb Ethernet				
Emulex OCe14104B-NX PCIe 10Gb 4-Port SFP+ Ethernet Adapter	7ZT7A00493	AUKN	1*	2
PCIe Low Profile adapters - 25 Gb Ethernet				
Broadcom 57412 10/25GbE SFP28 1-Port PCIe Ethernet Adapter	7ZT7A00505	AUKS	3*	1, 2, 3
Broadcom 57414 10/25GbE SFP28 2-port PCIe Ethernet Adapter	4XC7A08238	B5T0	3*	1, 2, 3
PCIe Low Profile adapters - Omni-Path				
Intel OPA 100 Series Single-port PCIe 3.0 x16 HFA	00WE027	AU0B	1 / 2#*	2, 3

The maximum quantity shown is with one processor / two processors.
* The adapter comes without transceivers or cables; for ordering transceivers or cables, see the adapter product guide

Configuration notes:

- ML2 network adapters are supported in the ML2 x8 slot 2 supplied by the x8/x8ML2 Riser Card 1 (7XH7A05892).
- PCIe full-height network adapters are supported in the full-height PCIe x16 slot 2 supplied by the PCIe x8/x16 LP+FH Riser Card 1 (7XH7A05893).
- Omni-Path adapters are supported in the low profile or full-height PCIe x16 slots supplied by the riser cards 1 and 2.
- PCIe Low Profile network adapters (except Omni-Path adapters) are supported in the low profile and full-height PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

- Some adapters require supported transceivers or DAC cables to be purchased for the adapter. The maximum number of transceivers or cables that are supported per adapter equals the quantity of the adapter ports, and all adapter ports must have the same type of the transceiver or cable selected.

For more information, see the list of Product Guides in the Ethernet Adapters category:
http://lenovopress.com/servers/options/ethernet#rt=product-guide

SAS adapters for external storage

The following table lists SAS RAID controllers and HBAs for external storage attachments that are supported by the SR530 server.

Table 34. SAS RAID adapters and HBAs for external storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
12 Gbps SAS RAID adapters				
ThinkSystem RAID 930-8e 4GB Flash PCIe 12Gb Adapter	7Y37A01087	AUNQ	2	1, 2, 3
12 Gbps SAS HBAs				
ThinkSystem 430-8e SAS/SATA 12Gb HBA	7Y37A01090	AUNR	2	1, 2, 3
ThinkSystem 430-16e SAS/SATA 12Gb HBA	7Y37A01091	AUNN	2	1, 2, 3

Configuration notes:

- Low profile SAS RAID controllers and HBAs for external storage are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.
- The total quantity of the RAID 730-8i 2GB, RAID 930-8i, RAID 930-16i, and RAID 930-8e controllers in a supported combination in the server must not exceed 2 (up to 2 supercapacitors can be mounted in the server).

The following table summarizes features of supported RAID controllers and HBAs for external storage.

Table 35. Features and specifications of the RAID controllers and HBAs for external storage

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
Form factor	PCIe LP	PCIe LP	PCIe LP
SAS controller chip	SAS3516	SAS3408	SAS3416
Host interface	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	16
Connector type	SFF-8644 x4	SFF-8644 x4	SFF-8644 x4
Number of connectors	2	2	4
Drive interface	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD, SSD, SED	HDD, SSD, SED*	HDD, SSD, SED*
Hot-swap drive support	Yes	Yes	Yes
Number of devices	240	1024	1024
RAID levels	0/1/10/5/50/6/60	None	None
JBOD mode	Yes	Yes	Yes
Cache	4 GB	None	None
Cache protection	Flash backup (Included)	None	None
SED key management (SafeStore)	Yes	No	No
SSD I/O acceleration (FastPath)	Yes	No	No

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
SSD Caching (CacheCade Pro 2.0)	No**	No	No
Consistency check	Yes	No	No
Patrol read	Yes	No	No
Online capacity expansion	Yes	No	No
Online RAID level migration	Yes	No	No
Global Hot Spare	Yes	No	No
Auto-rebuild	Yes	No	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Fibre Channel host bus adapters

The following table lists Fibre Channel HBAs supported by the SR530 server.

Table 36. Fibre Channel HBAs

Description	Part number	Feature code	Maximum quantity	I/O slots supported
16 Gb Fibre Channel - PCIe				
Emulex 16Gb Gen6 FC Single-port HBA	01CV830	ATZU	3	1, 2, 3
Emulex 16Gb Gen6 FC Dual-port HBA	01CV840	ATZV	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Single-port HBA	01CV750	ATZB	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Dual-port HBA	01CV760	ATZC	3	1, 2, 3
8 Gb Fibre Channel - PCIe (available only in PRC and Asia Pacific)				
Emulex LPe12002-M8-L PCIe 8Gb 2-Port SFP+ FC HBA	4XC7A08221	B0X0	3	1, 2, 3
Emulex LPe12000-M8-L PCIe 8Gb 1-Port SFP+ FC HBA	4XC7A08220	B0WZ	3	1, 2, 3

Configuration note: FC HBAs are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

For more information, see the list of Product Guides in the Host bus adapters category:
http://lenovopress.com/servers/options/hba#rt=product-guide

Cooling

The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.

The following table shows additional cooling options.

Table 37. Cooling options

Description	Part number	Feature code	Maximum quantity
ThinkSystem SR530 FAN Option Kit	4F17A12354	AV0N	1

Configuration note: The SR530 FAN Option Kit (4F17A12354) includes two system fans that are required for field upgrades that add a second processor to the server. If two processors are selected in the initial server configurations, two fans for the second processor are derived by the configurator.

Power supplies and cables

The SR530 server supports up to two redundant power supplies and is capable of N+N redundancy depending on the configuration. A second power supply can be added to the models that come with one power supply. The following table lists the power supply options.

Table 38. Power supplies

Description	Part number	Feature code	Maximum quantity
ThinkSystem 550W (230V/115V) Platinum Hot-Swap Power Supply	7N67A00882	AVV6	2
ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply	7N67A00883	AVV7	2
ThinkSystem 750W (230V) Titanium Hot-Swap Power Supply	7N67A00884	AVV5	2

Configuration notes:

- Minimum of 1 and maximum of 2 power supplies per system.
- If 2 are installed, power supplies must be identical.
- Power supplies support AC (Worldwide) and HVDC (PRC only) power sources.

Important: The Standalone Solution Configuration Tool (SSCT) and Lenovo Data Center Solution Configurator (DCSC) power supply selection rules allow a subset of possible configurations due to power restrictions. Configurations that cannot be built in SSCT or DCSC due to power restrictions may still be supported. To verify support and ensure that the right power supply is chosen for optimal performance, you should always validate your server configuration using the latest version of the Lenovo Capacity Planner: http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

The SR530 server ship standard with or without a power cord (model dependent). A hot-swap power supply option ships without a power cord. The following table lists the rack power cables and line cords that can be ordered for the SR530 server.

Table 39. Power cables

Description	Part number	Feature code
Rack power cables		
1.0m, 10A/125-250V, C13 to IEC 320-C14 Rack Power Cable	00Y3043	A4VP
1.5m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7937	6201
2.0m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08369	6570
2.8m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08366	6311

Description	Part number	Feature code
2.8m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08370	6400
2.8m, 10A/100-250V, C13 to IEC 320-C20 Rack Power Cable	39Y7938	6204
4.3m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7932	6263
4.3m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08371	6583
Line cords		
Argentina 2.8m, 10A/250V, C13 to IRAM 2073 Line Cord	39Y7930	6222
Argentina 4.3m, 10A/250V, C13 to IRAM 2073 Line Cord	81Y2384	6492
Australia/New Zealand 2.8m, 10A/250V, C13 to AS/NZS 3112 Line Cord	39Y7924	6211
Australia/New Zealand 4.3m, 10A/250V, C13 to AS/NZS 3112 Line Cord	81Y2383	6574
Brazil 2.8m, 10A/250V, C13 to NBR 14136 Line Cord	69Y1988	6532
Brazil 4.3m, 10A/250V, C13 to NBR14136 Line Cord	81Y2387	6404
China 1.8m, 10A/250V, C13 to GB 2099.1 Line Cord	4L67A69954	6361
China 2.8m, 10A/250V, C13 to GB 2099.1 Line Cord	39Y7928	6210
China 4.3m, 10A/250V, C13 to GB 2099.1 Line Cord	81Y2378	6580
Denmark 2.8m, 10A/250V, C13 to DK2-5a Line Cord	39Y7918	6213
Denmark 4.3m, 10A/250V, C13 to DK2-5a Line Cord	81Y2382	6575
Europe 2.8m, 10A/250V, C13 to CEE7-VII Line Cord	39Y7917	6212
Europe 4.3m, 10A/250V, C13 to CEE7-VII Line Cord	81Y2376	6572
India 2.8m, 10A/250V, C13 to IS 6538 Line Cord	39Y7927	6269
India 4.3m, 10A/250V, C13 to IS 6538 Line Cord	81Y2386	6567
Israel 2.8m, 10A/250V, C13 to SI 32 Line Cord	39Y7920	6218
Israel 4.3m, 10A/250V, C13 to SI 32 Line Cord	81Y2381	6579
Italy 2.8m, 10A/250V, C13 to CEI 23-16 Line Cord	39Y7921	6217
Italy 4.3m, 10A/250V, C13 to CEI 23-16 Line Cord	81Y2380	6493
Japan 2.8m, 12A/125V, C13 to JIS C-8303 Line cord	46M2593	6314
Japan 2.8m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08357	5472
Japan 4.3m, 12A/125V, C13 to JIS C-8303 Line Cord	39Y7926	6335
Japan 4.3m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08362	6495
Korea 2.8m, 12A/250V, C13 to KS C8305 Line Cord	39Y7925	6219
Korea 4.3m, 12A/250V, C13 to KS C8305 Line Cord	81Y2385	6494
South Africa 2.8m, 10A/250V, C13 to SABS 164 Line Cord	39Y7922	6214
South Africa 4.3m, 10A/250V, C13 to SABS 164 Line Cord	81Y2379	6576
Switzerland 2.8m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	39Y7919	6216
Switzerland 4.3m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	81Y2390	6578
Taiwan 2.8m, 10A/125V, C13 to CNS 10917-3 Line Cord	23R7158	6386
Taiwan 2.8m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2375	6317
Taiwan 2.8m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2374	6402
Taiwan 4.3m, 10A/125V, C13 to CNS 10917-3 Line Cord	4L67A08363	AX8B
Taiwan 4.3m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2389	6531
Taiwan 4.3m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2388	6530
United Kingdom 2.8m, 10A/250V, C13 to BS 1363/A Line Cord	39Y7923	6215
United Kingdom 4.3m, 10A/250V, C13 to BS 1363/A Line Cord	81Y2377	6577
United States 2.8m, 10A/125V, C13 to NEMA 5-15P Line Cord	90Y3016	6313

Description	Part number	Feature code
United States 2.8m, 10A/250V, C13 to NEMA 6-15P Line Cord	46M2592	A1RF
United States 2.8m, 13A/125V, C13 to NEMA 5-15P Line Cord	00WH545	6401
United States 4.3m, 10A/125V, C13 to NEMA 5-15P Line Cord	4L67A08359	6370
United States 4.3m, 10A/250V, C13 to NEMA 6-15P Line Cord	4L67A08361	6373
United States 4.3m, 13A/125V, C13 to NEMA 5-15P Line Cord	4L67A08360	AX8A

Systems management

The SR530 supports the following systems management tools:

- Lenovo XClarity Controller
- Lenovo XClarity Provisioning Manager
- Lenovo XClarity Essentials
- Lenovo XClarity Administrator
- Lenovo XClarity Integrators
- Lenovo XClarity Energy Manager
- Lenovo Capacity Planner

Lenovo XClarity Controller

The SR530 server contains Lenovo XClarity Controller (XCC), which provides advanced service-processor control, monitoring, and alerting functions. XClarity Controller offers three functional levels: Standard, Advanced, and Enterprise.

By default, the SR530 server includes XClarity Controller Standard features, and it can be upgraded to Advanced or Enterprise functionality by using the Features on Demand (FoD) upgrades.

XClarity Controller Standard offers the following capabilities:

- Gathering and viewing system information and inventory
- Monitoring system status and health
- Alerting and notifications
- Event logging
- Configuring network connectivity
- Configuring security
- Updating system firmware
- Configuring server settings and devices
- Real-time power usage monitoring
- Remotely controlling server power (Power on, Power off, Restart)
- Managing FoD activation keys
- Redirecting serial console via IPMI
- Capturing the video display contents when an operating system hang condition is detected

XClarity Controller Advanced Upgrade adds the following functionality to the Standard features:

- Remotely viewing video with the following graphics resolutions:
  - Up to 1600x1200 with up to 23 bits per pixel; or
  - Up to 1920x1200 with up to 15 bits per pixel
- Remotely accessing the server using the keyboard and mouse from a remote client
- Remotely deploying an operating system
- Syslog alerting
- Redirecting serial console via SSH
- Displaying graphics for real-time and historical power usage data and temperature

XClarity Controller Enterprise Upgrade adds the following functionality to the Advanced features:

- Capping power usage
- Mapping the ISO and image files located on the local client as virtual drives for use by the server
- Mounting the remote ISO and image files via HTTPS, SFTP, CIFS, and NFS
- Collaborating across up to six users of the virtual console
- Controlling quality and bandwidth usage

The XClarity Controller provides remote server management through industry-standard interfaces:

- Intelligent Platform Management Interface (IPMI) Version 2.0
- Simple Network Management Protocol (SNMP) Version 3
- Common Information Model (CIM)
- Data Center Manageability Interface (DCMI) Version 1.5
- Redfish REpresentational State Transfer (REST) API
- Web browser with HTML5 support
- Command-line interface
- Virtual Operator Panel with XClarity Mobile App via the front USB port with XClarity Controller access

Virtual Operator Panel provides quick access to system status, firmware, network, health, and alerts information. With proper authentication, it also allows to configure systems management and network settings and to control system power (Power on, Power off, Restart). The Virtual Operator Panel can be accessed from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access (See Components and connectors).

Note: Depending on the system settings, the front USB port can be assigned to XClarity Controller for management functions, or to the system as a regular USB 2.0 port, or switched between two functions by using the system ID button.

IPMI via the Ethernet port (IPMI over LAN) is supported, however it is disabled by default. For CTO orders you can specify whether you want to the feature enabled or disabled in the factory, using the feature codes listed in the following table.

Table 40. IPMI-over-LAN settings

Part number	Feature code	Description
CTO only	B7XZ	Disable IPMI-over-LAN (default)
CTO only	B7Y0	Enable IPMI-over-LAN

The following table lists the XClarity Controller FoD upgrades.

Table 41. XClarity Controller FoD upgrades

Description	Part number	Feature code	Maximum quantity
ThinkSystem XClarity Controller Standard to Advanced Upgrade	4L47A09132	AVUT	1
ThinkSystem XClarity Controller Standard to Enterprise Upgrade	None*	AUPW	1
ThinkSystem XClarity Controller Advanced to Enterprise Upgrade	4L47A09133	None**	1

* Factory-installed only.
** Field upgrade only.

Configuration notes:

- For factory-installed upgrades, either Standard to Advanced Upgrade (feature AVUT) or Standard to Enterprise Upgrade (feature AUPW) can be selected, but not both.
- For field upgrades, the Advanced to Enterprise Upgrade (4L47A09133) requires the Standard to Advanced Upgrade to be activated on the server previously with either the factory-installed feature AVUT or field upgrade 4L47A09132.

Lenovo XClarity Provisioning Manager

Lenovo XClarity Provisioning Manager is a UEFI-embedded GUI application that combines the functions of configuring system setup settings, configuring RAID, and updating applications and firmware. It also enables you to install the supported operating systems and associated device drivers, run diagnostics, and collect service data.

Lenovo XClarity Provisioning Manager has the following features:

- Automatic hardware detection
- Collecting and viewing system inventory information
- Configuring UEFI system setup settings
- Updating the system firmware
- Configuring RAID by using the RAID Setup Wizard or Advanced mode
- Installing an operating system and device drivers automatically or manually
- Running diagnostics and collecting service data

Lenovo XClarity Essentials

Lenovo offers the following XClarity Essentials software tools that can help you set up, use, and maintain the server at no additional cost:

- Lenovo XClarity Essentials OneCLI
  OneCLI is a collection of server management tools that utilize a command line interface program to manage firmware, hardware, and operating systems. It provides functions to collect full system health information (including health status), configure system setting, and update system firmware and drivers.
- Lenovo XClarity Essentials UpdateXpress
  The UpdateXpress tool is a standalone GUI application for firmware and device driver updates that enables you to maintain your server firmware and device drivers up-to-date and help you avoid unnecessary server outages. The tool acquires and deploys individual updates and UpdateXpress System Packs (UXSPs) which are integration-tested bundles.
- Lenovo XClarity Essentials Bootable Media Creator
  The Bootable Media Creator (BOMC) tool is used to create bootable media for offline firmware update.

For more information and downloads, visit the Lenovo XClarity Essentials web page:
http://support.lenovo.com/us/en/documents/LNVO-center

Lenovo XClarity Administrator

Lenovo XClarity is a centralized systems management solution that helps administrators deliver infrastructure faster. This solution integrates easily with Lenovo x86 servers, RackSwitch switches, and DS Series storage, providing automated agent-less discovery, monitoring, firmware updates, configuration management, and bare metal deployment of operating systems and hypervisors across multiple servers.

Lenovo XClarity Administrator is an optional software component for the SR530 server which can be downloaded and used at no charge to discover and monitor the SR530 and manage firmware upgrades for them.

If software support is required for Lenovo XClarity Administrator, or Lenovo XClarity Administrator premium features (such as configuration management and operating system deployment) are required, or both, Lenovo XClarity Pro software subscription should be ordered. Lenovo XClarity Pro is licensed on a per managed system basis, that is, each managed Lenovo system requires a license.

The following table lists the geo-specific Lenovo XClarity software license options.

Table 42. Lenovo XClarity software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Pro, per Managed Endpoint w/1 Yr SW S&S	00MT201	00MT207	1
Lenovo XClarity Pro, per Managed Endpoint w/3 Yr SW S&S	00MT202	00MT208	1
Lenovo XClarity Pro, per Managed Endpoint w/5 Yr SW S&S	00MT203	00MT209	1

* NA = North America; AP = Asia Pacific
** EMEA = Europe, Middle East, Africa; LA = Latin America

Lenovo XClarity Administrator offers the following standard features that are available at no charge:

- Auto-discovery and monitoring of Lenovo x86 servers, RackSwitch switches, Flex System chassis, and DS Series storage systems
- Firmware updates and compliance enforcement
- External alerts and notifications via SNMP traps, syslog remote logging, and e-mail
- Secure connections to managed endpoints
- NIST 800-131A or FIPS 140-2 compliant cryptographic standards between the management solution and managed endpoints
- Integration into existing higher level management systems such as cloud automation and orchestration tools through REST APIs, providing extensive external visibility and control over hardware resources
- An intuitive, easy-to-use GUI
- Scripting with Windows PowerShell, providing command-line visibility and control over hardware resources

Lenovo XClarity Administrator offers the following premium features that require an optional Pro license:

- Pattern-based configuration management that allows to define configurations once and apply repeatedly without errors when deploying new servers or redeploying existing servers without disrupting the fabric
- Bare-metal deployment of operating systems and hypervisors to streamline infrastructure provisioning

For more information, refer to the Lenovo XClarity Administrator Product Guide:
http://lenovopress.com/tips1200

Lenovo XClarity Integrators

Lenovo offers at no charge (if software support is required, a Lenovo XClarity Pro software subscription license should be ordered) two software plug-in modules, Lenovo XClarity Integrators, to manage physical infrastructure from leading external virtualization management software tools from Microsoft and VMware:

- Lenovo XClarity Integrator for Microsoft System Center
- Lenovo XClarity Integrator for VMware vCenter

Lenovo XClarity Integrators offer the following additional features:

- Ability to discover, manage, and monitor Lenovo server hardware from VMware vCenter or Microsoft System Center
- Deployment of firmware updates and configuration patterns to Lenovo x86 rack servers and Flex System from the virtualization management tool
- Non-disruptive server maintenance in clustered environments that reduces workload downtime by dynamically migrating workloads from affected hosts during rolling server updates or reboots
- Greater service level uptime and assurance in clustered environments during unplanned hardware events by dynamically triggering workload migration from impacted hosts when impending hardware failures are predicted

For more information, refer to the Lenovo XClarity Integrators web page:
http://www3.lenovo.com/us/en/data-center/software/systems-management/xclarity-integrators

Lenovo XClarity Energy Manager

Lenovo XClarity Energy Manager provides a stand-alone, web-based agent-less power management console that provides real time data and enables you to observe, plan and manage power and cooling for Lenovo servers. Using built-in intelligence, it identifies server power consumption trends and ideal power settings and performs cooling analysis so that you can define and optimize power-saving policies.

Lenovo XClarity Energy Manager offers the following capabilities:

- Monitors room, row, rack, and device levels in the data center
- Reports vital server information, such as power, temperature and resource utilization
- Monitors inlet temperature to locate hot spots, reducing the risk of data or device damage
- Provides finely-grained controls to limit platform power in compliance with IT policy
- Generates alerts when a user-defined threshold is reached

Lenovo XClarity Energy Manager is an optional software component for the SR530 server that is licensed on a per managed node basis, that is, each managed server requires a license. The 1-node Energy Manager license is included in the XClarity Controller Enterprise upgrade.

To manage systems without XClarity Controller Enterprise licenses, a node license pack should be purchased. The following table lists the geo-specific Lenovo XClarity Energy Manager software license options.

Table 43. Lenovo XClarity Energy Manager software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Energy Manager, 1 Node w/ 1 Yr S&S	01DA225	01DA228	1

* NA = North America; AP = Asia Pacific.
** EMEA = Europe, Middle East, Africa; LA = Latin America.

For more information, refer to the Lenovo XClarity Energy Manager web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lxem

Lenovo Capacity Planner

Lenovo Capacity Planner is a power consumption evaluation tool that enhances data center planning by enabling IT administrators and pre-sales professionals to understand various power characteristics of racks, servers, and other devices. Capacity Planner can dynamically calculate the power consumption, current, British Thermal Unit (BTU), and volt-ampere (VA) rating at the rack level, improving the planning efficiency for large-scale deployments.

For more information, refer to the Capacity Planner web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

Security

The SR530 server offers the following security features:

- Power-on password
- Administrator's password
- Secure firmware updates
- Onboard Trusted Platform Module (TPM) version 1.2 or 2.0 (configurable UEFI system setting)
- Trusted Cryptographic Module (TCM) (optional; available in PRC only)
- Nationz Trusted Platform Module v2.0 (optional; available in PRC only)
- Lockable front bezel (optional)
- Security Key Lifecycle Manager (SKLM) encryption key management for SEDs - FoD upgrade (optional)
- Lenovo Business Vantage security software (optional; available in PRC only)

The server is NIST SP 800-147B compliant.

The following table lists the security options that are available for the SR530 server.

Table 44. Security options

Description	Part number	Feature code	Maximum quantity
Lockable front bezel			
ThinkSystem 1U Security Bezel	7Z17A02581	AUWR	1
Trusted Cryptographic Module (PRC only)			
ThinkSystem Trusted Cryptographic Module	None*	AVKE	1
Trusted Platform Module (PRC only)			
ThinkSystem Nationz Trusted Platform Module v2.0	None*	B22N	1
Security Key Lifecycle Manager - FoD (United States, Canada, Asia Pacific, and Japan)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00D9998	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00D9999	AS6C	1
Security Key Lifecycle Manager - FoD (Latin America, Europe, Middle East, and Africa)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00FP648	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00FP649	AS6C	1

* Factory-installed only; no field upgrade.

Lenovo Business Vantage is a security software tool suite (available only in PRC) designed to work with the TCM or Nationz TPM for enhanced security, to keep user data safe, and to erase confidential data completely from a drive.

Lenovo Business Vantage provides the following features:

- Encrypts files to ensure data safety by using the TCM or Nationz TPM.
- Erases confidential data from a hard disk.
- Prohibits unauthorized access to the USB port of devices.
- Encrypts files to ensure data security on a USB storage device.

For more information, refer to the Lenovo Business Vantage web page:
http://support.lenovo.com.cn/lenovo/wsi/es/es.html

Rack installation

The following table lists the rack installation options that are available for the SR530 server.

Table 45. Rack installation options

Description	Part number	Feature code	Maximum quantity
4-post rail kits			
ThinkSystem Tool-less Slide Rail	7M27A05702	AXCA	1
ThinkSystem Tool-less Slide Rail Kit with 1U CMA	7M27A05701	AXCB	1
ThinkSystem Screw-in Slide Rail	4M17A07274	AXFN	1
ThinkSystem Screw-in Slide Rail Kit with 1U CMA	4M17A07281	B0TE	1
ThinkSystem Tool-less Friction Rail	4M17A07273	AXFM	1
Cable management arm (CMA) upgrade			
ThinkSystem 1U CMA Upgrade Kit for Tool-less Slide Rail	7M27A05699	None^	1*
ThinkSystem 1U CMA Upgrade Kit for Screw-in Slide Rail	4M17A07276	AXFP	1**
Front VGA port			
ThinkSystem SR530/SR630 Front VGA Connector (for 3.5" models)	None***	AUWU	1
ThinkSystem SR530/SR570/SR630 Front VGA Connector Upgrade Kit (for 2.5" models)	7Z17A02579	AUWW	1

^ Field upgrade only.
* The CMA Upgrade Kit for Tool-less Slide Rail is supported with the Tool-less Slide Rail (7M27A05702) only.
** The CMA Upgrade Kit for Screw-in Slide Rail is supported with the Screw-in Slide Rail (4M17A07274) only.
*** Factory-installed only; no field upgrade.

The following table summarizes the rail kit features and specifications.

Table 46. Rail kit features and specifications summary

Feature	Tool-less Slide Rail		Screw-in Slide Rail		Tool-less Friction Rail
	Without CMA	With CMA	Without CMA	With CMA	
Part number	7M27A05702	7M27A05701	4M17A07274	4M17A07281	4M17A07273
CMA	7M27A05699	Included	4M17A07276	Included	No support
Rail length	730 mm (28.74 in.)	807 mm (31.8 in.)	836.8 mm (32.9 in.)	836.8 mm (32.9 in.)	728.1 mm (28.7 in.)
Rail type	Full-out slide (ball bearing)		Full-out slide (ball bearing)		Half-out slide (friction)
Tool-less installation	Yes		No		Yes
In-rack server maintenance	Yes		Yes		No
1U PDU support	Yes		Yes		Yes
0U PDU support	Limited*		Limited*		Limited**
Rack type	IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant
Mounting holes	Square or round		Square, round, or threaded		Square or round
Mounting flange thickness	2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)
Distance between front and rear mounting flanges^	609.6 mm (24 in.) – 863.6 mm (34 in.)		609.6 mm (24 in.) – 812.8 mm (32 in.)		609.6 mm (24 in.) – 863.6 mm (34 in.)

* If a 0U PDU is used, the rack cabinet must be at least 1100 mm (43.31 in.) deep if no CMA is used, or at least 1200 mm (47.24 in.) deep if a CMA is used.
** If a 0U PDU used, the rack must be at least 1000 mm (39.37 in.) deep.
^ Measured when mounted on the rack, from the front surface of the front mounting flange to the rear most point of the rail.

Operating systems

The server supports the following operating systems:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 8.1
- Red Hat Enterprise Linux 8.2
- Red Hat Enterprise Linux 8.3
- SUSE Linux Enterprise Server 12 SP4
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 12 Xen SP4
- SUSE Linux Enterprise Server 12 Xen SP5
- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Server 15 SP1
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 15 Xen
- SUSE Linux Enterprise Server 15 Xen SP1
- SUSE Linux Enterprise Server 15 Xen SP2
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2

For a complete list of supported, certified and tested operating systems, plus additional details and links to relevant web sites, see the Operating System Interoperability Guide: https://lenovopress.com/osig#servers=sr530-7x07-7x08-sp-gen-2

For configure-to-order configurations, the server can be preloaded with VMware ESXi installed on M.2 cards. Ordering information is listed in the following table.

Table 47. VMware ESXi preload

Part number	Feature code	Description
CTO only	B3VW	VMware ESXi 6.5 U2 (Factory Installed)
CTO only	B6U0	VMware ESXi 6.5 U3 (factory installed)
CTO only	B3VX	VMware ESXi 6.7 (Factory Installed)
CTO only	B4XA	VMware ESXi 6.7 U1 (Factory Installed)
CTO only	B6U1	VMware ESXi 6.7 U2 (factory installed)
CTO only	B88T	VMware ESXi 6.7 U3 (factory installed)
CTO only	BBZG	VMware ESXi 7.0 (Factory Installed)
CTO only	BE5E	VMware ESXi 7.0 U1 (Factory Installed)

Physical specifications

The SR530 has the following overall physical dimensions, excluding components that extend outside the standard chassis, such as EIA flanges, front security bezel (if any), and power supply handles:

- Width: 435 mm (17.1 inches)
- Height: 43 mm (1.7 inches)

- Depth: 750 mm (29.5 inches)

The following table lists the detailed dimensions. See the figure below for the definition of each dimension.

Table 48. Detailed dimensions

Dimension	Description
482 mm	X_a = Width, to the outsides of the front EIA flanges
435 mm	X_b = Width, to the rack rail mating surfaces
435 mm	X_c = Width, to the outer most chassis body feature
43 mm	Y_a = Height, from the bottom of chassis to the top of the chassis
715 mm	Z_a = Depth, from the rack flange mating surface to the rearmost I/O port surface
716 mm	Z_b = Depth, from the rack flange mating surface to the rearmost feature of the chassis body
744 mm	Z_c = Depth, from the rack flange mating surface to the rearmost feature such as power supply handle
35 mm	Z_d = Depth, from the forwardmost feature on front of EIA flange to the rack flange mating surface
47 mm	Z_e = Depth, from the front of security bezel (if applicable) or forwardmost feature to the rack flange mating surface

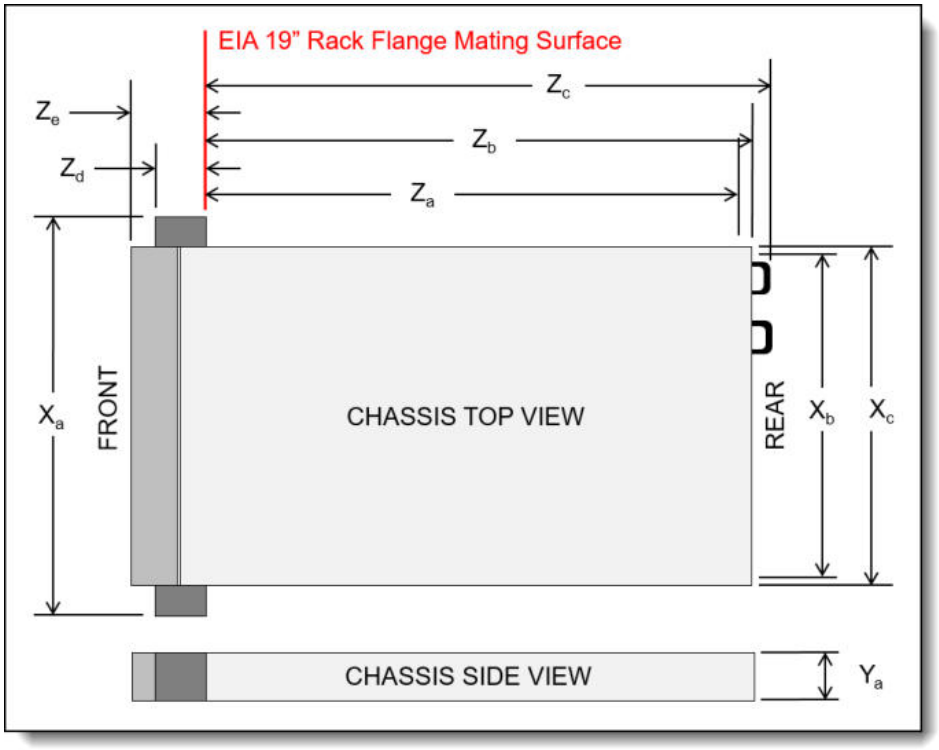


Figure 8. Server dimensions

The shipping dimensions (cardboard packaging) of the SR530 are as follows:

- Width: 587 mm (23.1 inches)
- Height: 225 mm (8.9 inches)
- Depth: 998 mm (39.3 inches)

The SR530 server has the following weight:

- Minimum configuration: 10.2 kg (22.5 lb)
- Maximum configuration: 16.0 kg (35.3 lb)

Operating environment

The SR530 server complies with ASHRAE class A2 specifications. The server performance might be impacted when the operating temperature is outside the ASHRAE A2 specifications. Depending on the hardware configuration, some server models comply with ASHRAE class A3 and class A4 specifications. To comply with ASHRAE class A3 and class A4 specifications, the server models must meet the following hardware configuration requirements at the same time:

- Two power supplies must be installed
- No system fan failure

The SR530 server is supported in the following environment:

- Air temperature:
  - Operating:
    - ASHRAE Class A4: 5 °C - 45 °C (41 °F - 113 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 125-m (410-ft) increase in altitude
    - ASHRAE Class A3: 5 °C - 40 °C (41 °F - 104 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 175-m (574-ft) increase in altitude
    - ASHRAE Class A2: 10 °C - 35 °C (50 °F - 95 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 300-m (984-ft) increase in altitude
  - Non-operating: 5 °C - 45 °C (41 °F - 113 °F)
  - Storage: -40 °C - +60 °C (-40 °F - 140 °F)
- Maximum altitude: 3,050 m (10,000 ft)
- Humidity:
  - Operating:
    - ASHRAE Class A4: 8% - 90% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A3: 8% - 85% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A2: 8% - 80% (non-condensing); maximum dew point: 21 °C (70 °F)
  - Storage: 8% - 90% (non-condensing)
- Electrical:
  - 100 - 127 (nominal) V AC; 50 Hz / 60 Hz
  - 200 - 240 (nominal) V AC; 50 Hz / 60 Hz
  - 180 - 300 V DC (HVDC; supported in PRC only)
- Acoustics:
  - Minimum configuration:
    - Operating: 5.0 bels
    - Idle: 4.5 bels
  - Maximum configuration:
    - Operating: 5.5 bels
    - Idle: 5.2 bels
- Vibration:
  - Operating: 0.21 G rms at 5 Hz to 500 Hz for 15 minutes across 3 axes
  - Non-operating: 1.04 G rms at 2 Hz to 200 Hz for 15 minutes across 6 surfaces
- Shock:
  - Operating: 15 G for 3 milliseconds in each direction (positive and negative X, Y, and Z axes)
  - Non-operating:
    - 12 kg - 22 kg: 50 G for 152 in./sec velocity change across 6 surfaces
    - 23 kg - 31 kg: 35 G for 152 in./sec velocity change across 6 surfaces

The following table lists the maximum system power load, rated inlet current, and system heat output based on the power supply and source voltage.

Table 49. Rated system power, inlet current, and system heat output

Power supply	Source voltage	Maximum power load per system (two power supplies)	Rated current per inlet	System heat output
550 W Platinum	100 - 127 V AC	722 W	6.2 A	2463 BTU/hour
	200 - 240 V AC	704 W	3 A	2402 BTU/hour
	180 - 300 V DC	702 W	2.5 A	2395 BTU/hour
750 W Platinum	100 - 127 V AC	984 W	8.4 A	3357 BTU/hour
	200 - 240 V AC	958 W	4.1 A	3269 BTU/hour
	180 - 300 V DC	958 W	3.5 A	3269 BTU/hour
750 W Titanium	200 - 240 V AC	949 W	4.1 A	3238 BTU/hour
	180 - 300 V DC	948 W	3.5 A	3235 BTU/hour

Warranty and support

The SR530 server has a one-year (7X07) or three-year (Machine Type 7X08) warranty.

The standard warranty terms are customer-replaceable unit (CRU) and onsite (for field-replaceable units FRUs only) with standard call center support during normal business hours and 9x5 Next Business Day Parts Delivered.

Lenovo's additional support services provide a sophisticated, unified support structure for your data center, with an experience consistently ranked number one in customer satisfaction worldwide. Available offerings include:

- **Premier Support**

  Premier Support provides a Lenovo-owned customer experience and delivers direct access to technicians skilled in hardware, software, and advanced troubleshooting, in addition to the following:

  - Direct technician-to-technician access through a dedicated phone line
  - 24x7x365 remote support
  - Single point of contact service
  - End to end case management
  - Third-party collaborative software support
  - Online case tools and live chat support
  - On-demand remote system analysis
- **Warranty Upgrade (Preconfigured Support)**

  Services are available to meet the on-site response time targets that match the criticality of your systems.

  - 3, 4, or 5 years of service coverage
  - 1-year or 2-year post-warranty extensions
  - **Foundation Service**: 9x5 service coverage with next business day onsite response. YourDrive YourData is an optional extra (see below).
  - **Essential Service:** 24x7 service coverage with 4-hour onsite response or 24-hour committed repair (available only in select countries). Bundled with YourDrive YourData.
  - **Advanced Service:** 24x7 service coverage with 2-hour onsite response or 6-hour committed repair (available only in select countries). Bundled with YourDrive YourData.

- **Managed Services**

  Lenovo Managed Services provides continuous 24x7 remote monitoring (plus 24x7 call center availability) and proactive management of your data center using state-of-the-art tools, systems, and practices by a team of highly skilled and experienced Lenovo services professionals.

  Quarterly reviews check error logs, verify firmware & OS device driver levels, and software as needed. We'll also maintain records of latest patches, critical updates, and firmware levels, to ensure you systems are providing business value through optimized performance.

- **Technical Account Management (TAM)**

  A Lenovo Technical Account Manager helps you optimize the operation of your data center based on a deep understanding of your business. You gain direct access to your Lenovo TAM, who serves as your single point of contact to expedite service requests, provide status updates, and furnish reports to track incidents over time. In addition, your TAM will help proactively make service recommendations and manage your service relationship with Lenovo to make certain your needs are met.

- **Enterprise Server Software Support**

  Enterprise Software Support is an additional support service providing customers with software support on Microsoft, Red Hat, SUSE, and VMware applications and systems. Around the clock availability for critical problems plus unlimited calls and incidents helps customers address challenges fast, without incremental costs. Support staff can answer troubleshooting and diagnostic questions, address product comparability and interoperability issues, isolate causes of problems, report defects to software vendors, and more.

- **YourDrive YourData**

  Lenovo's YourDrive YourData is a multi-drive retention offering that ensures your data is always under your control, regardless of the number of drives that are installed in your Lenovo server. In the unlikely event of a drive failure, you retain possession of your drive while Lenovo replaces the failed drive part. Your data stays safely on your premises, in your hands. The YourDrive YourData service can be purchased in convenient bundles and is optional with Foundation Service. It is bundled with Essential Service and Advanced Service.

- **Health Check**

  Having a trusted partner who can perform regular and detailed health checks is central to maintaining efficiency and ensuring that your systems and business are always running at their best. Health Check supports Lenovo-branded server, storage, and networking devices, as well as select Lenovo-supported products from other vendors that are sold by Lenovo or a Lenovo-Authorized Reseller.

Examples of region-specific warranty terms are second or longer business day parts delivery or parts-only base warranty.

If warranty terms and conditions include onsite labor for repair or replacement of parts, Lenovo will dispatch a service technician to the customer site to perform the replacement. Onsite labor under base warranty is limited to labor for replacement of parts that have been determined to be field-replaceable units (FRUs). Parts that are determined to be customer-replaceable units (CRUs) do not include onsite labor under base warranty.

If warranty terms include parts-only base warranty, Lenovo is responsible for delivering only replacement parts that are under base warranty (including FRUs) that will be sent to a requested location for self-service. Parts-only service does not include a service technician being dispatched onsite. Parts must be changed at customer's own cost and labor and defective parts must be returned following the instructions supplied with the spare parts.

Lenovo Service offerings are region-specific. Not all preconfigured support and upgrade options are available in every region. For information about Lenovo service upgrade offerings that are available in your region, refer to the following resources:

- Service part numbers in Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com/#/services
- Lenovo Services Availability Locator
  http://lenovolocator.com/

For service definitions, region-specific details, and service limitations, please refer to the following documents:

- Lenovo Statement of Limited Warranty for Data Center Group (DCG) Servers and System Storage
  http://pcsupport.lenovo.com/us/en/solutions/ht503310
- Lenovo Data Center Services Agreement
  http://support.lenovo.com/us/en/solutions/ht116628

Services

Lenovo Services is a dedicated partner to your success. Our goal is to reduce your capital outlays, mitigate your IT risks, and accelerate your time to productivity.

Note: Some service options may not be available in all countries. For more information, go to https://www.lenovo.com/systems/services. For information about Lenovo service upgrade offerings that are available in your region, contact your local Lenovo sales representative or business partner.

Here's a more in-depth look at what we can do for you:

- **Asset Recovery Services**

  Asset Recovery Services (ARS) helps customers recover the maximum value from their end-of-life equipment in a cost-effective and secure way. On top of simplifying the transition from old to new equipment, ARS mitigates environmental and data security risks associated with data center equipment disposal. Lenovo ARS is a cash-back solution for equipment based on its remaining market value, yielding maximum value from aging assets and lowering total cost of ownership for your customers. For more information, see the ARS page, https://lenovopress.com/lp1266-reduce-e-waste-and-grow-your-bottom-line-with-lenovo-ars.

- **Assessment Services**

  An Assessment helps solve your IT challenges through an onsite, multi-day session with a Lenovo technology expert. We perform a tools-based assessment which provides a comprehensive and thorough review of a company's environment and technology systems. In addition to the technology based functional requirements, the consultant also discusses and records the non-functional business requirements, challenges, and constraints. Assessments help organizations like yours, no matter how large or small, get a better return on your IT investment and overcome challenges in the ever-changing technology landscape.

- **Design Services**

  Professional Services consultants perform infrastructure design and implementation planning to support your strategy. The high-level architectures provided by the assessment service are turned into low level designs and wiring diagrams, which are reviewed and approved prior to implementation. The implementation plan will demonstrate an outcome-based proposal to provide business capabilities through infrastructure with a risk-mitigated project plan.

- **Basic Hardware Installation**

  Lenovo experts can seamlessly manage the physical installation of your server, storage, or networking hardware. Working at a time convenient for you (business hours or off shift), the technician will unpack and inspect the systems on your site, install options, mount in a rack cabinet, connect to power and network, check and update firmware to the latest levels, verify operation, and dispose of the packaging, allowing your team to focus on other priorities.

- **Deployment Services**

  When investing in new IT infrastructures, you need to ensure your business will see quick time to value with little to no disruption. Lenovo deployments are designed by development and engineering teams who know our Products & Solutions better than anyone else, and our technicians own the process from delivery to completion. Lenovo will conduct remote preparation and planning, configure & integrate systems, validate systems, verify and update appliance firmware, train on administrative tasks, and provide post-deployment documentation. Customer's IT teams leverage our skills to enable IT staff to transform with higher level roles and tasks.

- **Integration, Migration, and Expansion Services**

  Move existing physical & virtual workloads easily, or determine technical requirements to support increased workloads while maximizing performance. Includes tuning, validation, and documenting ongoing run processes. Leverage migration assessment planning documents to perform necessary migrations.

Regulatory compliance

The ThinkSystem SR530 server conforms to the following regulations:

- United States: FCC Part 15, Class A; UL 60950-1
- Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1
- Mexico: NOM-19
- Argentina: IEC60950-1
- European Union: CE Mark (EN55022 Class A, IEC/EN60950-1, EN55024, EN61000-3-2, EN61000-3-3)
- Germany: TUV-GS (IEC/EN 60950-1, EK1-ITB2000)
- Russia, Kazakhstan, Belarus: EAC (TR CU 004/2011, TR CU 020/2011)
- China: CCC GB4943.1, GB9254 Class A, GB17625.1
- India: BIS
- Japan: VCCI, Class A
- Taiwan: BSMI CNS13438, Class A; CNS14336-1
- Korea: KN22, Class A; KN24
- Australia/New Zealand: AS/NZS CISPR 22 Class A
- Reduction of Hazardous Substances (ROHS)
- Energy Star 3.0 (excluding configurations with Bronze 3204, Gold 5222, or Platinum 8256 processors)

Note: For more information on the Energy Star 3.0 certification, refer to the *Energy Star 3.0 Certifications for ThinkSystem Servers* publication:
http://lenovopress.com/lp1230

External drive enclosures

The server supports attachment to external drive enclosures using a RAID controller with external ports or a SAS host bus adapter. Adapters supported by the server are listed in the SAS adapters for external storage section.

Note: Information provided in this section is for ordering reference purposes only. For the operating system and adapter support details, refer to the interoperability matrix for a particular storage enclosure that can be found on the Lenovo Data Center Support web site:
http://datacentersupport.lenovo.com

Table 50. External drive enclosures

Description	Part number		
	Worldwide	Japan	PRC
Lenovo Storage D1212 LFF Disk Expansion with Dual SAS IO Modules	4587A11	4587A1J	4587A1C
Lenovo Storage D1224 SFF Disk Expansion with Dual SAS IO Modules	4587A31	4587A3J	4587A3C
Lenovo Storage D3284 4TB x 84 HD Expansion Enclosure	641311F		
Lenovo Storage D3284 6TB x 84 HD Expansion Enclosure	641312F		
Lenovo Storage D3284 8TB x 84 HD Expansion Enclosure	641313F		
Lenovo Storage D3284 10TB x 84 HD Expansion Enclosure	641314F		

For details about supported drives, adapters, and cables, see the following Lenovo Press Product Guides:

- Lenovo Storage D1212 and D1224
  http://lenovopress.com/lp0512
- Lenovo Storage D3284
  http://lenovopress.com/lp0513

External storage systems

Lenovo offers the ThinkSystem DE Series and ThinkSystem DM Series external storage systems for high-performance storage. See the DE Series and DM Series product guides for specific controller models, expansion enclosures and configuration options:

- ThinkSystem DE Series Storage
  https://lenovopress.com/storage/thinksystem/de-series#rt=product-guide
- ThinkSystem DM Series Storage
  https://lenovopress.com/storage/thinksystem/dm-series#rt=product-guide

External backup units

The following table lists the external backup options that are offered by Lenovo.

Table 51. External backup options

Part number	Description
External RDX USB drives	
4T27A10725	ThinkSystem RDX External USB 3.0 Dock
External SAS tape backup drives	
6160S6E	IBM TS2260 Tape Drive Model H6S
6160S7E	IBM TS2270 Tape Drive Model H7S
6160S8E	IBM TS2280 Tape Drive Model H8S
External SAS tape backup autoloaders	
6171S5R	IBM TS2900 Tape Autoloader w/LTO5 HH SAS
6171S6R	IBM TS2900 Tape Autoloader w/LTO6 HH SAS
6171S7R	IBM TS2900 Tape Autoloader w/LTO7 HH SAS
External tape backup libraries	
6741A1F	IBM TS4300 3U Tape Library-Base Unit
6741A3F	IBM TS4300 3U Tape Library-Expansion Unit
Full High 8 Gb Fibre Channel for TS4300	
01KP954	LTO 8 FH Fibre Channel Drive
01KP938	LTO 7 FH Fibre Channel Drive
01KP935	LTO 6 FH Fibre Channel Drive
Half High 8 Gb Fibre Channel for TS4300	
01KP952	LTO 8 HH Fibre Channel Drive
01KP936	LTO 7 HH Fibre Channel Drive
01KP933	LTO 6 HH Fibre Channel Drive
Half High 6 Gb SAS for TS4300	
01KP953	LTO 8 HH SAS Drive
01KP937	LTO 7 HH SAS Drive
01KP934	LTO 6 HH SAS Drive

For more information, see the list of Product Guides in the Backup units category:
https://lenovopress.com/servers/options/backup

Fibre Channel SAN switches

Lenovo offers the ThinkSystem DB Series of Fibre Channel SAN switches and directors for high-performance storage expansion. See the DB Series product guides for models and configuration options:

- ThinkSystem DB Series SAN Switches and Directors: https://lenovopress.com/storage/switches/rack#rt=product-guide

Rack cabinets

The following table lists the supported rack cabinets.

Table 52. Rack cabinets

Part number	Description
7D2B0001WW / 7D2N0001WW	12U 1200mm Deep Micro Datacenter Rack
7D2C0001WW / 7D2P0001WW	18U 1200mm Deep Micro Datacenter Rack
93072RX	25U Standard Rack
93072PX	25U Static S2 Standard Rack
93634PX	42U 1100mm Dynamic Rack
93634EX	42U 1100mm Dynamic Expansion Rack
93604PX	42U 1200mm Deep Dynamic Rack
93614PX	42U 1200mm Deep Static Rack
93084EX	42U Enterprise Expansion Rack
93084PX	42U Enterprise Rack
93074RX	42U Standard Rack

For specifications about these racks, see the Lenovo Rack Cabinet Reference, available from: https://lenovopress.com/lp1287-lenovo-rack-cabinet-reference

For more information, see the list of Product Guides in the Rack cabinets category: https://lenovopress.com/servers/options/racks

KVM switches and consoles

The following table lists the supported KVM consoles, keyboards, and KVM switches.

Table 53. Console keyboards

Part number	Description
Console keyboards	
7ZB7A05469	ThinkSystem Keyboard w/ Int. Pointing Device USB - Arabic 253 RoHS v2
7ZB7A05468	ThinkSystem Keyboard w/ Int. Pointing Device USB - Belg/UK 120 RoHS v2
7ZB7A05206	ThinkSystem Keyboard w/ Int. Pointing Device USB - Czech 489 RoHS v2
7ZB7A05207	ThinkSystem Keyboard w/ Int. Pointing Device USB - Danish 159 RoHS v2
7ZB7A05208	ThinkSystem Keyboard w/ Int. Pointing Device USB - Dutch 143 RoHS v2
7ZB7A05210	ThinkSystem Keyboard w/ Int. Pointing Device USB - Fr/Canada 445 RoHS v2
7ZB7A05209	ThinkSystem Keyboard w/ Int. Pointing Device USB - French 189 RoHS v2
7ZB7A05211	ThinkSystem Keyboard w/ Int. Pointing Device USB - German 129 RoHS v2
7ZB7A05212	ThinkSystem Keyboard w/ Int. Pointing Device USB - Greek 219 RoHS v2
7ZB7A05213	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hebrew 212 RoHS v2
7ZB7A05214	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hungarian 208 RoHS v2

Part number	Description
7ZB7A05215	ThinkSystem Keyboard w/ Int. Pointing Device USB - Italian 141 RoHS v2
7ZB7A05216	ThinkSystem Keyboard w/ Int. Pointing Device USB - Japanese 194 RoHS v2
7ZB7A05217	ThinkSystem Keyboard w/ Int. Pointing Device USB - Korean 413 RoHS v2
7ZB7A05218	ThinkSystem Keyboard w/ Int. Pointing Device USB - LA Span 171 RoHS v2
7ZB7A05219	ThinkSystem Keyboard w/ Int. Pointing Device USB - Norwegian 155 RoHS v2
7ZB7A05220	ThinkSystem Keyboard w/ Int. Pointing Device USB - Polish 214 RoHS v2
7ZB7A05221	ThinkSystem Keyboard w/ Int. Pointing Device USB - Portuguese 163 RoHS v2
7ZB7A05222	ThinkSystem Keyboard w/ Int. Pointing Device USB - Russian 441 RoHS v2
7ZB7A05223	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovak 245 RoHS v2
7ZB7A05231	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovenian 234 RoHS v2
7ZB7A05224	ThinkSystem Keyboard w/ Int. Pointing Device USB - Spanish 172 RoHS v2
7ZB7A05225	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swed/Finn 153 RoHS v2
7ZB7A05226	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swiss F/G 150 RoHS v2
7ZB7A05227	ThinkSystem Keyboard w/ Int. Pointing Device USB - Thai 191 RoHS v2
7ZB7A05467	ThinkSystem Keyboard w/ Int. Pointing Device USB - Trad Chinese/US 467 RoHS v2
7ZB7A05228	ThinkSystem Keyboard w/ Int. Pointing Device USB - Turkish 179 RoHS v2
7ZB7A05229	ThinkSystem Keyboard w/ Int. Pointing Device USB - UK Eng 166 RoHS v2
7ZB7A05470	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Eng 103P RoHS v2
7ZB7A05230	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Euro 103P RoHS v2
ThinkSystem Digital and Analog KVM Console switches and cables	
1754D1T	ThinkSystem Digital 2x1x16 KVM Switch (DVI video output port)
1754A1T	ThinkSystem Analog 1x8 KVM Switch (DVI video output port)
4X97A11108	ThinkSystem VGA to DVI Conversion Cable
4X97A11109	ThinkSystem Single-USB Conversion Cable for Digital KVM
4X97A11107	ThinkSystem Dual-USB Conversion Cable for Digital KVM
4X97A11106	ThinkSystem USB Conversion Cable for Analog KVM
GCM and LCM Console switches and cables	
1754D2X	Global 4x2x32 Console Manager (GCM32)
1754D1X	Global 2x2x16 Console Manager (GCM16)
1754A2X	Local 2x16 Console Manager (LCM16)
1754A1X	Local 1x8 Console Manager (LCM8)
43V6147	Single Cable USB Conversion Option (UCO)
39M2895	USB Conversion Option (4 Pack UCO)
46M5383	Virtual Media Conversion Option Gen2 (VCO2)
46M5382	Serial Conversion Option (SCO)

For more information, see the list of Product Guides in the KVM Switches and Consoles category:
http://lenovopress.com/servers/options/kvm

Power distribution units

The following table lists the power distribution units (PDUs) that are offered by Lenovo.

Table 54. Power distribution units

Part number	Description
0U Basic PDUs	
00YJ776	0U 36 C13/6 C19 24A/200-240V 1 Phase PDU with NEMA L6-30P line cord
00YJ777	0U 36 C13/6 C19 32A/200-240V 1 Phase PDU with IEC60309 332P6 line cord
00YJ778	0U 21 C13/12 C19 32A/200-240V/346-415V 3 Phase PDU with IEC60309 532P6 line cord
00YJ779	0U 21 C13/12 C19 48A/200-240V 3 Phase PDU with IEC60309 460P9 line cord
Switched and Monitored PDUs	
00YJ780	0U 20 C13/4 C19 Switched and Monitored 32A/200-240V/1Ph PDU w/ IEC60309 332P6 line cord
00YJ781	0U 20 C13/4 C19 Switched and Monitored 24A/200-240V/1Ph PDU w/ NEMA L6-30P line cord
00YJ782	0U 18 C13/6 C19 Switched / Monitored 32A/200-240V/346-415V/3Ph PDU w/ IEC60309 532P6 cord
00YJ783	0U 12 C13/12 C19 Switched and Monitored 48A/200-240V/3Ph PDU w/ IEC60309 460P9 line cord
46M4003	1U 9 C19/3 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
46M4004	1U 12 C13 Switched and Monitored DPI PDU (without line cord)
46M4005	1U 12 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
Ultra Density Enterprise PDUs (9x IEC 320 C13 + 3x IEC 320 C19 outlets)	
71762NX	Ultra Density Enterprise C19/C13 PDU Module (without line cord)
71763NU	Ultra Density Enterprise C19/C13 PDU 60A/208V/3ph with IEC 309 3P+Gnd line cord
C13 Enterprise PDUs (12x IEC 320 C13 outlets)	
39M2816	DPI C13 Enterprise PDU+ (without line cord)
39Y8941	DPI Single Phase C13 Enterprise PDU (without line cord)
C19 Enterprise PDUs (6x IEC 320 C19 outlets)	
39Y8948	DPI Single Phase C19 Enterprise PDU (without line cord)
39Y8923	DPI 60A 3 Phase C19 Enterprise PDU with IEC 309 3P+G (208 V) fixed line cord
Front-end PDUs (3x IEC 320 C19 outlets)	
39Y8938	DPI 30amp/125V Front-end PDU with NEMA L5-30P line cord
39Y8939	DPI 30amp/250V Front-end PDU with NEMA L6-30P line cord
39Y8934	DPI 32amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8940	DPI 60amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8935	DPI 63amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
NEMA PDUs (6x NEMA 5-15R outlets)	
39Y8905	DPI 100-127V PDU with Fixed NEMA L5-15P line cord
Line cords for PDUs that ship without a line cord	
40K9611	DPI 32a Line Cord (IEC 309 3P+N+G)
40K9612	DPI 32a Line Cord (IEC 309 P+N+G)
40K9613	DPI 63a Cord (IEC 309 P+N+G)
40K9614	DPI 30a Line Cord (NEMA L6-30P)
40K9615	DPI 60a Cord (IEC 309 2P+G)
40K9617	DPI Australian/NZ 3112 Line Cord
40K9618	DPI Korean 8305 Line Cord

For more information, see the Lenovo Press documents in the PDU category:
https://lenovopress.com/servers/options/pdu

Uninterruptible power supply units

The following table lists the uninterruptible power supply (UPS) units that are offered by Lenovo.

Table 55. Uninterruptible power supply units

Part number	Description
55941AX	RT1.5kVA 2U Rack or Tower UPS (100-125VAC)
55941KX	RT1.5kVA 2U Rack or Tower UPS (200-240VAC)
55942AX	RT2.2kVA 2U Rack or Tower UPS (100-125VAC)
55942KX	RT2.2kVA 2U Rack or Tower UPS (200-240VAC)
55943AX	RT3kVA 2U Rack or Tower UPS (100-125VAC)
55943KX	RT3kVA 2U Rack or Tower UPS (200-240VAC)
55945KX	RT5kVA 3U Rack or Tower UPS (200-240VAC)
55946KX	RT6kVA 3U Rack or Tower UPS (200-240VAC)
55948KX	RT8kVA 6U Rack or Tower UPS (200-240VAC)
55949KX	RT11kVA 6U Rack or Tower UPS (200-240VAC)
55948PX	RT8kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55949PX	RT11kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55943KT†	ThinkSystem RT3kVA 2U Standard UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55943LT†	ThinkSystem RT3kVA 2U Long Backup UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55946KT†	ThinkSystem RT6kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)
5594XKT†	ThinkSystem RT10kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)

† Only available in China and countries in the Asia Pacific region.

For more information, see the list of Product Guides in the UPS category:
https://lenovopress.com/servers/options/ups

Lenovo Financial Services

Lenovo Financial Services reinforces Lenovo's commitment to deliver pioneering products and services that are recognized for their quality, excellence, and trustworthiness. Lenovo Financial Services offers financing solutions and services that complement your technology solution anywhere in the world.

We are dedicated to delivering a positive finance experience for customers like you who want to maximize your purchase power by obtaining the technology you need today, protect against technology obsolescence, and preserve your capital for other uses.

We work with businesses, non-profit organizations, governments and educational institutions to finance their entire technology solution. We focus on making it easy to do business with us. Our highly experienced team of finance professionals operates in a work culture that emphasizes the importance of providing outstanding customer service. Our systems, processes and flexible policies support our goal of providing customers with a positive experience.

We finance your entire solution. Unlike others, we allow you to bundle everything you need from hardware and software to service contracts, installation costs, training fees, and sales tax. If you decide weeks or months later to add to your solution, we can consolidate everything into a single invoice.

Our Premier Client services provide large accounts with special handling services to ensure these complex transactions are serviced properly. As a premier client, you have a dedicated finance specialist who manages your account through its life, from first invoice through asset return or purchase. This specialist develops an in-depth understanding of your invoice and payment requirements. For you, this dedication provides a high-quality, easy, and positive financing experience.

For your region specific offers please ask your Lenovo sales representative or your technology provider about the use of Lenovo Financial Services. For more information, see the following Lenovo website:

https://www.lenovo.com/us/en/landingpage/lenovo-financial-services/

Related publications and links

For more information, see these resources:

- ThinkSystem SR530 product page
  https://www.lenovo.com/us/en/data-center/servers/racks/ThinkSystem-SR530/p/77XX7SRSR53
- Datasheet for the ThinkSystem SR530:
  https://lenovopress.com/ds0002-lenovo-thinksystem-sr530
- 3D Interactive Tour of the ThinkSystem SR530:
  https://lenovopress.com/lp0670-3d-tour-thinksystem-sr530
- Walkthrough Video for the ThinkSystem SR530:
  https://lenovopress.com/lp0744-thinksystem-sr530-server-video-walkthrough
- User Manuals for the ThinkSystem SR530:
  https://thinksystem.lenovofiles.com/help/topic/7X07/introduction.html?cp=4_2
  - Quick Start Guide
  - Setup Guide
  - Rack Installation Guides
  - Maintenance Manual
  - Messages and Codes Reference
  - UEFI Manual
- Lenovo Data Center Support Downloads - ThinkSystem SR530:
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x07/downloads
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x08/downloads
- Lenovo Hardware Installation & Removal Videos on the ThinkSystem SR530:
  - YouTube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
  - Youku: https://list.youku.com/albumlist/show/id_50437162
- Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com

Related product families

Product families related to this document are the following:

- 2-Socket Rack Servers
- ThinkSystem SR530 Server

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2021. All rights reserved.

This document, LP1045, was created or updated on March 2, 2021.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  http://lenovopress.com/LP1045
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at http://lenovopress.com/LP1045.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
Bootable Media Creator
Flex System
Lenovo Services
RackSwitch
System x®
ThinkSystem
TopSeller
TruDDR4
UpdateXpress System Packs
XClarity®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Hyper-V®, Microsoft®, PowerShell, Windows PowerShell®, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Lenovo ThinkSystem SR530 Server (Xeon SP Gen 2)

Product Guide

Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.

Featuring the second generation of the Intel Xeon Processor Scalable Family (Xeon SP Gen 2), the SR530 server offers a balance of performance, capacity and value. The SR530 server supports up to two processors, up to 768 GB of 2933 MHz TruDDR4 memory, 8x 2.5-inch or 4x 3.5-inch drive bays with an extensive choice of SAS/SATA SSDs and SAS/SATA HDDs, and flexible I/O expansion options with a LOM slot and up to 3x PCIe slots.

The SR530 server offers basic software RAID or advanced hardware RAID protection and a wide range of networking options, including embedded LOM, selectable LOM, ML2, and PCIe network adapters. The next-generation Lenovo XClarity Controller, which is built into the SR530 server, provides advanced service processor control, monitoring, and alerting functions.

The following figure shows the ThinkSystem SR530 server with 3.5-inch front hot-swap drives. Other drive configurations are also available.



Figure 1. Lenovo ThinkSystem SR530 with 3.5-inch hot-swap drives

Did you know?

The SR530 server delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies that can deliver 96% (Titanium) or 94% (Platinum) efficiency at 50% load when connected to a 200 - 240 V AC power source.

The SR530 server is designed to meet ASHRAE A4 standards (up to 45 °C) in select configurations, which enable customers to lower energy costs, while still maintaining world-class reliability.

Key features

The SR530 server offers a balance of processing power, expandability, and cost for small and medium businesses up to the large enterprise. Ease of use and comprehensive systems management tools help make deployment easier and efficient design improves your business environment and helps save operational costs.

Scalability and performance

The SR530 server offers numerous features to boost performance, improve scalability, and reduce costs:

- Improves productivity by offering superior system performance with the second generation of the Intel Xeon Processor Scalable Family with up to 22-core processors, up to 30.25 MB of last level cache (LLC), up to 2933 MHz memory speeds, and up to 10.4 GT/s Ultra Path Interconnect (UPI) links.
    - Support for up to two processors, 44 cores, and 88 threads allows to maximize the concurrent execution of multithreaded applications.
    - Intelligent and adaptive system performance with energy efficient Intel Turbo Boost 2.0 Technology allows CPU cores to run at maximum speeds during peak workloads by temporarily going beyond processor thermal design power (TDP).
    - Intel Hyper-Threading Technology boosts performance for multithreaded applications by enabling simultaneous multithreading within each processor core, up to two threads per core.
    - Intel Virtualization Technology integrates hardware-level virtualization hooks that allow operating system vendors to better utilize the hardware for virtualization workloads.
    - Intel Speed Select Technology provides improvements in server utilization and guaranteed per-core performance service levels with more granular control over processor performance.
    - Intel Deep Learning Boost (Vector Neural Network Instruction set [VNNI]) is designed to deliver significant, more efficient Deep Learning (Inference) acceleration for high-performance Artificial Intelligence (AI) workloads.
    - Intel Advanced Vector Extensions 512 (AVX-512) enable acceleration of enterprise-class and high performance computing (HPC) workloads.
- Helps maximize system performance for data intensive applications with up to 2933 MHz memory speeds and up to 768 GB of memory capacity.
- Offers flexible and scalable internal storage in a 1U rack form factor with up to 8x 2.5-inch drives for performance-optimized configurations or up to 4x 3.5-inch drives for capacity-optimized configurations, providing a wide selection of SAS/SATA HDDs/SSDs.
- Provides I/O scalability with a LOM slot and up to three PCI Express (PCIe) 3.0 I/O expansion slots in a 1U rack form factor.
- Reduces I/O latency and increases overall system performance with Intel Integrated I/O Technology that embeds the PCI Express 3.0 controller into the Intel Xeon Processor Scalable Family.

Availability and serviceability

The SR530 server provides many features to simplify serviceability and increase system uptime:

- Offers protection in the event of a non-correctable memory failure with Single Device Data Correction (SDDC, also known as Chipkill, requires x4-based DIMMs), Adaptive Double Device Data Correction (ADDDC, also known as Redundant Bit Steering [RBS], requires x4-based DIMMs and Intel Xeon Gold or Platinum processors), memory mirroring, and memory rank sparing.
- Provides easy access to upgrades and serviceable parts (such as processors, memory DIMMs, and adapter cards) with tool-less cover removal.
- Offers affordable data protection with software RAID and Simple Swap drives and advanced hardware RAID data redundancy with hot-swap drives.
- Provides availability for applications with redundant hot-swap power supplies and redundant non-hot-swap fans.
- Speeds up troubleshooting tasks to reduce service time with diagnostics built into the XClarity Provisioning Manager.

- Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
- Continuously monitors system parameters, triggers alerts, and performs recovery actions in case of failure to minimize downtime with Built-in XClarity Controller (XCC).
- Provides quick access to system status, firmware, network, health, and alerts information via Virtual Operator Panel from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access.

Manageability and security

Powerful systems management features simplify local and remote management of the SR530 server and deliver enterprise-class data protection:

- Provides advanced service processor control, monitoring, and alerting functions with XClarity Controller, a next generation service processor.
- Improves Unified Extensible Firmware Interface (UEFI) system setup, configuration, updates, simplified error handling, and operating system deployment with the embedded XClarity Provisioning Manager.
- Offers XClarity Essentials software tools that can help you set up, use, and maintain the server.
- Increases uptime, reduces costs, and improves productivity through advanced server management capabilities with Lenovo XClarity Administrator that provides comprehensive hardware management.
- Provides on-the-go monitoring and management of devices in XClarity Administrator from anywhere with the Lenovo XClarity mobile app, which can help improve efficiency and reduce downtime risks.
- Centralizes infrastructure resource management with Lenovo XClarity Integrators for VMware vCenter and Microsoft System Center, extending XClarity Administrator features to virtualization management software tools and enabling users to deploy and manage infrastructure end-to-end.
- Offers advanced cryptographic functionality (such as digital signatures and remote attestation) with an integrated Trusted Platform Module (TPM) or optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC).
- Keeps user data safe with Lenovo Business Vantage, a security software tool suite designed to work with the Trusted Cryptographic Module (available only in PRC).
- Offers enterprise-class data protection with advanced RAID and optional self-encrypting drives.
- Provides faster, stronger encryption with industry-standard AES NI support.
- Helps prevent certain classes of malicious buffer overflow attacks with Intel Execute Disable Bit functionality, when combined with a supporting operating system.
- Enhances security through hardware-based resistance to malicious software attacks with Intel Trusted Execution Technology, allowing an application to run in its own isolated space, protected from all other software running on a system.

Energy efficiency

The SR530 server offers the following energy-efficiency features to save energy, reduce operational costs, increase energy availability, and contribute to the green environment:

- Delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies.
- Enables customers to lower energy costs with design to meet ASHRAE A4 standards in select configurations.
- Reduces power drawn with Intel Intelligent Power Capability that powers individual processor elements on and off as needed.
- Helps reduce power consumption with variable speed fans.
- Helps achieve lower heat output and reduced cooling needs with Lenovo XClarity Energy Manager that provides advanced data center power notification, analysis, and policy-based management.

Components and connectors

The following figure shows the front of the SR530 server with four 3.5-inch drive bays.

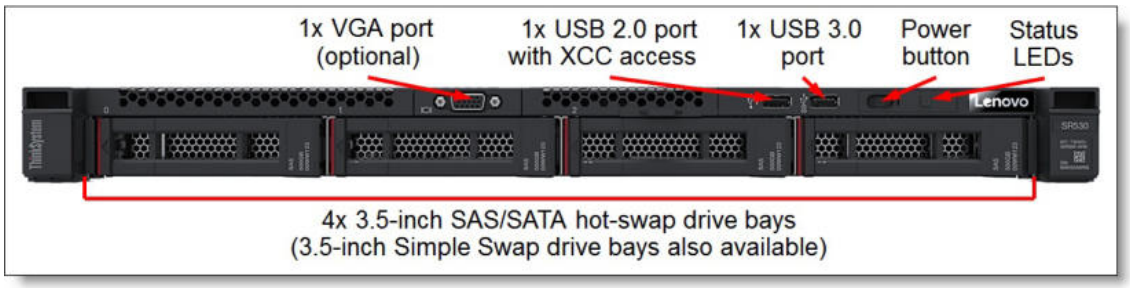


Figure 2. Front view of the SR530: 4x 3.5-inch drive bays

The following figure shows the front of the SR530 server with eight 2.5-inch drive bays.

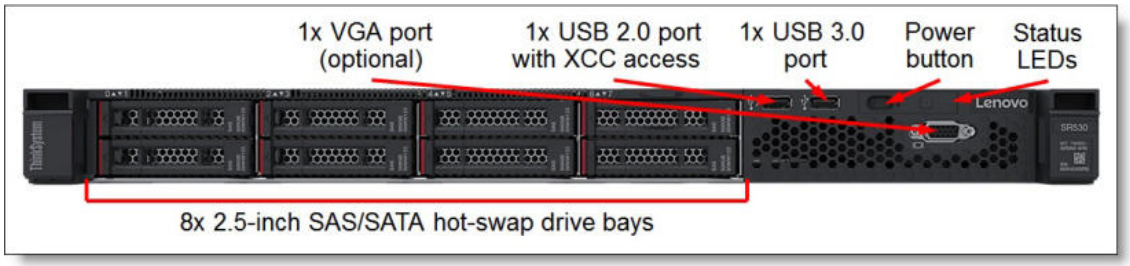


Figure 3. Front view of the SR530: 8x 2.5-inch drive bays

The front of the SR530 server includes the following components:

- Up to 8x 2.5-inch or 4x 3.5-inch hot-swap drive bays, or 4x 3.5-inch Simple Swap drive bays.
- One VGA port (optional).
- One USB 3.0 port.
- One USB 2.0 port with XClarity Controller access.
- Power button.
- Status LEDs.

The following figure shows the rear of the SR530 server with three PCIe low profile slots.

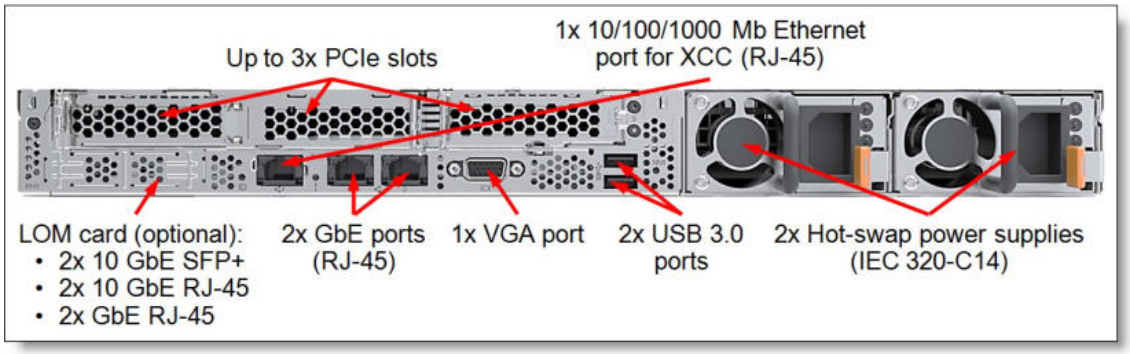


Figure 4. Rear view of the SR530

The rear of the SR530 server includes the following components:

- Up to three PCIe expansion slots (depending on the riser cards selected).
- One LOM card slot.
- One 1 GbE port for XClarity Controller.
- One VGA port.
- Two USB 3.0 ports.
- Up to two hot-swap power supplies.

The following figure shows the locations of key components inside the SR530 server.

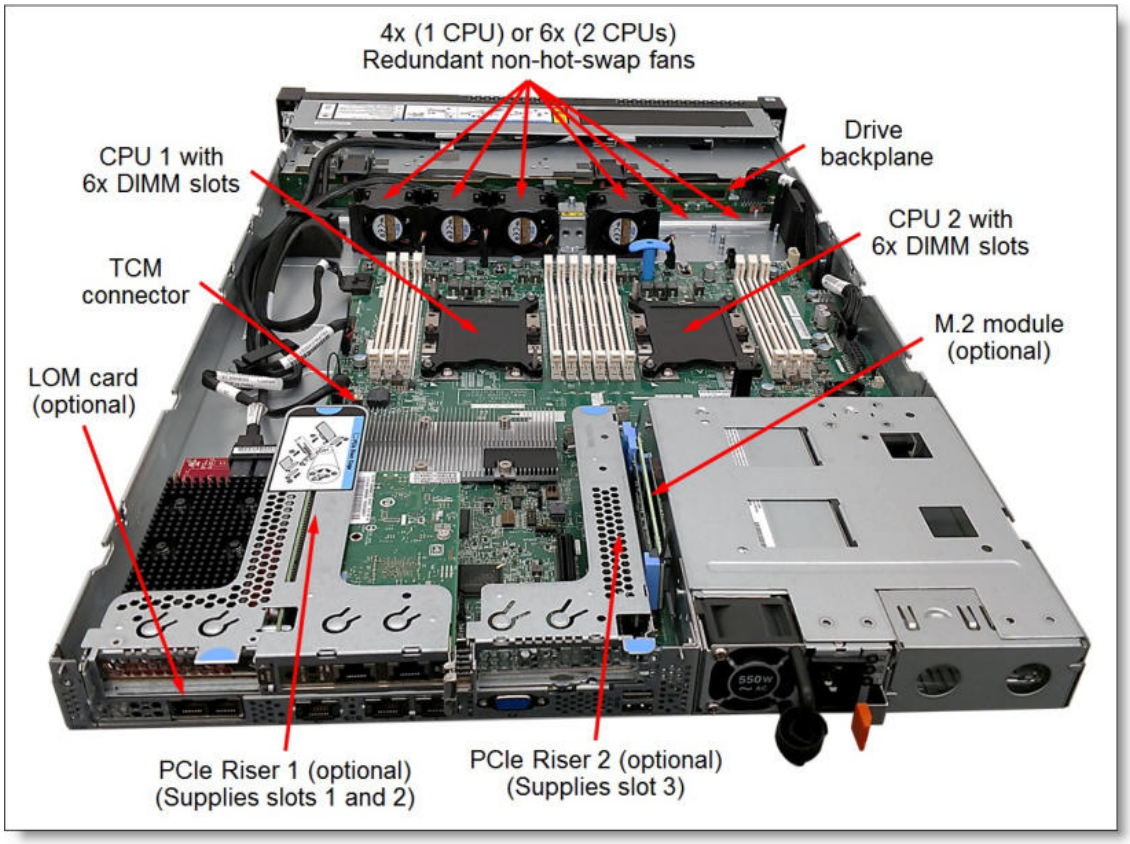


Figure 5. Internal view of the SR530

The following key components are located inside the SR530 server:

- Up to two processors.
- 12 DIMM slots (6 DIMM slots per processor).
- Drive backplanes.
- One M.2 module connector.
- One LOM card connector.
- Two slots for PCIe riser cards.
- One TCM connector.
- Four (one processor) or six (two processors) non-hot-swap system fans.

System specifications

The following table lists the system specifications for the SR530 server.

Table 1. SR530 system specifications

Attribute	Specification
Machine types	7X07 - 1 year warranty 7X08 - 3 year warranty
Form factor	1U rack-mount.
Processor	Up to two Intel Xeon Gen 2 Bronze, Silver, Gold, or Platinum processors: • Up to 22 cores (1.9 GHz core speeds) • Up to 3.8 GHz core speeds (4 cores) • Two UPI links up to 10.4 GT/s each • Up to 30.25 MB cache • Up to 2933 MHz memory speed

Attribute	Specification
Chipset	Intel C622.
Memory	Up to 12 DIMM sockets (6 DIMMs per processor; six memory channels per processor with one DIMM per channel) with support for the following TruDDR4 RDIMM types and capacities: • 8 GB, 16 GB, 32 GB, and 64 GB 2933 MHz. • 16 GB and 32 GB 2666 MHz.
Memory protection	Error correction code (ECC), SDDC (for x4-based memory DIMMs), ADDDC (for x4-based memory DIMMs, requires Intel Xeon Gold or Platinum processors), memory mirroring, memory rank sparing, patrol scrubbing, and demand scrubbing.
Memory capacity	Up to 768 GB with 12x 64 GB RDIMMs (Up to 384 GB per processor).
Drive bays	• 4 LFF SATA Simple Swap drive bays • 4 LFF SAS/SATA hot-swap drive bays • 8 SFF SAS/SATA hot-swap drive bays

Internal storage capacity	• 2.5-inch drives:
	  ◦ 122.88TB using 8x 15.36TB 2.5-inch SAS/SATA SSDs
	  ◦ 19.2TB using 8x 2.4TB 2.5-inch HDDs
	• 3.5-inch drives:
	  ◦ 72TB using 4x 18TB 3.5-inch HDDs
	  ◦ 30.72TB using 4x 7.68TB 3.5-inch SAS/SATA SSDs

Storage controller	6 Gbps SATA
	• Non-RAID: Onboard SATA AHCI
	• RAID 0/1/10/5: Onboard SATA RAID (Intel RSTe)
	
	12 Gbps SAS/6 Gbps SATA RAID
	• RAID 0/1/10/5/50:
	  ◦ RAID 530-8i
	  ◦ RAID 730-8i 1GB Cache
	• RAID 0/1/10/5/50/6/60:
	  ◦ RAID 730-8i 2GB Flash
	  ◦ RAID 930-8i 2GB Flash
	  ◦ RAID 930-16i 4GB or 8GB Flash
	
	12 Gbps SAS/6 Gbps SATA non-RAID: 430-8i HBA

Optical drive bays	None. Support for an external USB DVD RW Optical Disk Drive (SeeOptical drives).

Network interfaces	• 2x Integrated 1 GbE RJ-45 ports (no 10/100 Mb support)
	• Onboard LOM slot for up to two additional 1/10 Gb Ethernet ports:
	  ◦ 2x 1 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE SFP+ ports (no 10/100 Mb support)
	• Optional Mezzanine LOM (ML2) slot for dual-port 10 GbE cards with SFP+ or RJ-45 connectors.
	• 1x RJ-45 10/100/1000 Mb Ethernet systems management port.

I/O expansion slots	Up to three slots depending on the riser cards installed. The slots are as follows: • Slot 1: PCIe 3.0 x8; low profile • Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length • Slot 3: PCIe 3.0 x8 or x16; low profile PCIe x16 slot 3 requires the second processor to be installed.
Ports	• Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. • Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
Cooling	Four (one processor) or six (two processors) non-hot-swap system fans with N+1 redundancy.
Power supply	Up to two redundant hot-swap 550 W or 750 W (100 - 240 V) High Efficiency Platinum or 750 W (200 - 240 V) High Efficiency Titanium AC power supplies. HVDC support (PRC only).

Attribute	Specification
Video	Matrox G200 with 16 MB memory integrated into the XClarity Controller. Maximum resolution is 1920x1200 at 60 Hz with 32 bits per pixel.
Hot-swap parts	Drives (select models) and power supplies.
Systems management	XClarity Controller (XCC) Standard, Advanced, or Enterprise (Pilot 4 chip), proactive platform alerts, XClarity Provisioning Manager, XClarity Essentials, XClarity Administrator, XClarity Integrators for VMware vCenter and Microsoft System Center, XClarity Energy Manager, Capacity Planner.
Security features	Power-on password, administrator's password, secure firmware updates, Trusted Platform Module (TPM) 1.2 or 2.0 (configurable UEFI setting). Optional lockable front bezel. Optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC). Optional Lenovo Business Vantage security software (available only in PRC).
Operating systems	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. See the Operating systems section for specifics.
Warranty	One-year (7X07) or three-year (7X08) customer-replaceable unit (CRU) and onsite limited warranty with 9x5 Next Business Day Parts Delivered.
Service and support	Optional service upgrades are available through Lenovo Services: 2-hour or 4-hour response time, 6-hour or 24-hour committed service repair, warranty extension up to 5 years, 1-year or 2-year post-warranty extensions, YourDrive Your Data, Enterprise Software Support, and Basic Hardware Installation Services.
Dimensions	Width: 435 mm (17.1 in.), height: 43 mm (1.7 in.), depth: 750 mm (29.5 in.). See Physical specifications for details.
Weight	Minimum configuration: 10.2 kg (22.5 lb), maximum: 16 kg (35.3 lb)

Models

ThinkSystem SR530 models can be configured by using the Lenovo Data Center Solution Configurator (DCSC).

Configure-to-order (CTO) models are used to create models with factory-integrated server customizations. For CTO models, two base CTO models are available for the SR530 as listed in the following table, CTO1WW and CTOLWW:

- The CTO1WW base CTO model is for general business and is selectable by choosing **General Purpose** mode in DCSC.
- The CTOLWW base model is intended for High Performance Computing (HPC) and Artificial Intelligence (AI) configurations and solutions, including configurations for Lenovo Scalable Infrastructure (LeSI), and is enabled using either the **HPC & AI LeSI Solutions** mode or **HPC & AI ThinkSystem Hardware** mode in DCSC. CTOLWW configurations can also be built using System x and Cluster Solutions Configurator (x-config).

Preconfigured server models may also be available for the SR530, however these are region-specific; that is, each region may define their own server models, and not all server models are available in every region.

The following table lists the base CTO models of the ThinkSystem SR530 server.

Table 2. Base CTO models

Description	Machine Type/Model General purpose	Machine Type/Model for HPC and AI
ThinkSystem SR530 - 3 year Warranty	7X08CTO1WW	7X08CTOLWW
ThinkSystem SR530 - 1 year Warranty	7X07CTO1WW	7X07CTOLWW

The following table lists the base chassis for CTO models of the SR530 server.

Table 3. Base chassis for CTO models

Feature code	Description
AV0T	ThinkSystem SR530 3.5" Chassis with 4 Bays
AV0S	ThinkSystem SR530 2.5" Chassis with 8 Bays

All models of the SR530 server are shipped with the following items:

- *Rack Installation Guide*
- *Electronic Publications Flyer*

Models table conventions: The model tables shown in this section use the following conventions:

- XClarity Controller: "S" = Standard, "A" = Advanced, "E" = Enterprise.
- Front VGA port: "Y" = Included; "N" = Not included, optional.
- Tool-less Rail Kit: "Y" = Included; "N" = Not included, optional.
- Cable Management Arm (CMA): "Y" = Included; "N" = Not included, optional.
- Power cord:
  - "R1" = 1.5 m C13-C14 rack power cable.
  - "R2" = 2.8 m C13-C14 rack power cable.
  - "L2" = 2.8 m line cord.
  - "N" = Not included; see Power supplies and cables for the ordering information.

The following tables list the models of the SR530 server for the following regions:

- Brazil
- Latin America (except Brazil)
- Europe, Middle East, and Africa (EMEA)
- India
- Hong Kong, Taiwan, Korea
- Japan
- Association of Southeast Asian Nations (ASEAN)
- Australia and New Zealand

Table 4. SR530 server models: Brazil

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Brazil													
7X08A0A1BR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
TopSeller models - Brazil													
7X08100QBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x SATA AHCI	4 / 4 SS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A0A2BR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
7X08A09YBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09ZBR	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0APBR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 5. SR530 server models: Latin America (except Brazil)

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
TopSeller models - Latin America (except Brazil)													
7X08A09WLA	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09XLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0AQLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	Y	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 6. SR530 server models: EMEA

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - EMEA													
7X08A0ACEA	1x 3206R 8C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	R2
7X08A075EA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AZEA	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	None	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	N	R2
7X08A0ADEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AHEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A078EA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A06WEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A07FEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AEEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AJEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A07CEA	1x 4214 12C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AKEA	1x 4214R 12C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A070EA	1x 4216 16C 100W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0ALEA	1x 5218R 20C 125W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 7. SR530 server models: India

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - India													
7X08A08TSG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07USG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A07WSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A084SG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07YSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A079SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06VSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07SSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07JSG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ASG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08PSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A098SG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A077SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A095SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07RSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08VSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08WSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06USG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A094SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A089SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ESG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08KSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 8. SR530 server models: Hong Kong, Taiwan, Korea

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Hong Kong, Taiwan, Korea													
7X08A09CCN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085CN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08100VCN	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	Y	N	Y
7X08A071CN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YCN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09BCN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080CN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CCN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A082CN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09DCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07NCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A088CN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GCN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A087CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08MCN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092CN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06XCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07KCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 9. SR530 server models: Japan

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Japan													
7X08A0AWJP	1x 5218R 20C 125W 2.1GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
TopSeller models - Japan													
7X08A08AJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08DJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08EJP	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07HJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08SJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08QJP	1x 4214 12C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07QJP	1x 4215 8C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07LJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07MJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08HJP	1x 5215 10C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08FJP	1x 5217 8C 115W 3.0GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08YJP	1x 5218 16C 125W 2.3GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A090JP	1x 5220 18C 125W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08UJP	1x 5222 4C 105W 3.8GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A096JP	1x 6230 20C 125W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A0AXJP	1x 3206R 8C 85W 1.9GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AYJP	1x 4210R 10C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AVJP	1x 4214R 12C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 10. SR530 server models: ASEAN

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - ASEAN													
7X08A099SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A086SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A081SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ZSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A083SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A093SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07VSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ESG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RSG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A073SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A097SG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07PSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07TSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09FSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A091SG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 11. SR530 server models: Australia and New Zealand

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Australia and New Zealand (1-year warranty)													
7X07A00VAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	None	No bays / 8 HS SFF	Open bay	Open slot	None	1x 550W	S	Y	Y	N	R2
Relationship models - Australia and New Zealand (3-year warranty)													
7X08A099AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A071AU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YAU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XAU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080AU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A0B0AU	1x 4216 16C 100W 2.1GHz	1x 32GB(x4) 2933MHz	1x RAID 930-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W Platinum	E	Y	Y	N	Y
7X08A07VAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07EAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076AU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BAU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LAU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092AU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A06XAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
TopSeller models - Australia and New Zealand (3-year warranty)													
7X08A09GAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09HAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09LAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09KAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09NAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09MAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09JAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Processors

The SR530 server supports one or two Intel Xeon Bronze, Silver, Gold, or Platinum processors of up to 125 W TDP. The following table lists the specifications of the processors for the SR530 server.

Processor specifications table abbreviations:

- UPI: Ultra Path Interconnect
- TDP: Thermal Design Power
- HT: Hyper-Threading
- TB: Turbo Boost 2.0
- VT-x: Virtualization Technology
- VT-d: Virtualization Technology for Directed I/O
- SST-PP: Speed Select Technology - Performance Profile
- FMA: Fused-Multiply Add (AVX-512)
- RAS: Reliability, Availability, and Serviceability
    - Std: Standard RAS
    - Adv: Advanced RAS

Table 12. Processor specifications

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
Intel Xeon Bronze processors														
3204	6 / 6	1.9 / 1.9 GHz	8.25 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	Std

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
3206R	8 / 8	1.9 / 1.9 GHz	11 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	
Intel Xeon Silver processors														
4208	8 / 16	2.1 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4209T	8 / 16	2.2 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	70 W	Y	Y	Y	Y	N	1	Std
4210	10 / 20	2.2 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4210R	10 / 20	2.4 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4214R	12 / 24	2.4 / 3.5 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214Y	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	Y	1	Std
	10 / 20	2.3 / 3.2 GHz												
	8 / 16	2.4 / 3.2 GHz												
4215	8 / 16	2.5 / 3.5 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4216	16 / 32	2.1 / 3.2 GHz	22 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
Intel Xeon Gold processors														
5215	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	1 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5215L	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	4.5 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5217	8 / 16	3.0 / 3.7 GHz	11 MB	2666 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	1	Adv
5218	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218B	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218R	20 / 40	2.1 / 4.0 GHz	27.5 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218T	16 / 32	2.1 / 3.8 GHz	22 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5220	18 / 36	2.2 / 3.9 GHz	24.75 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220S	18 / 36	2.7 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220T	18 / 36	1.9 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5222	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv
6209U	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	N/A	125 W	Y	Y	Y	Y	N	2	Adv
6222V	20 / 40	1.8 / 3.6 GHz	27.5 MB	2400 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	2	Adv
6226	12 / 24	2.7 / 3.7 GHz	19.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230N	20 / 40	2.3 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230T	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6238T	22 / 44	1.9 / 3.7 GHz	30.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
Intel Xeon Platinum processors														
8253	16 / 32	2.2 / 3.0 GHz	22 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
8256	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv

Configuration notes:

- The Intel Xeon Gold 5218 and 5218B processors have similar specifications; however, they use different silicon designs and cannot be mixed in the same system.
- The processors that support SST-PP offer three distinct operating points that are defined by a core count with a base speed associated with that core count. The operating point is static, it is selected during the boot process and cannot be changed at runtime.

For the SR530 server models that come with one processor, the second processor can be ordered, if required (see the following table for ordering information). The second processor must be of the same model as the first processor. The second processor option includes a processor and a heatsink; two additional system fans are not included and need to be purchased with the second processor (see Cooling for details).

Table 13. Processor options

Description	Part number	Feature code*
Intel Xeon Bronze processors		
SR530/SR570/SR630 Intel Xeon Bronze 3204 6C 85W 1.9GHz Processor w/o FAN	4XG7A37939	B4HU
SR530/SR570/SR630 Intel Xeon Bronze 3206R 8C 85W 1.9GHz Processor w/o FAN	4XG7A37990	B7N3
Intel Xeon Silver processors		
SR530/SR570/SR630 Intel Xeon Silver 4208 8C 85W 2.1GHz Processor w/o FAN	4XG7A37936	B4HT
SR530/SR570/SR630 Intel Xeon Silver 4209T 8C 70W 2.2GHz Processor w/o FAN	4XG7A37945	B4P4
SR530/SR570/SR630 Intel Xeon Silver 4210 10C 85W 2.2GHz Processor w/o FAN	4XG7A37933	B4HS
SR530/SR570/SR630 Intel Xeon Silver 4210R 10C 100W 2.4GHz Processor w/o FAN	4XG7A37988	B7N5
SR530/SR570/SR630 Intel Xeon Silver 4214 12C 85W 2.2GHz Processor w/o FAN	4XG7A37930	B4HR
SR530/SR570/SR630 Intel Xeon Silver 4214R 12C 100W 2.4GHz Processor w/o FAN	4XG7A37987	B7N6
SR530/SR570/SR630 Intel Xeon Silver 4214Y 12/10/8C 85W 2.2GHz Processor w/o FAN	4XG7A37942	B4NW
SR530/SR570/SR630 Intel Xeon Silver 4215 8C 85W 2.5GHz Processor w/o FAN	4XG7A37927	B4HQ
SR530/SR570/SR630 Intel Xeon Silver 4216 16C 100W 2.1GHz Processor w/o FAN	4XG7A37924	B4HP
Intel Xeon Gold processors		
SR530/SR570/SR630 Intel Xeon Gold 5215 10C 85W 2.5GHz Processor w/o FAN	4XG7A37917	B4HN
SR530/SR570/SR630 Intel Xeon Gold 5215L 10C 85W 2.5GHz Processor w/o FAN	4XG7A37911	B4P9
SR530/SR570 Intel Xeon Gold 5217 8C 115W 3.0GHz Processor w/o FAN	4XG7A37921	B4HM
SR530/SR570/SR630 Intel Xeon Gold 5218 16C 125W 2.3GHz Processor w/o FAN	4XG7A37896	B4HL
SR530/SR570/SR630 Intel Xeon Gold 5218B 16C 125W 2.3GHz Processor w/o FAN	4XG7A37959	B6BS
SR530/SR570/SR630 Intel Xeon Gold 5218R 20C 125W 2.1GHz Processor w/o FAN	4XG7A63296	BAZS
SR530/SR570 Intel Xeon Gold 5218T 16C 105W 2.1GHz Processor w/o FAN	4XG7A38017	B4P3
SR530/SR570/SR630 Intel Xeon Gold 5220 18C 125W 2.2GHz Processor w/o FAN	4XG7A37893	B4HK
SR530/SR570/SR630 Intel Xeon Gold 5220S 18C 125W 2.7GHz Processor w/o FAN	4XG7A38018	B6CW
SR530/SR570 Intel Xeon Gold 5220T 18C 105W 1.9GHz Processor w/o FAN	4XG7A38004	B6CQ
SR530/SR570 Intel Xeon Gold 5222 4C 105W 3.8GHz Processor w/o FAN	4XG7A37953	B5S1
Intel Xeon Gold 6209U 20C 125W 2.1GHz Processor	None**	B6CX
SR530/SR570/SR630 Intel Xeon Gold 6222V 20C 115W 1.8GHz Processor w/o FAN	4XG7A38022	B6CV
SR530/SR570/SR630 Intel Xeon Gold 6226 12C 125W 2.7GHz Processor w/o FAN	4XG7A38020	B6CL
SR530/SR570/SR630 Intel Xeon Gold 6230 20C 125W 2.1GHz Processor w/o FAN	4XG7A37890	B4HJ
SR530/SR570 Intel Xeon Gold 6230N 20C 125W 2.3GHz Processor w/o FAN	4XG7A38029	B5RY
SR530/SR570 Intel Xeon Gold 6230T 20C 125W 2.1GHz Processor w/o FAN	4XG7A38007	B6CP
SR530/SR570 Intel Xeon Gold 6238T 22C 125W 1.9GHz Processor w/o FAN	4XG7A37908	B4P2
Intel Xeon Platinum processors		
SR530/SR570/SR630 Intel Xeon Platinum 8253 16C 125W 2.2GHz Processor w/o FAN	4XG7A37899	B5RZ
SR530/SR570 Intel Xeon Platinum 8256 4C 105W 3.8GHz Processor w/o FAN	4XG7A37949	B5S2

* For CTO configurations, the feature code represents a processor, and fans and heatsinks are derived by the configuration tool.
** Factory-installed only; no field upgrade. Supported in the uniprocessor configurations only.

Memory

The SR530 server supports up to 6 TruDDR4 memory RDIMMs when one processor is installed and up to 12 RDIMMs when two processors are installed for a total of up to 768 GB of memory capacity (up to 384 TB per processor). Each processor has six memory channels, and there is a one DIMM per channel.

Lenovo TruDDR4 memory uses the highest-quality components sourced from Tier 1 DRAM suppliers and only memory that meets strict requirements is selected. It is compatibility tested and tuned on every ThinkSystem server to maximize performance and reliability.

TruDDR4 memory has a unique signature programmed into the DIMM, which enables Lenovo servers to verify whether the memory installed is qualified and supported. Lenovo qualified and supported TruDDR4 memory is covered by Lenovo warranty, and service and support provided worldwide.

The following memory protection technologies are supported by the processor's integrated memory controllers:

- ECC
- SDDC (for x4-based memory DIMMs)
- ADDDC (for x4-based memory DIMMs; Gold and Platinum processors only)
- Memory mirroring
- Memory rank sparing
- Patrol scrubbing
- Demand scrubbing

The following table lists memory options available for the SR530 server.

Table 14. Memory options

Description	Part number	Feature code	Maximum quantity*
RDIMMs - 2933 MHz			
ThinkSystem 8GB TruDDR4 2933MHz (1Rx8 1.2V) RDIMM	4ZC7A08706	B4H1	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (1Rx4 1.2V) RDIMM	4ZC7A08707	B4LY	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (2Rx8 1.2V) RDIMM	4ZC7A08708	B4H2	6 / 12
ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08709	B4H3	6 / 12
ThinkSystem 64GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08710	B4H4	6 / 12
RDIMMs - 2666 MHz			
ThinkSystem 16GB TruDDR4 2666 MHz (1Rx4 1.2V) RDIMM	7X77A01302	AUNB	6 / 12
ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM	7X77A01303	AUNC	6 / 12
ThinkSystem 32GB TruDDR4 2666 MHz (2Rx4 1.2V) RDIMM	7X77A01304	AUND	6 / 12

* The maximum quantity shown is with one processor / two processors.

Configuration notes:

- All RDIMMs in the server operate at the same speed, which is determined as the lowest value of:
  - RDIMM rated speed (2666 MHz or 2933 MHz).
  - Memory speed supported by the specific processor (2133 MHz, 2400 MHz, 2666 MHz, or 2933 MHz).

  Note: Maximum memory speed can be achieved when Max performance mode is enabled in UEFI.
- Mixing RDIMMs of different ranks (single- or dual-rank), DRAM chip types (x4 or x8), speeds (2666 MHz or 2933 MHz), and capacities (8 GB, 16 GB, 32 GB, or 64 GB) is supported in the independent channel mode (the default operational mode).
- For server configurations with memory protection, the following rules apply:
  - Single Device Data Correction (SDDC) works only in the independent channel mode and supports only x4-based memory DIMMs.
  - Adaptive Double Device Data Correction (ADDDC) works with x4-based memory DIMMs and requires two DIMM ranks per channel, Intel Xeon Gold or Platinum processors, and the Closed Page memory access mode.
  - If memory mirroring is used, then DIMMs must be installed in quantities of 2 or 4 per processor for mirroring across two memory channels, or in quantities of 3 or 6 per processor for mirroring across three memory channels. Mixing two- and three-channel mirroring in the server is allowed (one processor uses two-channel mirroring, and another processor uses three-channel mirroring). All DIMMs in the server must be identical in type and size.
  - If memory rank sparing is used, then a minimum of two ranks must be installed per populated channel (a least one dual-rank or quad-rank DIMM; single-rank DIMMs are not supported). With rank sparing, one rank in each populated channel is reserved as spare memory for other ranks on the same channel. All DIMMs in the server must be identical in type and size.
  - SDDC, memory mirroring, and memory rank sparing modes are mutually exclusive. Only one operational memory mode can be enabled on the server.

Internal storage

The SR530 server supports the following internal drive bay configurations:

1. 4 LFF SATA Simple Swap drive bays
2. 4 LFF SAS/SATA hot-swap drive bays
3. 8 SFF SAS/SATA hot-swap drive bays

In addition, the SR530 server models can be configured with one or two internal M.2 SATA SSDs. The server also supports configurations without drive bays.

The following figure shows the internal drive bay configurations.

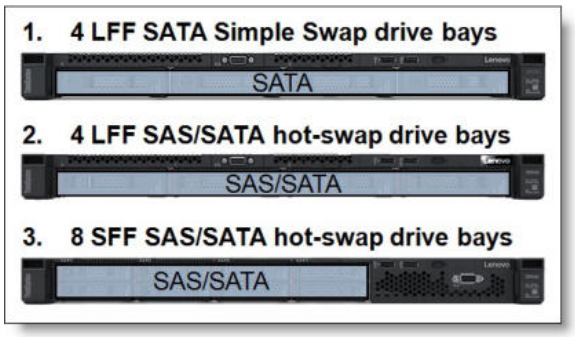


Figure 6. Internal drive bay configurations

The following table lists the internal storage options for the SR530 server.

Table 15. Internal storage options

Description	Part number	Feature code	Maximum quantity
Factory-installed backplane kits			
ThinkSystem 1U 3.5" SATA/SAS 4-Bay Backplane	None*	AUW8	1
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane	None*	AUWB	1
Backplane kit field upgrade options			
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane Kit	7XH7A05896	None**	1
M.2 enablement kits			
ThinkSystem M.2 Enablement Kit	7Y37A01092	AUMU	1
ThinkSystem M.2 with Mirroring Enablement Kit	7Y37A01093	AUMV	1

* These backplane kits can be factory-installed in standard or custom (CTO or Special Bid) models, and they might not have an option part number assigned.
** Field upgrade only; used for upgrading models without any drive bays to 8x 2.5" SAS/SATA hot-swap drive bays.

M.2 Enablement Kit configuration notes:

- The M.2 Enablement Kit (7Y37A01092) supports one M.2 SATA SSD which is connected to the SATA port on the Intel Platform Controller Hub (PCH).
- The M.2 with Mirroring Enablement Kit (7Y37A01093) is connected to the Intel PCH via the PCIe link, and the kit supports two M.2 SATA SSDs that can be configured in a RAID-1 or RAID-0 drive group, or they can operate as two separate drives.

The following tables list supported internal storage configurations with the SAS/SATA backplanes.

Table 16. Internal storage configurations

Drive bay configuration	Backplane kit type and quantity		Storage controller type and quantity*
	4x 3.5" SATA/SAS	8x 2.5" SATA/SAS	
4x 3.5" chassis (Feature code AV0T)			
4x 3.5-in. SATA Simple Swap	0	0	Onboard AHCI (non-RAID) / Intel RSTe (RAID) (4)
4x 3.5-in. SAS/SATA hot-swap	1	0	1x RAID 530-8i/730-8i 1GB (4)
			1x RAID 730-8i 2GB/930-8i (4)
			1x 430-8i HBA (4)
8x 2.5" chassis (Feature code AV0S)			
8x 2.5-in. SAS/SATA hot-swap	0	1	1x RAID 530-8i/730-8i 1GB (8)
			1x RAID 730-8i 2GB/930-8i/930-16i (8)
			1x 430-8i HBA (8)

* The number in brackets (x) specifies the quantity of drive bays connected to each of the controllers.

Configuration note: Models without any drive bays are based on the 8x 2.5" chassis (feature code AV0S), and they support adding drive bays by using the 2.5" 8-drive backplane kit (7XH7A05896).

Controllers for internal storage

The following table lists the storage controllers and options for internal storage of the SR530 server.

Table 17. RAID controllers and HBAs for internal storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
6 Gbps SATA controllers				
Onboard AHCI (non-RAID) / Intel RSTe (RAID)	Onboard*	Onboard*	1	-
12 Gb SAS/SATA RAID controllers				
ThinkSystem RAID 530-8i PCIe 12Gb Adapter	7Y37A01082	AUNG	1	1
ThinkSystem RAID 730-8i 1GB Cache PCIe 12Gb Adapter	7Y37A01083	AUNH	1	1
ThinkSystem RAID 730-8i 2GB Flash PCIe 12Gb Adapter	4Y37A09722	B4RQ	1	1
ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter	7Y37A01084	AUNJ	1	1
ThinkSystem RAID 930-16i 4GB Flash PCIe 12Gb Adapter	7Y37A01085	AUNK	1	1
ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter	4Y37A09721	B31E	1	1
12 Gb SAS/SATA non-RAID HBAs				
ThinkSystem 430-8i SAS/SATA 12Gb HBA	7Y37A01088	AUNL	1	1

* The onboard SATA controller integrated into the Intel C622 Platform Controller Hub (PCH) supports non-RAID (JBOD) AHCI mode or a hardware-assist, software RAID feature (Intel Rapid Storage Technology Enterprise [RSTe]).

Configuration note: Low profile SAS RAID controllers and HBAs for internal storage are supported in the PCIe x8 slot 1 supplied by the riser card 1.

The following table summarizes features of supported SAS/SATA storage controllers.

Table 18. Storage controller features and specifications (LP = Low profile, FHHL = Full-height half-length)

Feature	Intel RSTe	RAID 530-8i	RAID 730-8i 1GB	RAID 730-8i 2GB	RAID 930-8i	RAID 930-16i	430-8i HBA
Form factor	Onboard	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP
SAS controller	None	SAS3408	SAS3108	SAS3108	SAS3508	SAS3516	SAS3408
Host interface	PCH	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	6 Gb SATA	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	8	8	8	16	8
Connector type	SATA x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4
Number of connectors	2	2	2	2	2	4	2
Drive interface	SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD	HDD, SSD, SED	HDD, SSD	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED*
Hot-swap drive support	No	Yes	Yes	Yes	Yes	Yes	Yes
Number of drives	8	8	8	8	8	16^	8
RAID levels	0/1/10/5	0/1/10/5/50	0/1/10/5/50	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	None
JBOD mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cache	None	None	1 GB	2 GB	2 GB	4 GB; 8 GB	None
Cache protection	None	None	None	Flash backup (Included)	Flash backup (Included)	Flash backup (Included)	None
SED key management (SafeStore)	No	Yes	No	Yes	Yes	Yes	No
SSD I/O acceleration (FastPath)	No	Yes	No	Yes	Yes	Yes	No
SSD Caching (CacheCade Pro 2.0)	No	No	No	No	No**	No**	No
Consistency check	Yes	Yes	Yes	Yes	Yes	Yes	No
Patrol read	Yes	Yes	Yes	Yes	Yes	Yes	No
Online capacity expansion	Yes	Yes	Yes	Yes	Yes	Yes	No
Online RAID level migration	Yes	Yes	Yes	Yes	Yes	Yes	No
Global Hot Spare	Yes	Yes	Yes	Yes	Yes	Yes	No
Auto-rebuild	Yes	Yes	Yes	Yes	Yes	Yes	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
^ Up to 8 drives is supported by the RAID 930-16i in the SR530 server.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

Important: The onboard Intel RSTe is not supported by virtualization hypervisors, including VMware vSphere (ESXi), Linux KVM, Xen, and Microsoft Hyper-V.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Drives for internal storage

The following tables list the hard disk drive and solid-state drive options for the internal disk storage of the server.

2.5-inch hot-swap drives:

- 2.5-inch hot-swap 12 Gb SAS HDDs
- 2.5-inch hot-swap 6 Gb SATA HDDs
- 2.5-inch hot-swap 12 Gb SAS SSDs
- 2.5-inch hot-swap 6 Gb SATA SSDs

3.5-inch hot-swap drives:

- 3.5-inch hot-swap 12 Gb SAS HDDs
- 3.5-inch hot-swap 6 Gb SATA HDDs
- 3.5-inch hot-swap 12 Gb SAS SSDs
- 3.5-inch hot-swap 6 Gb SATA SSDs

Simple-swap drives:

- 3.5-inch simple-swap 6 Gb SATA HDDs

M.2 drives:

- M.2 SATA drives

M.2 drive support: The use of M.2 drives requires an additional adapter as described in the Internal storage section.

Table 19. 2.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00024	AULY	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00025	AULZ	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00026	AUM0	ThinkSystem 2.5" 900GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00027	AUM1	ThinkSystem 2.5" 1.2TB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00028	AUM2	ThinkSystem 2.5" 1.8TB 10K SAS 12Gb Hot Swap 512e HDD	8
7XB7A00069	B0YS	ThinkSystem 2.5" 2.4TB 10K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00021	AULV	ThinkSystem 2.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00022	AULW	ThinkSystem 2.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00023	AULX	ThinkSystem 2.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00034	AUM6	ThinkSystem 2.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00035	AUM7	ThinkSystem 2.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
2.5-inch hot-swap SED HDDs - 12 Gb SAS 10K			
7XB7A00030	AUM4	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD SED	8
7XB7A00031	AUM5	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD SED	8

Table 20. 2.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00036	AUUE	ThinkSystem 2.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	8
7XB7A00037	AUUJ	ThinkSystem 2.5" 2TB 7.2K SATA 6Gb Hot Swap 512e HDD	8

Table 21. 2.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17062	B8HU	ThinkSystem 2.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17063	B8J4	ThinkSystem 2.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17064	B8JD	ThinkSystem 2.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17065	B8JA	ThinkSystem 2.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13654	B4A1	ThinkSystem 2.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13655	B4A2	ThinkSystem 2.5" PM1645 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A38175	B91A	ThinkSystem 2.5" PM1643a 960GB Entry SAS 12Gb Hot Swap SSD	8
4XB7A38176	B91B	ThinkSystem 2.5" PM1643a 1.92TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17054	B91C	ThinkSystem 2.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17055	B91D	ThinkSystem 2.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17056	BC4R	ThinkSystem 2.5" PM1643a 15.36TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A13645	B4A7	ThinkSystem 2.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	8

Table 22. 2.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17087	B8J1	ThinkSystem 2.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17088	B8HY	ThinkSystem 2.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17089	B8J6	ThinkSystem 2.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17090	B8JE	ThinkSystem 2.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17091	B8J7	ThinkSystem 2.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13633	B49L	ThinkSystem 2.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13634	B49M	ThinkSystem 2.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13635	B49N	ThinkSystem 2.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13636	B49P	ThinkSystem 2.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13637	B49Q	ThinkSystem 2.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10237	B488	ThinkSystem 2.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10239	B48A	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10240	B48B	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10241	B48C	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			

Part number	Feature	Description	Maximum supported
4XB7A38271	BCTC	ThinkSystem 2.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38272	BCTD	ThinkSystem 2.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38273	BCTE	ThinkSystem 2.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38274	BCTF	ThinkSystem 2.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38275	BCTG	ThinkSystem 2.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17075	B8HV	ThinkSystem 2.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17076	B8JM	ThinkSystem 2.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17077	B8HP	ThinkSystem 2.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17078	B8J5	ThinkSystem 2.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17079	B8JP	ThinkSystem 2.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17080	B8J2	ThinkSystem 2.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38185	B9AC	ThinkSystem 2.5" 5210 960GB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38144	B7EW	ThinkSystem 2.5" 5210 1.92TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38145	B7EX	ThinkSystem 2.5" 5210 3.84TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38146	B7EY	ThinkSystem 2.5" 5210 7.68TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A10247	B498	ThinkSystem 2.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10248	B499	ThinkSystem 2.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10249	B49A	ThinkSystem 2.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13622	B49B	ThinkSystem 2.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13623	B49C	ThinkSystem 2.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10195	B34H	ThinkSystem 2.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10196	B34J	ThinkSystem 2.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10197	B34K	ThinkSystem 2.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10198	B34L	ThinkSystem 2.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10199	B34M	ThinkSystem 2.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10200	B4D2	ThinkSystem 2.5" PM883 7.68TB Entry SATA 6Gb Hot Swap SSD	8
7SD7A05740	B0Z0	ThinkSystem 2.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10155	B2X4	ThinkSystem 2.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10157	B2X6	ThinkSystem 2.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	8

Table 23. 3.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00063	B1JJ	ThinkSystem 3.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	4
3.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00038	AUU2	ThinkSystem 3.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00039	AUU3	ThinkSystem 3.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00040	AUUC	ThinkSystem 3.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00041	AUU4	ThinkSystem 3.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00042	AUU5	ThinkSystem 3.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00043	AUU6	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00044	AUU7	ThinkSystem 3.5" 6TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00045	B0YR	ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00046	AUUG	ThinkSystem 3.5" 10TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00067	B117	ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13906	B496	ThinkSystem 3.5" 14TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13911	B7EZ	ThinkSystem 3.5" 16TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A38266	BCFP	ThinkSystem 3.5" 18TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap SED HDDs - 12 Gb NL SAS			
7XB7A00047	AUUH	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD FIPS	4

Table 24. 3.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00049	AUUF	ThinkSystem 3.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00050	AUUD	ThinkSystem 3.5" 2TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00051	AUU8	ThinkSystem 3.5" 4TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00052	AUUA	ThinkSystem 3.5" 6TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00053	AUU9	ThinkSystem 3.5" 8TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00054	AUUB	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00068	B118	ThinkSystem 3.5" 12TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13907	B497	ThinkSystem 3.5" 14TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13914	B7F0	ThinkSystem 3.5" 16TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A38130	BCFH	ThinkSystem 3.5" 18TB 7.2K SATA 6Gb Hot Swap 512e HDD	4

Table 25. 3.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17066	B8HT	ThinkSystem 3.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17043	B8JN	ThinkSystem 3.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17067	B8JK	ThinkSystem 3.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17068	B8JG	ThinkSystem 3.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A13658	B4A4	ThinkSystem 3.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A17058	B91E	ThinkSystem 3.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A17059	BEVK	ThinkSystem 3.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A13649	B4A8	ThinkSystem 3.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	4

Table 26. 3.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17096	B8JL	ThinkSystem 3.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17097	B8JF	ThinkSystem 3.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17098	B8J0	ThinkSystem 3.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17099	B8HR	ThinkSystem 3.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17100	B8HX	ThinkSystem 3.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13639	B49R	ThinkSystem 3.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13640	B49S	ThinkSystem 3.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13641	B49T	ThinkSystem 3.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13642	B49U	ThinkSystem 3.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13643	B49V	ThinkSystem 3.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10242	B48D	ThinkSystem 3.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10244	B48F	ThinkSystem 3.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10245	B48G	ThinkSystem 3.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10246	B48H	ThinkSystem 3.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			
4XB7A38276	BCTH	ThinkSystem 3.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38277	BCTJ	ThinkSystem 3.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38278	BCTK	ThinkSystem 3.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38279	BCTL	ThinkSystem 3.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38281	BCTM	ThinkSystem 3.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17081	B8JB	ThinkSystem 3.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17082	B8J9	ThinkSystem 3.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17083	B8JC	ThinkSystem 3.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17084	B8HZ	ThinkSystem 3.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17085	B8HQ	ThinkSystem 3.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17086	B8J3	ThinkSystem 3.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Part number	Feature	Description	Maximum supported
4XB7A13625	B49D	ThinkSystem 3.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13626	B49E	ThinkSystem 3.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13627	B49F	ThinkSystem 3.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13628	B49G	ThinkSystem 3.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13629	B49H	ThinkSystem 3.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17176	B6TM	ThinkSystem 3.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17177	B6TN	ThinkSystem 3.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17178	B6TP	ThinkSystem 3.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17179	B6JY	ThinkSystem 3.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17180	B6JZ	ThinkSystem 3.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	4
7SD7A05735	B0Z5	ThinkSystem 3.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10160	B2X9	ThinkSystem 3.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10162	B2XB	ThinkSystem 3.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Table 27. 3.5-inch simple-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch simple-swap HDDs - 6 Gb NL SATA			
7XB7A00055	AUZS	ThinkSystem 1TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00056	AUZT	ThinkSystem 2TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00057	AUZU	ThinkSystem 4TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00058	AXC7	ThinkSystem 6TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00059	AXC6	ThinkSystem 8TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00060	AXC8	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Simple Swap 512e HDD	4

Table 29. M.2 SATA drives

Part number	Feature	Description	Maximum supported
M.2 SSDs - 6 Gb SATA - Entry (<3 DWPD)			
7N47A00129	AUUL	ThinkSystem M.2 32GB SATA 6Gbps Non-Hot Swap SSD	2
7N47A00130	AUUV	ThinkSystem M.2 128GB SATA 6Gbps Non-Hot Swap SSD	2
7SD7A05703	B11V	ThinkSystem M.2 5100 480GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17071	B8HS	ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17073	B919	ThinkSystem M.2 5300 480GB SATA 6Gbps Non-Hot Swap SSD	2

Optical drives

The server supports the external USB optical drive listed in the following table.

Table 30. External optical drive

Part number	Feature code	Description
7XA7A05926	AVV8	ThinkSystem External USB DVD RW Optical Disk Drive

The drive is based on the Lenovo Slim DVD Burner DB65 drive and supports the following formats: DVD-RAM, DVD-RW, DVD+RW, DVD+R, DVD-R, DVD-ROM, CD-RW, CD-R, CD-ROM.

I/O expansion

The SR530 server supports one LOM card slot and up to three PCIe slots with different riser cards installed into two riser sockets on the system planar (one riser socket supports installation of one riser card).

The slot form factors are as follows:

- LOM card slot
- Slot 1: PCIe 3.0 x8; low profile
- Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length
- Slot 3: PCIe 3.0 x8 or x16; low profile

Configuration notes:

- PCIe x16 slot 3 requires the second processor to be installed.
- The COM Port Upgrade Kit is installed in place of one of the PCIe slots 1, 2, or 3.

The locations of the PCIe slots are shown in the following figure.

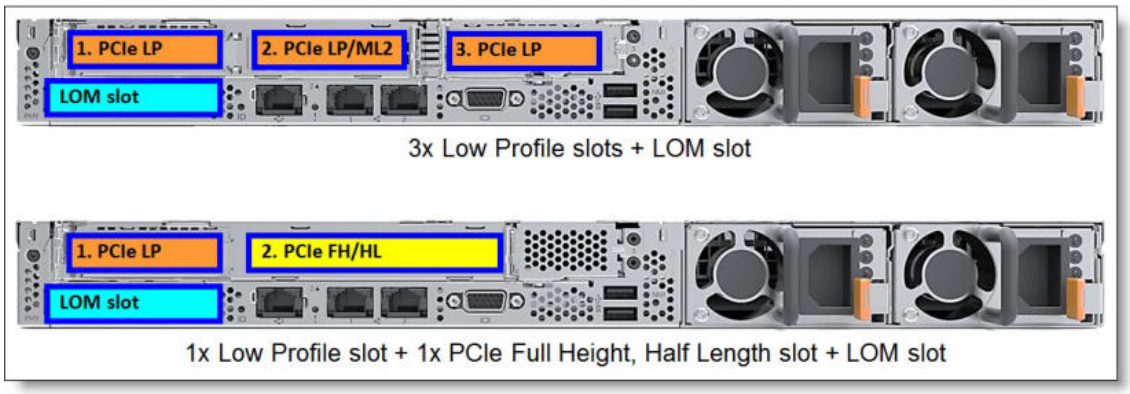


Figure 7. Slot locations

Riser 1 supplies slots 1 and 2, and Riser 2 supplies slot 3. The slots that are available for use depend on the number of riser cards that are installed and whether the second processor is installed, as shown in the following table.

Table 31. Slots available for use

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
None	None	LOM	-
None	PCIe x8	LOM, 3	-
None	PCIe x16	LOM	3
PCIe x8/x16 or PCIe x8/x8ML2	None	LOM, 1, 2	-
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x8	LOM, 1, 2, 3	-

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x16	LOM, 1, 2	3

The following table lists available PCIe riser card options.

Table 32. PCIe riser cards and miscellaneous options

Description	Part number	Feature code	Maximum quantity
x8 Riser Card 1 options (Riser card 1 supplies slots 1 and 2)			
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+LP Riser 1 Kit	7XH7A02682	AUWC	1
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+FH Riser 1 Kit	7XH7A05893	None*	1
ThinkSystem SR530/SR570 x8/x8ML2 PCIe LP+LP Riser 1 Kit	7XH7A05892	AV0X	1
Riser Card 2 option (Riser card 2 supplies slot 3)			
ThinkSystem SR530/SR570/SR630 x16 PCIe LP Riser 2 Kit	7XH7A02685	AUWA	1
ThinkSystem SR530/SR570 x8 PCIe LP Riser 2 Kit	7XH7A05891	AV0W	1
Serial port upgrade kit			
ThinkSystem COM Port Upgrade Kit	7Z17A02577	AUSL	1

* The LP+FH Riser 1 can be factory-installed by selecting the feature codes AUWC (LP+LP Riser 1) and AUWS (LP+FH Bracket).

The COM Port Upgrade Kit, part number 7Z17A02577, is used for mounting the external serial port on the rear of the SR530. This option includes the bracket and the cable. The COM Port option is mounted in place of one of the PCIe slots 1, 2, or 3.

Network adapters

The SR530 server has two onboard 1 GbE ports (no 10/100 Mb support) and up to two additional onboard 1/10 GbE network ports (no 10/100 Mb support) with optional LOM cards. Onboard ports and LOM cards use the Intel Ethernet Connection X722 1/10 GbE technology integrated into the Intel C622 Platform Controller Hub (PCH). The server also supports ML2 adapters that are installed in the custom ML2 slot provided by an ML2 riser card. The LOM cards support direct connectivity to the XClarity Controller via the Network Controller Sideband Interface (NSCI) for out-of-band systems management.

Note: ML2 network adapters do not support NSCI when used in the SR530 server.

The integrated Intel Ethernet Connection X722 has the following features:

- Two 1 Gb Ethernet ports (no 10/100 Mb Ethernet support)
- Two 1/10 Gb Ethernet capable ports (no 10/100 Mb Ethernet support)
- NIC Teaming (load balancing and failover)
- Data Center Bridging
- iWARP (RDMA over IP)
- VMDq and SR-IOV virtualization (10 Gb speeds only, 4 PFs, 128 VFs per device)
- IEEE 802.1q Virtual Local Area Networks (VLANs)
- NVGRE, VXLAN, IPinGRE, and MACinUDP network virtualization
- IEEE 802.1Qbg Edge Virtual Bridging
- TCP, IP, and UDP checksum offload
- Large Send Offload (LSO) and Generic Send Offload (GSO)
- Receive Side Scaling (RSS) for TCP and UDP traffic
- Jumbo frames up to 9.5 Kbytes

The following table lists the network adapters that are supported with the SR530 server.

Table 33. Network adapters

Description	Part number	Feature code	Max qty	I/O slots supported
LOM cards - 1 Gb Ethernet				
ThinkSystem 1Gb 2-port RJ45 LOM	7ZT7A00544	AUKG	1	LOM slot
LOM cards - 10 Gb Ethernet				
ThinkSystem 10Gb 2-port Base-T LOM	7ZT7A00548	AUKL	1	LOM slot
ThinkSystem 10Gb 2-port SFP+ LOM	7ZT7A00546	AUKJ	1*	LOM slot
ML2 adapters - 10 Gb Ethernet				
Broadcom NX-E ML2 10Gb 2-Port Base-T Ethernet Adapter	7ZT7A00497	AUKQ	1	2 (ML2)
Emulex VFA5.2 ML2 Dual Port 10GbE SFP+ Adapter	00AG560	AT7U	1*	2 (ML2)
Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	01CV770	AU7Z	1*	2 (ML2)
Intel X710-DA2 ML2 2x10GbE SFP+ Adapter	00JY940	ATRH	1*	2 (ML2)
PCIe Low Profile adapters - 1 Gb Ethernet				
Broadcom 5720 1GbE RJ45 2-Port PCIe Ethernet Adapter	7ZT7A00482	AUZX	3	1, 2, 3
Broadcom 5719 1GbE RJ45 4-Port PCIe Ethernet Adapter	7ZT7A00484	AUZV	3	1, 2, 3
ThinkSystem I350-F1 PCIe 1Gb 1-Port SFP Ethernet Adapter	7ZT7A00533	AUZZ	3	1, 2, 3
ThinkSystem I350-T2 PCIe 1Gb 2-Port RJ45 Ethernet Adapter	7ZT7A00534	AUZY	3	1, 2, 3
ThinkSystem I350-T4 PCIe 1Gb 4-Port RJ45 Ethernet Adapter	7ZT7A00535	AUZW	3	1, 2, 3
PCIe Low Profile adapters - 10 Gb Ethernet				
Broadcom 57416 10GBASE-T 2-Port PCIe Ethernet Adapter	7ZT7A00496	AUKP	3	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ PCIe Adapter	00AG570	AT7S	3*	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	00AG580	AT7T	3*	1, 2, 3
Intel X550-T2 Dual Port 10GBase-T Adapter	00MM860	ATPX	3	1, 2, 3
Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter	7ZT7A00537	AUKX	3*	1, 2, 3
QLogic QL41134 PCIe 10Gb 4-Port Base-T Ethernet Adapter	4XC7A08225	B31G	3	1, 2, 3
PCIe Full Height adapters - 10 Gb Ethernet				
Emulex OCe14104B-NX PCIe 10Gb 4-Port SFP+ Ethernet Adapter	7ZT7A00493	AUKN	1*	2
PCIe Low Profile adapters - 25 Gb Ethernet				
Broadcom 57412 10/25GbE SFP28 1-Port PCIe Ethernet Adapter	7ZT7A00505	AUKS	3*	1, 2, 3
Broadcom 57414 10/25GbE SFP28 2-port PCIe Ethernet Adapter	4XC7A08238	B5T0	3*	1, 2, 3
PCIe Low Profile adapters - Omni-Path				
Intel OPA 100 Series Single-port PCIe 3.0 x16 HFA	00WE027	AU0B	1 / 2#*	2, 3

The maximum quantity shown is with one processor / two processors.
* The adapter comes without transceivers or cables; for ordering transceivers or cables, see the adapter product guide

Configuration notes:

- ML2 network adapters are supported in the ML2 x8 slot 2 supplied by the x8/x8ML2 Riser Card 1 (7XH7A05892).
- PCIe full-height network adapters are supported in the full-height PCIe x16 slot 2 supplied by the PCIe x8/x16 LP+FH Riser Card 1 (7XH7A05893).
- Omni-Path adapters are supported in the low profile or full-height PCIe x16 slots supplied by the riser cards 1 and 2.
- PCIe Low Profile network adapters (except Omni-Path adapters) are supported in the low profile and full-height PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

- Some adapters require supported transceivers or DAC cables to be purchased for the adapter. The maximum number of transceivers or cables that are supported per adapter equals the quantity of the adapter ports, and all adapter ports must have the same type of the transceiver or cable selected.

For more information, see the list of Product Guides in the Ethernet Adapters category:
http://lenovopress.com/servers/options/ethernet#rt=product-guide

SAS adapters for external storage

The following table lists SAS RAID controllers and HBAs for external storage attachments that are supported by the SR530 server.

Table 34. SAS RAID adapters and HBAs for external storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
12 Gbps SAS RAID adapters				
ThinkSystem RAID 930-8e 4GB Flash PCIe 12Gb Adapter	7Y37A01087	AUNQ	2	1, 2, 3
12 Gbps SAS HBAs				
ThinkSystem 430-8e SAS/SATA 12Gb HBA	7Y37A01090	AUNR	2	1, 2, 3
ThinkSystem 430-16e SAS/SATA 12Gb HBA	7Y37A01091	AUNN	2	1, 2, 3

Configuration notes:

- Low profile SAS RAID controllers and HBAs for external storage are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.
- The total quantity of the RAID 730-8i 2GB, RAID 930-8i, RAID 930-16i, and RAID 930-8e controllers in a supported combination in the server must not exceed 2 (up to 2 supercapacitors can be mounted in the server).

The following table summarizes features of supported RAID controllers and HBAs for external storage.

Table 35. Features and specifications of the RAID controllers and HBAs for external storage

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
Form factor	PCIe LP	PCIe LP	PCIe LP
SAS controller chip	SAS3516	SAS3408	SAS3416
Host interface	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	16
Connector type	SFF-8644 x4	SFF-8644 x4	SFF-8644 x4
Number of connectors	2	2	4
Drive interface	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD, SSD, SED	HDD, SSD, SED*	HDD, SSD, SED*
Hot-swap drive support	Yes	Yes	Yes
Number of devices	240	1024	1024
RAID levels	0/1/10/5/50/6/60	None	None
JBOD mode	Yes	Yes	Yes
Cache	4 GB	None	None
Cache protection	Flash backup (Included)	None	None
SED key management (SafeStore)	Yes	No	No
SSD I/O acceleration (FastPath)	Yes	No	No

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
SSD Caching (CacheCade Pro 2.0)	No**	No	No
Consistency check	Yes	No	No
Patrol read	Yes	No	No
Online capacity expansion	Yes	No	No
Online RAID level migration	Yes	No	No
Global Hot Spare	Yes	No	No
Auto-rebuild	Yes	No	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Fibre Channel host bus adapters

The following table lists Fibre Channel HBAs supported by the SR530 server.

Table 36. Fibre Channel HBAs

Description	Part number	Feature code	Maximum quantity	I/O slots supported
16 Gb Fibre Channel - PCIe				
Emulex 16Gb Gen6 FC Single-port HBA	01CV830	ATZU	3	1, 2, 3
Emulex 16Gb Gen6 FC Dual-port HBA	01CV840	ATZV	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Single-port HBA	01CV750	ATZB	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Dual-port HBA	01CV760	ATZC	3	1, 2, 3
8 Gb Fibre Channel - PCIe (available only in PRC and Asia Pacific)				
Emulex LPe12002-M8-L PCIe 8Gb 2-Port SFP+ FC HBA	4XC7A08221	B0X0	3	1, 2, 3
Emulex LPe12000-M8-L PCIe 8Gb 1-Port SFP+ FC HBA	4XC7A08220	B0WZ	3	1, 2, 3

Configuration note: FC HBAs are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

For more information, see the list of Product Guides in the Host bus adapters category:
http://lenovopress.com/servers/options/hba#rt=product-guide

Cooling

The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.

The following table shows additional cooling options.

Table 37. Cooling options

Description	Part number	Feature code	Maximum quantity
ThinkSystem SR530 FAN Option Kit	4F17A12354	AV0N	1

Configuration note: The SR530 FAN Option Kit (4F17A12354) includes two system fans that are required for field upgrades that add a second processor to the server. If two processors are selected in the initial server configurations, two fans for the second processor are derived by the configurator.

Power supplies and cables

The SR530 server supports up to two redundant power supplies and is capable of N+N redundancy depending on the configuration. A second power supply can be added to the models that come with one power supply. The following table lists the power supply options.

Table 38. Power supplies

Description	Part number	Feature code	Maximum quantity
ThinkSystem 550W (230V/115V) Platinum Hot-Swap Power Supply	7N67A00882	AVV6	2
ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply	7N67A00883	AVV7	2
ThinkSystem 750W (230V) Titanium Hot-Swap Power Supply	7N67A00884	AVV5	2

Configuration notes:

- Minimum of 1 and maximum of 2 power supplies per system.
- If 2 are installed, power supplies must be identical.
- Power supplies support AC (Worldwide) and HVDC (PRC only) power sources.

Important: The Standalone Solution Configuration Tool (SSCT) and Lenovo Data Center Solution Configurator (DCSC) power supply selection rules allow a subset of possible configurations due to power restrictions. Configurations that cannot be built in SSCT or DCSC due to power restrictions may still be supported. To verify support and ensure that the right power supply is chosen for optimal performance, you should always validate your server configuration using the latest version of the Lenovo Capacity Planner: http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

The SR530 server ship standard with or without a power cord (model dependent). A hot-swap power supply option ships without a power cord. The following table lists the rack power cables and line cords that can be ordered for the SR530 server.

Table 39. Power cables

Description	Part number	Feature code
Rack power cables		
1.0m, 10A/125-250V, C13 to IEC 320-C14 Rack Power Cable	00Y3043	A4VP
1.5m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7937	6201
2.0m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08369	6570
2.8m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08366	6311

Description	Part number	Feature code
2.8m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08370	6400
2.8m, 10A/100-250V, C13 to IEC 320-C20 Rack Power Cable	39Y7938	6204
4.3m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7932	6263
4.3m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08371	6583
Line cords		
Argentina 2.8m, 10A/250V, C13 to IRAM 2073 Line Cord	39Y7930	6222
Argentina 4.3m, 10A/250V, C13 to IRAM 2073 Line Cord	81Y2384	6492
Australia/New Zealand 2.8m, 10A/250V, C13 to AS/NZS 3112 Line Cord	39Y7924	6211
Australia/New Zealand 4.3m, 10A/250V, C13 to AS/NZS 3112 Line Cord	81Y2383	6574
Brazil 2.8m, 10A/250V, C13 to NBR 14136 Line Cord	69Y1988	6532
Brazil 4.3m, 10A/250V, C13 to NBR14136 Line Cord	81Y2387	6404
China 1.8m, 10A/250V, C13 to GB 2099.1 Line Cord	4L67A69954	6361
China 2.8m, 10A/250V, C13 to GB 2099.1 Line Cord	39Y7928	6210
China 4.3m, 10A/250V, C13 to GB 2099.1 Line Cord	81Y2378	6580
Denmark 2.8m, 10A/250V, C13 to DK2-5a Line Cord	39Y7918	6213
Denmark 4.3m, 10A/250V, C13 to DK2-5a Line Cord	81Y2382	6575
Europe 2.8m, 10A/250V, C13 to CEE7-VII Line Cord	39Y7917	6212
Europe 4.3m, 10A/250V, C13 to CEE7-VII Line Cord	81Y2376	6572
India 2.8m, 10A/250V, C13 to IS 6538 Line Cord	39Y7927	6269
India 4.3m, 10A/250V, C13 to IS 6538 Line Cord	81Y2386	6567
Israel 2.8m, 10A/250V, C13 to SI 32 Line Cord	39Y7920	6218
Israel 4.3m, 10A/250V, C13 to SI 32 Line Cord	81Y2381	6579
Italy 2.8m, 10A/250V, C13 to CEI 23-16 Line Cord	39Y7921	6217
Italy 4.3m, 10A/250V, C13 to CEI 23-16 Line Cord	81Y2380	6493
Japan 2.8m, 12A/125V, C13 to JIS C-8303 Line cord	46M2593	6314
Japan 2.8m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08357	5472
Japan 4.3m, 12A/125V, C13 to JIS C-8303 Line Cord	39Y7926	6335
Japan 4.3m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08362	6495
Korea 2.8m, 12A/250V, C13 to KS C8305 Line Cord	39Y7925	6219
Korea 4.3m, 12A/250V, C13 to KS C8305 Line Cord	81Y2385	6494
South Africa 2.8m, 10A/250V, C13 to SABS 164 Line Cord	39Y7922	6214
South Africa 4.3m, 10A/250V, C13 to SABS 164 Line Cord	81Y2379	6576
Switzerland 2.8m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	39Y7919	6216
Switzerland 4.3m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	81Y2390	6578
Taiwan 2.8m, 10A/125V, C13 to CNS 10917-3 Line Cord	23R7158	6386
Taiwan 2.8m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2375	6317
Taiwan 2.8m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2374	6402
Taiwan 4.3m, 10A/125V, C13 to CNS 10917-3 Line Cord	4L67A08363	AX8B
Taiwan 4.3m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2389	6531
Taiwan 4.3m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2388	6530
United Kingdom 2.8m, 10A/250V, C13 to BS 1363/A Line Cord	39Y7923	6215
United Kingdom 4.3m, 10A/250V, C13 to BS 1363/A Line Cord	81Y2377	6577
United States 2.8m, 10A/125V, C13 to NEMA 5-15P Line Cord	90Y3016	6313

Description	Part number	Feature code
United States 2.8m, 10A/250V, C13 to NEMA 6-15P Line Cord	46M2592	A1RF
United States 2.8m, 13A/125V, C13 to NEMA 5-15P Line Cord	00WH545	6401
United States 4.3m, 10A/125V, C13 to NEMA 5-15P Line Cord	4L67A08359	6370
United States 4.3m, 10A/250V, C13 to NEMA 6-15P Line Cord	4L67A08361	6373
United States 4.3m, 13A/125V, C13 to NEMA 5-15P Line Cord	4L67A08360	AX8A

Systems management

The SR530 supports the following systems management tools:

- Lenovo XClarity Controller
- Lenovo XClarity Provisioning Manager
- Lenovo XClarity Essentials
- Lenovo XClarity Administrator
- Lenovo XClarity Integrators
- Lenovo XClarity Energy Manager
- Lenovo Capacity Planner

Lenovo XClarity Controller

The SR530 server contains Lenovo XClarity Controller (XCC), which provides advanced service-processor control, monitoring, and alerting functions. XClarity Controller offers three functional levels: Standard, Advanced, and Enterprise.

By default, the SR530 server includes XClarity Controller Standard features, and it can be upgraded to Advanced or Enterprise functionality by using the Features on Demand (FoD) upgrades.

XClarity Controller Standard offers the following capabilities:

- Gathering and viewing system information and inventory
- Monitoring system status and health
- Alerting and notifications
- Event logging
- Configuring network connectivity
- Configuring security
- Updating system firmware
- Configuring server settings and devices
- Real-time power usage monitoring
- Remotely controlling server power (Power on, Power off, Restart)
- Managing FoD activation keys
- Redirecting serial console via IPMI
- Capturing the video display contents when an operating system hang condition is detected

XClarity Controller Advanced Upgrade adds the following functionality to the Standard features:

- Remotely viewing video with the following graphics resolutions:
  - Up to 1600x1200 with up to 23 bits per pixel; or
  - Up to 1920x1200 with up to 15 bits per pixel
- Remotely accessing the server using the keyboard and mouse from a remote client
- Remotely deploying an operating system
- Syslog alerting
- Redirecting serial console via SSH
- Displaying graphics for real-time and historical power usage data and temperature

XClarity Controller Enterprise Upgrade adds the following functionality to the Advanced features:

- Capping power usage
- Mapping the ISO and image files located on the local client as virtual drives for use by the server
- Mounting the remote ISO and image files via HTTPS, SFTP, CIFS, and NFS
- Collaborating across up to six users of the virtual console
- Controlling quality and bandwidth usage

The XClarity Controller provides remote server management through industry-standard interfaces:

- Intelligent Platform Management Interface (IPMI) Version 2.0
- Simple Network Management Protocol (SNMP) Version 3
- Common Information Model (CIM)
- Data Center Manageability Interface (DCMI) Version 1.5
- Redfish REpresentational State Transfer (REST) API
- Web browser with HTML5 support
- Command-line interface
- Virtual Operator Panel with XClarity Mobile App via the front USB port with XClarity Controller access

Virtual Operator Panel provides quick access to system status, firmware, network, health, and alerts information. With proper authentication, it also allows to configure systems management and network settings and to control system power (Power on, Power off, Restart). The Virtual Operator Panel can be accessed from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access (See Components and connectors).

Note: Depending on the system settings, the front USB port can be assigned to XClarity Controller for management functions, or to the system as a regular USB 2.0 port, or switched between two functions by using the system ID button.

IPMI via the Ethernet port (IPMI over LAN) is supported, however it is disabled by default. For CTO orders you can specify whether you want to the feature enabled or disabled in the factory, using the feature codes listed in the following table.

Table 40. IPMI-over-LAN settings

Part number	Feature code	Description
CTO only	B7XZ	Disable IPMI-over-LAN (default)
CTO only	B7Y0	Enable IPMI-over-LAN

The following table lists the XClarity Controller FoD upgrades.

Table 41. XClarity Controller FoD upgrades

Description	Part number	Feature code	Maximum quantity
ThinkSystem XClarity Controller Standard to Advanced Upgrade	4L47A09132	AVUT	1
ThinkSystem XClarity Controller Standard to Enterprise Upgrade	None*	AUPW	1
ThinkSystem XClarity Controller Advanced to Enterprise Upgrade	4L47A09133	None**	1

* Factory-installed only.
** Field upgrade only.

Configuration notes:

- For factory-installed upgrades, either Standard to Advanced Upgrade (feature AVUT) or Standard to Enterprise Upgrade (feature AUPW) can be selected, but not both.
- For field upgrades, the Advanced to Enterprise Upgrade (4L47A09133) requires the Standard to Advanced Upgrade to be activated on the server previously with either the factory-installed feature AVUT or field upgrade 4L47A09132.

Lenovo XClarity Provisioning Manager

Lenovo XClarity Provisioning Manager is a UEFI-embedded GUI application that combines the functions of configuring system setup settings, configuring RAID, and updating applications and firmware. It also enables you to install the supported operating systems and associated device drivers, run diagnostics, and collect service data.

Lenovo XClarity Provisioning Manager has the following features:

- Automatic hardware detection
- Collecting and viewing system inventory information
- Configuring UEFI system setup settings
- Updating the system firmware
- Configuring RAID by using the RAID Setup Wizard or Advanced mode
- Installing an operating system and device drivers automatically or manually
- Running diagnostics and collecting service data

Lenovo XClarity Essentials

Lenovo offers the following XClarity Essentials software tools that can help you set up, use, and maintain the server at no additional cost:

- Lenovo XClarity Essentials OneCLI
  OneCLI is a collection of server management tools that utilize a command line interface program to manage firmware, hardware, and operating systems. It provides functions to collect full system health information (including health status), configure system setting, and update system firmware and drivers.
- Lenovo XClarity Essentials UpdateXpress
  The UpdateXpress tool is a standalone GUI application for firmware and device driver updates that enables you to maintain your server firmware and device drivers up-to-date and help you avoid unnecessary server outages. The tool acquires and deploys individual updates and UpdateXpress System Packs (UXSPs) which are integration-tested bundles.
- Lenovo XClarity Essentials Bootable Media Creator
  The Bootable Media Creator (BOMC) tool is used to create bootable media for offline firmware update.

For more information and downloads, visit the Lenovo XClarity Essentials web page:
http://support.lenovo.com/us/en/documents/LNVO-center

Lenovo XClarity Administrator

Lenovo XClarity is a centralized systems management solution that helps administrators deliver infrastructure faster. This solution integrates easily with Lenovo x86 servers, RackSwitch switches, and DS Series storage, providing automated agent-less discovery, monitoring, firmware updates, configuration management, and bare metal deployment of operating systems and hypervisors across multiple servers.

Lenovo XClarity Administrator is an optional software component for the SR530 server which can be downloaded and used at no charge to discover and monitor the SR530 and manage firmware upgrades for them.

If software support is required for Lenovo XClarity Administrator, or Lenovo XClarity Administrator premium features (such as configuration management and operating system deployment) are required, or both, Lenovo XClarity Pro software subscription should be ordered. Lenovo XClarity Pro is licensed on a per managed system basis, that is, each managed Lenovo system requires a license.

The following table lists the geo-specific Lenovo XClarity software license options.

Table 42. Lenovo XClarity software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Pro, per Managed Endpoint w/1 Yr SW S&S	00MT201	00MT207	1
Lenovo XClarity Pro, per Managed Endpoint w/3 Yr SW S&S	00MT202	00MT208	1
Lenovo XClarity Pro, per Managed Endpoint w/5 Yr SW S&S	00MT203	00MT209	1

* NA = North America; AP = Asia Pacific
** EMEA = Europe, Middle East, Africa; LA = Latin America

Lenovo XClarity Administrator offers the following standard features that are available at no charge:

- Auto-discovery and monitoring of Lenovo x86 servers, RackSwitch switches, Flex System chassis, and DS Series storage systems
- Firmware updates and compliance enforcement
- External alerts and notifications via SNMP traps, syslog remote logging, and e-mail
- Secure connections to managed endpoints
- NIST 800-131A or FIPS 140-2 compliant cryptographic standards between the management solution and managed endpoints
- Integration into existing higher level management systems such as cloud automation and orchestration tools through REST APIs, providing extensive external visibility and control over hardware resources
- An intuitive, easy-to-use GUI
- Scripting with Windows PowerShell, providing command-line visibility and control over hardware resources

Lenovo XClarity Administrator offers the following premium features that require an optional Pro license:

- Pattern-based configuration management that allows to define configurations once and apply repeatedly without errors when deploying new servers or redeploying existing servers without disrupting the fabric
- Bare-metal deployment of operating systems and hypervisors to streamline infrastructure provisioning

For more information, refer to the Lenovo XClarity Administrator Product Guide:
http://lenovopress.com/tips1200

Lenovo XClarity Integrators

Lenovo offers at no charge (if software support is required, a Lenovo XClarity Pro software subscription license should be ordered) two software plug-in modules, Lenovo XClarity Integrators, to manage physical infrastructure from leading external virtualization management software tools from Microsoft and VMware:

- Lenovo XClarity Integrator for Microsoft System Center
- Lenovo XClarity Integrator for VMware vCenter

Lenovo XClarity Integrators offer the following additional features:

- Ability to discover, manage, and monitor Lenovo server hardware from VMware vCenter or Microsoft System Center
- Deployment of firmware updates and configuration patterns to Lenovo x86 rack servers and Flex System from the virtualization management tool
- Non-disruptive server maintenance in clustered environments that reduces workload downtime by dynamically migrating workloads from affected hosts during rolling server updates or reboots
- Greater service level uptime and assurance in clustered environments during unplanned hardware events by dynamically triggering workload migration from impacted hosts when impending hardware failures are predicted

For more information, refer to the Lenovo XClarity Integrators web page:
http://www3.lenovo.com/us/en/data-center/software/systems-management/xclarity-integrators

Lenovo XClarity Energy Manager

Lenovo XClarity Energy Manager provides a stand-alone, web-based agent-less power management console that provides real time data and enables you to observe, plan and manage power and cooling for Lenovo servers. Using built-in intelligence, it identifies server power consumption trends and ideal power settings and performs cooling analysis so that you can define and optimize power-saving policies.

Lenovo XClarity Energy Manager offers the following capabilities:

- Monitors room, row, rack, and device levels in the data center
- Reports vital server information, such as power, temperature and resource utilization
- Monitors inlet temperature to locate hot spots, reducing the risk of data or device damage
- Provides finely-grained controls to limit platform power in compliance with IT policy
- Generates alerts when a user-defined threshold is reached

Lenovo XClarity Energy Manager is an optional software component for the SR530 server that is licensed on a per managed node basis, that is, each managed server requires a license. The 1-node Energy Manager license is included in the XClarity Controller Enterprise upgrade.

To manage systems without XClarity Controller Enterprise licenses, a node license pack should be purchased. The following table lists the geo-specific Lenovo XClarity Energy Manager software license options.

Table 43. Lenovo XClarity Energy Manager software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Energy Manager, 1 Node w/ 1 Yr S&S	01DA225	01DA228	1

* NA = North America; AP = Asia Pacific.
** EMEA = Europe, Middle East, Africa; LA = Latin America.

For more information, refer to the Lenovo XClarity Energy Manager web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lxem

Lenovo Capacity Planner

Lenovo Capacity Planner is a power consumption evaluation tool that enhances data center planning by enabling IT administrators and pre-sales professionals to understand various power characteristics of racks, servers, and other devices. Capacity Planner can dynamically calculate the power consumption, current, British Thermal Unit (BTU), and volt-ampere (VA) rating at the rack level, improving the planning efficiency for large-scale deployments.

For more information, refer to the Capacity Planner web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

Security

The SR530 server offers the following security features:

- Power-on password
- Administrator's password
- Secure firmware updates
- Onboard Trusted Platform Module (TPM) version 1.2 or 2.0 (configurable UEFI system setting)
- Trusted Cryptographic Module (TCM) (optional; available in PRC only)
- Nationz Trusted Platform Module v2.0 (optional; available in PRC only)
- Lockable front bezel (optional)
- Security Key Lifecycle Manager (SKLM) encryption key management for SEDs - FoD upgrade (optional)
- Lenovo Business Vantage security software (optional; available in PRC only)

The server is NIST SP 800-147B compliant.

The following table lists the security options that are available for the SR530 server.

Table 44. Security options

Description	Part number	Feature code	Maximum quantity
Lockable front bezel			
ThinkSystem 1U Security Bezel	7Z17A02581	AUWR	1
Trusted Cryptographic Module (PRC only)			
ThinkSystem Trusted Cryptographic Module	None*	AVKE	1
Trusted Platform Module (PRC only)			
ThinkSystem Nationz Trusted Platform Module v2.0	None*	B22N	1
Security Key Lifecycle Manager - FoD (United States, Canada, Asia Pacific, and Japan)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00D9998	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00D9999	AS6C	1
Security Key Lifecycle Manager - FoD (Latin America, Europe, Middle East, and Africa)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00FP648	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00FP649	AS6C	1

* Factory-installed only; no field upgrade.

Lenovo Business Vantage is a security software tool suite (available only in PRC) designed to work with the TCM or Nationz TPM for enhanced security, to keep user data safe, and to erase confidential data completely from a drive.

Lenovo Business Vantage provides the following features:

- Encrypts files to ensure data safety by using the TCM or Nationz TPM.
- Erases confidential data from a hard disk.
- Prohibits unauthorized access to the USB port of devices.
- Encrypts files to ensure data security on a USB storage device.

For more information, refer to the Lenovo Business Vantage web page:
http://support.lenovo.com.cn/lenovo/wsi/es/es.html

Rack installation

The following table lists the rack installation options that are available for the SR530 server.

Table 45. Rack installation options

Description	Part number	Feature code	Maximum quantity
4-post rail kits			
ThinkSystem Tool-less Slide Rail	7M27A05702	AXCA	1
ThinkSystem Tool-less Slide Rail Kit with 1U CMA	7M27A05701	AXCB	1
ThinkSystem Screw-in Slide Rail	4M17A07274	AXFN	1
ThinkSystem Screw-in Slide Rail Kit with 1U CMA	4M17A07281	B0TE	1
ThinkSystem Tool-less Friction Rail	4M17A07273	AXFM	1
Cable management arm (CMA) upgrade			
ThinkSystem 1U CMA Upgrade Kit for Tool-less Slide Rail	7M27A05699	None^	1*
ThinkSystem 1U CMA Upgrade Kit for Screw-in Slide Rail	4M17A07276	AXFP	1**
Front VGA port			
ThinkSystem SR530/SR630 Front VGA Connector (for 3.5" models)	None***	AUWU	1
ThinkSystem SR530/SR570/SR630 Front VGA Connector Upgrade Kit (for 2.5" models)	7Z17A02579	AUWW	1

^ Field upgrade only.
* The CMA Upgrade Kit for Tool-less Slide Rail is supported with the Tool-less Slide Rail (7M27A05702) only.
** The CMA Upgrade Kit for Screw-in Slide Rail is supported with the Screw-in Slide Rail (4M17A07274) only.
*** Factory-installed only; no field upgrade.

The following table summarizes the rail kit features and specifications.

Table 46. Rail kit features and specifications summary

Feature	Tool-less Slide Rail		Screw-in Slide Rail		Tool-less Friction Rail
	Without CMA	With CMA	Without CMA	With CMA	
Part number	7M27A05702	7M27A05701	4M17A07274	4M17A07281	4M17A07273
CMA	7M27A05699	Included	4M17A07276	Included	No support
Rail length	730 mm (28.74 in.)	807 mm (31.8 in.)	836.8 mm (32.9 in.)	836.8 mm (32.9 in.)	728.1 mm (28.7 in.)
Rail type	Full-out slide (ball bearing)		Full-out slide (ball bearing)		Half-out slide (friction)
Tool-less installation	Yes		No		Yes
In-rack server maintenance	Yes		Yes		No
1U PDU support	Yes		Yes		Yes
0U PDU support	Limited*		Limited*		Limited**
Rack type	IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant
Mounting holes	Square or round		Square, round, or threaded		Square or round
Mounting flange thickness	2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)
Distance between front and rear mounting flanges^	609.6 mm (24 in.) – 863.6 mm (34 in.)		609.6 mm (24 in.) – 812.8 mm (32 in.)		609.6 mm (24 in.) – 863.6 mm (34 in.)

* If a 0U PDU is used, the rack cabinet must be at least 1100 mm (43.31 in.) deep if no CMA is used, or at least 1200 mm (47.24 in.) deep if a CMA is used.
** If a 0U PDU used, the rack must be at least 1000 mm (39.37 in.) deep.
^ Measured when mounted on the rack, from the front surface of the front mounting flange to the rear most point of the rail.

Operating systems

The server supports the following operating systems:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 8.1
- Red Hat Enterprise Linux 8.2
- Red Hat Enterprise Linux 8.3
- SUSE Linux Enterprise Server 12 SP4
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 12 Xen SP4
- SUSE Linux Enterprise Server 12 Xen SP5
- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Server 15 SP1
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 15 Xen
- SUSE Linux Enterprise Server 15 Xen SP1
- SUSE Linux Enterprise Server 15 Xen SP2
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2

For a complete list of supported, certified and tested operating systems, plus additional details and links to relevant web sites, see the Operating System Interoperability Guide: https://lenovopress.com/osig#servers=sr530-7x07-7x08-sp-gen-2

For configure-to-order configurations, the server can be preloaded with VMware ESXi installed on M.2 cards. Ordering information is listed in the following table.

Table 47. VMware ESXi preload

Part number	Feature code	Description
CTO only	B3VW	VMware ESXi 6.5 U2 (Factory Installed)
CTO only	B6U0	VMware ESXi 6.5 U3 (factory installed)
CTO only	B3VX	VMware ESXi 6.7 (Factory Installed)
CTO only	B4XA	VMware ESXi 6.7 U1 (Factory Installed)
CTO only	B6U1	VMware ESXi 6.7 U2 (factory installed)
CTO only	B88T	VMware ESXi 6.7 U3 (factory installed)
CTO only	BBZG	VMware ESXi 7.0 (Factory Installed)
CTO only	BE5E	VMware ESXi 7.0 U1 (Factory Installed)

Physical specifications

The SR530 has the following overall physical dimensions, excluding components that extend outside the standard chassis, such as EIA flanges, front security bezel (if any), and power supply handles:

- Width: 435 mm (17.1 inches)
- Height: 43 mm (1.7 inches)

- Depth: 750 mm (29.5 inches)

The following table lists the detailed dimensions. See the figure below for the definition of each dimension.

Table 48. Detailed dimensions

Dimension	Description
482 mm	X_a = Width, to the outsides of the front EIA flanges
435 mm	X_b = Width, to the rack rail mating surfaces
435 mm	X_c = Width, to the outer most chassis body feature
43 mm	Y_a = Height, from the bottom of chassis to the top of the chassis
715 mm	Z_a = Depth, from the rack flange mating surface to the rearmost I/O port surface
716 mm	Z_b = Depth, from the rack flange mating surface to the rearmost feature of the chassis body
744 mm	Z_c = Depth, from the rack flange mating surface to the rearmost feature such as power supply handle
35 mm	Z_d = Depth, from the forwardmost feature on front of EIA flange to the rack flange mating surface
47 mm	Z_e = Depth, from the front of security bezel (if applicable) or forwardmost feature to the rack flange mating surface

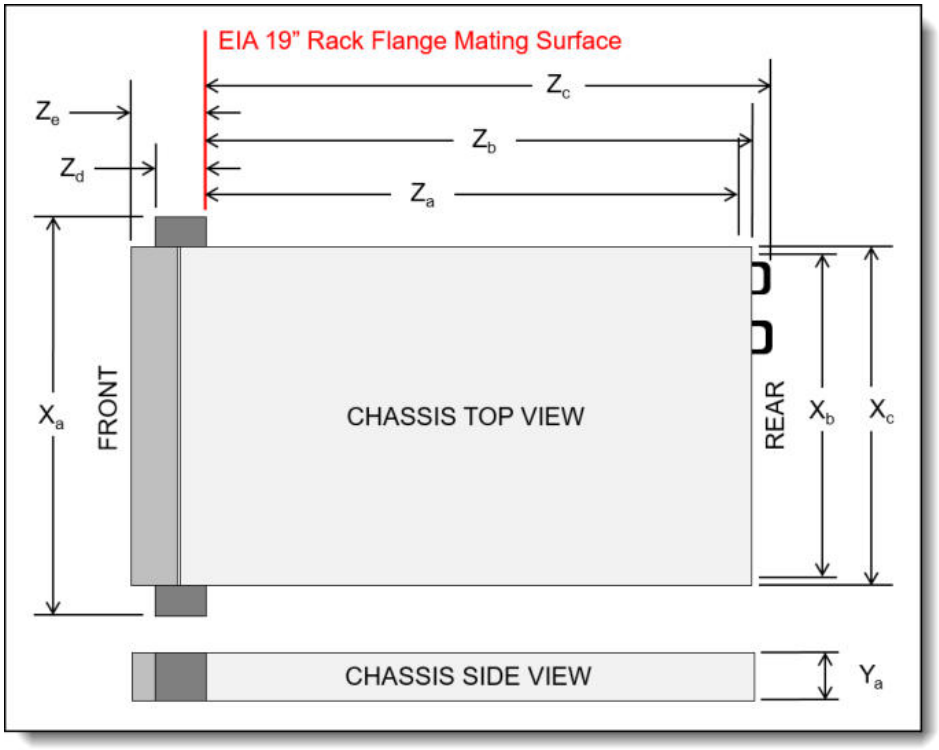


Figure 8. Server dimensions

The shipping dimensions (cardboard packaging) of the SR530 are as follows:

- Width: 587 mm (23.1 inches)
- Height: 225 mm (8.9 inches)
- Depth: 998 mm (39.3 inches)

The SR530 server has the following weight:

- Minimum configuration: 10.2 kg (22.5 lb)
- Maximum configuration: 16.0 kg (35.3 lb)

Operating environment

The SR530 server complies with ASHRAE class A2 specifications. The server performance might be impacted when the operating temperature is outside the ASHRAE A2 specifications. Depending on the hardware configuration, some server models comply with ASHRAE class A3 and class A4 specifications. To comply with ASHRAE class A3 and class A4 specifications, the server models must meet the following hardware configuration requirements at the same time:

- Two power supplies must be installed
- No system fan failure

The SR530 server is supported in the following environment:

- Air temperature:
  - Operating:
    - ASHRAE Class A4: 5 °C - 45 °C (41 °F - 113 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 125-m (410-ft) increase in altitude
    - ASHRAE Class A3: 5 °C - 40 °C (41 °F - 104 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 175-m (574-ft) increase in altitude
    - ASHRAE Class A2: 10 °C - 35 °C (50 °F - 95 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 300-m (984-ft) increase in altitude
  - Non-operating: 5 °C - 45 °C (41 °F - 113 °F)
  - Storage: -40 °C - +60 °C (-40 °F - 140 °F)
- Maximum altitude: 3,050 m (10,000 ft)
- Humidity:
  - Operating:
    - ASHRAE Class A4: 8% - 90% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A3: 8% - 85% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A2: 8% - 80% (non-condensing); maximum dew point: 21 °C (70 °F)
  - Storage: 8% - 90% (non-condensing)
- Electrical:
  - 100 - 127 (nominal) V AC; 50 Hz / 60 Hz
  - 200 - 240 (nominal) V AC; 50 Hz / 60 Hz
  - 180 - 300 V DC (HVDC; supported in PRC only)
- Acoustics:
  - Minimum configuration:
    - Operating: 5.0 bels
    - Idle: 4.5 bels
  - Maximum configuration:
    - Operating: 5.5 bels
    - Idle: 5.2 bels
- Vibration:
  - Operating: 0.21 G rms at 5 Hz to 500 Hz for 15 minutes across 3 axes
  - Non-operating: 1.04 G rms at 2 Hz to 200 Hz for 15 minutes across 6 surfaces
- Shock:
  - Operating: 15 G for 3 milliseconds in each direction (positive and negative X, Y, and Z axes)
  - Non-operating:
    - 12 kg - 22 kg: 50 G for 152 in./sec velocity change across 6 surfaces
    - 23 kg - 31 kg: 35 G for 152 in./sec velocity change across 6 surfaces

The following table lists the maximum system power load, rated inlet current, and system heat output based on the power supply and source voltage.

Table 49. Rated system power, inlet current, and system heat output

Power supply	Source voltage	Maximum power load per system (two power supplies)	Rated current per inlet	System heat output
550 W Platinum	100 - 127 V AC	722 W	6.2 A	2463 BTU/hour
	200 - 240 V AC	704 W	3 A	2402 BTU/hour
	180 - 300 V DC	702 W	2.5 A	2395 BTU/hour
750 W Platinum	100 - 127 V AC	984 W	8.4 A	3357 BTU/hour
	200 - 240 V AC	958 W	4.1 A	3269 BTU/hour
	180 - 300 V DC	958 W	3.5 A	3269 BTU/hour
750 W Titanium	200 - 240 V AC	949 W	4.1 A	3238 BTU/hour
	180 - 300 V DC	948 W	3.5 A	3235 BTU/hour

Warranty and support

The SR530 server has a one-year (7X07) or three-year (Machine Type 7X08) warranty.

The standard warranty terms are customer-replaceable unit (CRU) and onsite (for field-replaceable units FRUs only) with standard call center support during normal business hours and 9x5 Next Business Day Parts Delivered.

Lenovo's additional support services provide a sophisticated, unified support structure for your data center, with an experience consistently ranked number one in customer satisfaction worldwide. Available offerings include:

- **Premier Support**

  Premier Support provides a Lenovo-owned customer experience and delivers direct access to technicians skilled in hardware, software, and advanced troubleshooting, in addition to the following:

  - Direct technician-to-technician access through a dedicated phone line
  - 24x7x365 remote support
  - Single point of contact service
  - End to end case management
  - Third-party collaborative software support
  - Online case tools and live chat support
  - On-demand remote system analysis
- **Warranty Upgrade (Preconfigured Support)**

  Services are available to meet the on-site response time targets that match the criticality of your systems.

  - 3, 4, or 5 years of service coverage
  - 1-year or 2-year post-warranty extensions
  - **Foundation Service**: 9x5 service coverage with next business day onsite response. YourDrive YourData is an optional extra (see below).
  - **Essential Service:** 24x7 service coverage with 4-hour onsite response or 24-hour committed repair (available only in select countries). Bundled with YourDrive YourData.
  - **Advanced Service:** 24x7 service coverage with 2-hour onsite response or 6-hour committed repair (available only in select countries). Bundled with YourDrive YourData.

- **Managed Services**

  Lenovo Managed Services provides continuous 24x7 remote monitoring (plus 24x7 call center availability) and proactive management of your data center using state-of-the-art tools, systems, and practices by a team of highly skilled and experienced Lenovo services professionals.

  Quarterly reviews check error logs, verify firmware & OS device driver levels, and software as needed. We'll also maintain records of latest patches, critical updates, and firmware levels, to ensure you systems are providing business value through optimized performance.

- **Technical Account Management (TAM)**

  A Lenovo Technical Account Manager helps you optimize the operation of your data center based on a deep understanding of your business. You gain direct access to your Lenovo TAM, who serves as your single point of contact to expedite service requests, provide status updates, and furnish reports to track incidents over time. In addition, your TAM will help proactively make service recommendations and manage your service relationship with Lenovo to make certain your needs are met.

- **Enterprise Server Software Support**

  Enterprise Software Support is an additional support service providing customers with software support on Microsoft, Red Hat, SUSE, and VMware applications and systems. Around the clock availability for critical problems plus unlimited calls and incidents helps customers address challenges fast, without incremental costs. Support staff can answer troubleshooting and diagnostic questions, address product comparability and interoperability issues, isolate causes of problems, report defects to software vendors, and more.

- **YourDrive YourData**

  Lenovo's YourDrive YourData is a multi-drive retention offering that ensures your data is always under your control, regardless of the number of drives that are installed in your Lenovo server. In the unlikely event of a drive failure, you retain possession of your drive while Lenovo replaces the failed drive part. Your data stays safely on your premises, in your hands. The YourDrive YourData service can be purchased in convenient bundles and is optional with Foundation Service. It is bundled with Essential Service and Advanced Service.

- **Health Check**

  Having a trusted partner who can perform regular and detailed health checks is central to maintaining efficiency and ensuring that your systems and business are always running at their best. Health Check supports Lenovo-branded server, storage, and networking devices, as well as select Lenovo-supported products from other vendors that are sold by Lenovo or a Lenovo-Authorized Reseller.

Examples of region-specific warranty terms are second or longer business day parts delivery or parts-only base warranty.

If warranty terms and conditions include onsite labor for repair or replacement of parts, Lenovo will dispatch a service technician to the customer site to perform the replacement. Onsite labor under base warranty is limited to labor for replacement of parts that have been determined to be field-replaceable units (FRUs). Parts that are determined to be customer-replaceable units (CRUs) do not include onsite labor under base warranty.

If warranty terms include parts-only base warranty, Lenovo is responsible for delivering only replacement parts that are under base warranty (including FRUs) that will be sent to a requested location for self-service. Parts-only service does not include a service technician being dispatched onsite. Parts must be changed at customer's own cost and labor and defective parts must be returned following the instructions supplied with the spare parts.

Lenovo Service offerings are region-specific. Not all preconfigured support and upgrade options are available in every region. For information about Lenovo service upgrade offerings that are available in your region, refer to the following resources:

- Service part numbers in Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com/#/services
- Lenovo Services Availability Locator
  http://lenovolocator.com/

For service definitions, region-specific details, and service limitations, please refer to the following documents:

- Lenovo Statement of Limited Warranty for Data Center Group (DCG) Servers and System Storage
  http://pcsupport.lenovo.com/us/en/solutions/ht503310
- Lenovo Data Center Services Agreement
  http://support.lenovo.com/us/en/solutions/ht116628

Services

Lenovo Services is a dedicated partner to your success. Our goal is to reduce your capital outlays, mitigate your IT risks, and accelerate your time to productivity.

Note: Some service options may not be available in all countries. For more information, go to https://www.lenovo.com/systems/services. For information about Lenovo service upgrade offerings that are available in your region, contact your local Lenovo sales representative or business partner.

Here's a more in-depth look at what we can do for you:

- **Asset Recovery Services**

  Asset Recovery Services (ARS) helps customers recover the maximum value from their end-of-life equipment in a cost-effective and secure way. On top of simplifying the transition from old to new equipment, ARS mitigates environmental and data security risks associated with data center equipment disposal. Lenovo ARS is a cash-back solution for equipment based on its remaining market value, yielding maximum value from aging assets and lowering total cost of ownership for your customers. For more information, see the ARS page, https://lenovopress.com/lp1266-reduce-e-waste-and-grow-your-bottom-line-with-lenovo-ars.

- **Assessment Services**

  An Assessment helps solve your IT challenges through an onsite, multi-day session with a Lenovo technology expert. We perform a tools-based assessment which provides a comprehensive and thorough review of a company's environment and technology systems. In addition to the technology based functional requirements, the consultant also discusses and records the non-functional business requirements, challenges, and constraints. Assessments help organizations like yours, no matter how large or small, get a better return on your IT investment and overcome challenges in the ever-changing technology landscape.

- **Design Services**

  Professional Services consultants perform infrastructure design and implementation planning to support your strategy. The high-level architectures provided by the assessment service are turned into low level designs and wiring diagrams, which are reviewed and approved prior to implementation. The implementation plan will demonstrate an outcome-based proposal to provide business capabilities through infrastructure with a risk-mitigated project plan.

- **Basic Hardware Installation**

  Lenovo experts can seamlessly manage the physical installation of your server, storage, or networking hardware. Working at a time convenient for you (business hours or off shift), the technician will unpack and inspect the systems on your site, install options, mount in a rack cabinet, connect to power and network, check and update firmware to the latest levels, verify operation, and dispose of the packaging, allowing your team to focus on other priorities.

- **Deployment Services**

  When investing in new IT infrastructures, you need to ensure your business will see quick time to value with little to no disruption. Lenovo deployments are designed by development and engineering teams who know our Products & Solutions better than anyone else, and our technicians own the process from delivery to completion. Lenovo will conduct remote preparation and planning, configure & integrate systems, validate systems, verify and update appliance firmware, train on administrative tasks, and provide post-deployment documentation. Customer's IT teams leverage our skills to enable IT staff to transform with higher level roles and tasks.

- **Integration, Migration, and Expansion Services**

  Move existing physical & virtual workloads easily, or determine technical requirements to support increased workloads while maximizing performance. Includes tuning, validation, and documenting ongoing run processes. Leverage migration assessment planning documents to perform necessary migrations.

Regulatory compliance

The ThinkSystem SR530 server conforms to the following regulations:

- United States: FCC Part 15, Class A; UL 60950-1
- Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1
- Mexico: NOM-19
- Argentina: IEC60950-1
- European Union: CE Mark (EN55022 Class A, IEC/EN60950-1, EN55024, EN61000-3-2, EN61000-3-3)
- Germany: TUV-GS (IEC/EN 60950-1, EK1-ITB2000)
- Russia, Kazakhstan, Belarus: EAC (TR CU 004/2011, TR CU 020/2011)
- China: CCC GB4943.1, GB9254 Class A, GB17625.1
- India: BIS
- Japan: VCCI, Class A
- Taiwan: BSMI CNS13438, Class A; CNS14336-1
- Korea: KN22, Class A; KN24
- Australia/New Zealand: AS/NZS CISPR 22 Class A
- Reduction of Hazardous Substances (ROHS)
- Energy Star 3.0 (excluding configurations with Bronze 3204, Gold 5222, or Platinum 8256 processors)

Note: For more information on the Energy Star 3.0 certification, refer to the *Energy Star 3.0 Certifications for ThinkSystem Servers* publication:
http://lenovopress.com/lp1230

External drive enclosures

The server supports attachment to external drive enclosures using a RAID controller with external ports or a SAS host bus adapter. Adapters supported by the server are listed in the SAS adapters for external storage section.

Note: Information provided in this section is for ordering reference purposes only. For the operating system and adapter support details, refer to the interoperability matrix for a particular storage enclosure that can be found on the Lenovo Data Center Support web site:
http://datacentersupport.lenovo.com

Table 50. External drive enclosures

Description	Part number		
	Worldwide	Japan	PRC
Lenovo Storage D1212 LFF Disk Expansion with Dual SAS IO Modules	4587A11	4587A1J	4587A1C
Lenovo Storage D1224 SFF Disk Expansion with Dual SAS IO Modules	4587A31	4587A3J	4587A3C
Lenovo Storage D3284 4TB x 84 HD Expansion Enclosure	641311F		
Lenovo Storage D3284 6TB x 84 HD Expansion Enclosure	641312F		
Lenovo Storage D3284 8TB x 84 HD Expansion Enclosure	641313F		
Lenovo Storage D3284 10TB x 84 HD Expansion Enclosure	641314F		

For details about supported drives, adapters, and cables, see the following Lenovo Press Product Guides:

- Lenovo Storage D1212 and D1224
  http://lenovopress.com/lp0512
- Lenovo Storage D3284
  http://lenovopress.com/lp0513

External storage systems

Lenovo offers the ThinkSystem DE Series and ThinkSystem DM Series external storage systems for high-performance storage. See the DE Series and DM Series product guides for specific controller models, expansion enclosures and configuration options:

- ThinkSystem DE Series Storage
  https://lenovopress.com/storage/thinksystem/de-series#rt=product-guide
- ThinkSystem DM Series Storage
  https://lenovopress.com/storage/thinksystem/dm-series#rt=product-guide

External backup units

The following table lists the external backup options that are offered by Lenovo.

Table 51. External backup options

Part number	Description
External RDX USB drives	
4T27A10725	ThinkSystem RDX External USB 3.0 Dock
External SAS tape backup drives	
6160S6E	IBM TS2260 Tape Drive Model H6S
6160S7E	IBM TS2270 Tape Drive Model H7S
6160S8E	IBM TS2280 Tape Drive Model H8S
External SAS tape backup autoloaders	
6171S5R	IBM TS2900 Tape Autoloader w/LTO5 HH SAS
6171S6R	IBM TS2900 Tape Autoloader w/LTO6 HH SAS
6171S7R	IBM TS2900 Tape Autoloader w/LTO7 HH SAS
External tape backup libraries	
6741A1F	IBM TS4300 3U Tape Library-Base Unit
6741A3F	IBM TS4300 3U Tape Library-Expansion Unit
Full High 8 Gb Fibre Channel for TS4300	
01KP954	LTO 8 FH Fibre Channel Drive
01KP938	LTO 7 FH Fibre Channel Drive
01KP935	LTO 6 FH Fibre Channel Drive
Half High 8 Gb Fibre Channel for TS4300	
01KP952	LTO 8 HH Fibre Channel Drive
01KP936	LTO 7 HH Fibre Channel Drive
01KP933	LTO 6 HH Fibre Channel Drive
Half High 6 Gb SAS for TS4300	
01KP953	LTO 8 HH SAS Drive
01KP937	LTO 7 HH SAS Drive
01KP934	LTO 6 HH SAS Drive

For more information, see the list of Product Guides in the Backup units category:
https://lenovopress.com/servers/options/backup

Fibre Channel SAN switches

Lenovo offers the ThinkSystem DB Series of Fibre Channel SAN switches and directors for high-performance storage expansion. See the DB Series product guides for models and configuration options:

- ThinkSystem DB Series SAN Switches and Directors: https://lenovopress.com/storage/switches/rack#rt=product-guide

Rack cabinets

The following table lists the supported rack cabinets.

Table 52. Rack cabinets

Part number	Description
7D2B0001WW / 7D2N0001WW	12U 1200mm Deep Micro Datacenter Rack
7D2C0001WW / 7D2P0001WW	18U 1200mm Deep Micro Datacenter Rack
93072RX	25U Standard Rack
93072PX	25U Static S2 Standard Rack
93634PX	42U 1100mm Dynamic Rack
93634EX	42U 1100mm Dynamic Expansion Rack
93604PX	42U 1200mm Deep Dynamic Rack
93614PX	42U 1200mm Deep Static Rack
93084EX	42U Enterprise Expansion Rack
93084PX	42U Enterprise Rack
93074RX	42U Standard Rack

For specifications about these racks, see the Lenovo Rack Cabinet Reference, available from: https://lenovopress.com/lp1287-lenovo-rack-cabinet-reference

For more information, see the list of Product Guides in the Rack cabinets category: https://lenovopress.com/servers/options/racks

KVM switches and consoles

The following table lists the supported KVM consoles, keyboards, and KVM switches.

Table 53. Console keyboards

Part number	Description
Console keyboards	
7ZB7A05469	ThinkSystem Keyboard w/ Int. Pointing Device USB - Arabic 253 RoHS v2
7ZB7A05468	ThinkSystem Keyboard w/ Int. Pointing Device USB - Belg/UK 120 RoHS v2
7ZB7A05206	ThinkSystem Keyboard w/ Int. Pointing Device USB - Czech 489 RoHS v2
7ZB7A05207	ThinkSystem Keyboard w/ Int. Pointing Device USB - Danish 159 RoHS v2
7ZB7A05208	ThinkSystem Keyboard w/ Int. Pointing Device USB - Dutch 143 RoHS v2
7ZB7A05210	ThinkSystem Keyboard w/ Int. Pointing Device USB - Fr/Canada 445 RoHS v2
7ZB7A05209	ThinkSystem Keyboard w/ Int. Pointing Device USB - French 189 RoHS v2
7ZB7A05211	ThinkSystem Keyboard w/ Int. Pointing Device USB - German 129 RoHS v2
7ZB7A05212	ThinkSystem Keyboard w/ Int. Pointing Device USB - Greek 219 RoHS v2
7ZB7A05213	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hebrew 212 RoHS v2
7ZB7A05214	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hungarian 208 RoHS v2

Part number	Description
7ZB7A05215	ThinkSystem Keyboard w/ Int. Pointing Device USB - Italian 141 RoHS v2
7ZB7A05216	ThinkSystem Keyboard w/ Int. Pointing Device USB - Japanese 194 RoHS v2
7ZB7A05217	ThinkSystem Keyboard w/ Int. Pointing Device USB - Korean 413 RoHS v2
7ZB7A05218	ThinkSystem Keyboard w/ Int. Pointing Device USB - LA Span 171 RoHS v2
7ZB7A05219	ThinkSystem Keyboard w/ Int. Pointing Device USB - Norwegian 155 RoHS v2
7ZB7A05220	ThinkSystem Keyboard w/ Int. Pointing Device USB - Polish 214 RoHS v2
7ZB7A05221	ThinkSystem Keyboard w/ Int. Pointing Device USB - Portuguese 163 RoHS v2
7ZB7A05222	ThinkSystem Keyboard w/ Int. Pointing Device USB - Russian 441 RoHS v2
7ZB7A05223	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovak 245 RoHS v2
7ZB7A05231	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovenian 234 RoHS v2
7ZB7A05224	ThinkSystem Keyboard w/ Int. Pointing Device USB - Spanish 172 RoHS v2
7ZB7A05225	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swed/Finn 153 RoHS v2
7ZB7A05226	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swiss F/G 150 RoHS v2
7ZB7A05227	ThinkSystem Keyboard w/ Int. Pointing Device USB - Thai 191 RoHS v2
7ZB7A05467	ThinkSystem Keyboard w/ Int. Pointing Device USB - Trad Chinese/US 467 RoHS v2
7ZB7A05228	ThinkSystem Keyboard w/ Int. Pointing Device USB - Turkish 179 RoHS v2
7ZB7A05229	ThinkSystem Keyboard w/ Int. Pointing Device USB - UK Eng 166 RoHS v2
7ZB7A05470	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Eng 103P RoHS v2
7ZB7A05230	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Euro 103P RoHS v2
ThinkSystem Digital and Analog KVM Console switches and cables	
1754D1T	ThinkSystem Digital 2x1x16 KVM Switch (DVI video output port)
1754A1T	ThinkSystem Analog 1x8 KVM Switch (DVI video output port)
4X97A11108	ThinkSystem VGA to DVI Conversion Cable
4X97A11109	ThinkSystem Single-USB Conversion Cable for Digital KVM
4X97A11107	ThinkSystem Dual-USB Conversion Cable for Digital KVM
4X97A11106	ThinkSystem USB Conversion Cable for Analog KVM
GCM and LCM Console switches and cables	
1754D2X	Global 4x2x32 Console Manager (GCM32)
1754D1X	Global 2x2x16 Console Manager (GCM16)
1754A2X	Local 2x16 Console Manager (LCM16)
1754A1X	Local 1x8 Console Manager (LCM8)
43V6147	Single Cable USB Conversion Option (UCO)
39M2895	USB Conversion Option (4 Pack UCO)
46M5383	Virtual Media Conversion Option Gen2 (VCO2)
46M5382	Serial Conversion Option (SCO)

For more information, see the list of Product Guides in the KVM Switches and Consoles category:
http://lenovopress.com/servers/options/kvm

Power distribution units

The following table lists the power distribution units (PDUs) that are offered by Lenovo.

Table 54. Power distribution units

Part number	Description
0U Basic PDUs	
00YJ776	0U 36 C13/6 C19 24A/200-240V 1 Phase PDU with NEMA L6-30P line cord
00YJ777	0U 36 C13/6 C19 32A/200-240V 1 Phase PDU with IEC60309 332P6 line cord
00YJ778	0U 21 C13/12 C19 32A/200-240V/346-415V 3 Phase PDU with IEC60309 532P6 line cord
00YJ779	0U 21 C13/12 C19 48A/200-240V 3 Phase PDU with IEC60309 460P9 line cord
Switched and Monitored PDUs	
00YJ780	0U 20 C13/4 C19 Switched and Monitored 32A/200-240V/1Ph PDU w/ IEC60309 332P6 line cord
00YJ781	0U 20 C13/4 C19 Switched and Monitored 24A/200-240V/1Ph PDU w/ NEMA L6-30P line cord
00YJ782	0U 18 C13/6 C19 Switched / Monitored 32A/200-240V/346-415V/3Ph PDU w/ IEC60309 532P6 cord
00YJ783	0U 12 C13/12 C19 Switched and Monitored 48A/200-240V/3Ph PDU w/ IEC60309 460P9 line cord
46M4003	1U 9 C19/3 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
46M4004	1U 12 C13 Switched and Monitored DPI PDU (without line cord)
46M4005	1U 12 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
Ultra Density Enterprise PDUs (9x IEC 320 C13 + 3x IEC 320 C19 outlets)	
71762NX	Ultra Density Enterprise C19/C13 PDU Module (without line cord)
71763NU	Ultra Density Enterprise C19/C13 PDU 60A/208V/3ph with IEC 309 3P+Gnd line cord
C13 Enterprise PDUs (12x IEC 320 C13 outlets)	
39M2816	DPI C13 Enterprise PDU+ (without line cord)
39Y8941	DPI Single Phase C13 Enterprise PDU (without line cord)
C19 Enterprise PDUs (6x IEC 320 C19 outlets)	
39Y8948	DPI Single Phase C19 Enterprise PDU (without line cord)
39Y8923	DPI 60A 3 Phase C19 Enterprise PDU with IEC 309 3P+G (208 V) fixed line cord
Front-end PDUs (3x IEC 320 C19 outlets)	
39Y8938	DPI 30amp/125V Front-end PDU with NEMA L5-30P line cord
39Y8939	DPI 30amp/250V Front-end PDU with NEMA L6-30P line cord
39Y8934	DPI 32amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8940	DPI 60amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8935	DPI 63amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
NEMA PDUs (6x NEMA 5-15R outlets)	
39Y8905	DPI 100-127V PDU with Fixed NEMA L5-15P line cord
Line cords for PDUs that ship without a line cord	
40K9611	DPI 32a Line Cord (IEC 309 3P+N+G)
40K9612	DPI 32a Line Cord (IEC 309 P+N+G)
40K9613	DPI 63a Cord (IEC 309 P+N+G)
40K9614	DPI 30a Line Cord (NEMA L6-30P)
40K9615	DPI 60a Cord (IEC 309 2P+G)
40K9617	DPI Australian/NZ 3112 Line Cord
40K9618	DPI Korean 8305 Line Cord

For more information, see the Lenovo Press documents in the PDU category:
https://lenovopress.com/servers/options/pdu

Uninterruptible power supply units

The following table lists the uninterruptible power supply (UPS) units that are offered by Lenovo.

Table 55. Uninterruptible power supply units

Part number	Description
55941AX	RT1.5kVA 2U Rack or Tower UPS (100-125VAC)
55941KX	RT1.5kVA 2U Rack or Tower UPS (200-240VAC)
55942AX	RT2.2kVA 2U Rack or Tower UPS (100-125VAC)
55942KX	RT2.2kVA 2U Rack or Tower UPS (200-240VAC)
55943AX	RT3kVA 2U Rack or Tower UPS (100-125VAC)
55943KX	RT3kVA 2U Rack or Tower UPS (200-240VAC)
55945KX	RT5kVA 3U Rack or Tower UPS (200-240VAC)
55946KX	RT6kVA 3U Rack or Tower UPS (200-240VAC)
55948KX	RT8kVA 6U Rack or Tower UPS (200-240VAC)
55949KX	RT11kVA 6U Rack or Tower UPS (200-240VAC)
55948PX	RT8kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55949PX	RT11kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55943KT†	ThinkSystem RT3kVA 2U Standard UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55943LT†	ThinkSystem RT3kVA 2U Long Backup UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55946KT†	ThinkSystem RT6kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)
5594XKT†	ThinkSystem RT10kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)

† Only available in China and countries in the Asia Pacific region.

For more information, see the list of Product Guides in the UPS category:
https://lenovopress.com/servers/options/ups

Lenovo Financial Services

Lenovo Financial Services reinforces Lenovo's commitment to deliver pioneering products and services that are recognized for their quality, excellence, and trustworthiness. Lenovo Financial Services offers financing solutions and services that complement your technology solution anywhere in the world.

We are dedicated to delivering a positive finance experience for customers like you who want to maximize your purchase power by obtaining the technology you need today, protect against technology obsolescence, and preserve your capital for other uses.

We work with businesses, non-profit organizations, governments and educational institutions to finance their entire technology solution. We focus on making it easy to do business with us. Our highly experienced team of finance professionals operates in a work culture that emphasizes the importance of providing outstanding customer service. Our systems, processes and flexible policies support our goal of providing customers with a positive experience.

We finance your entire solution. Unlike others, we allow you to bundle everything you need from hardware and software to service contracts, installation costs, training fees, and sales tax. If you decide weeks or months later to add to your solution, we can consolidate everything into a single invoice.

Our Premier Client services provide large accounts with special handling services to ensure these complex transactions are serviced properly. As a premier client, you have a dedicated finance specialist who manages your account through its life, from first invoice through asset return or purchase. This specialist develops an in-depth understanding of your invoice and payment requirements. For you, this dedication provides a high-quality, easy, and positive financing experience.

For your region specific offers please ask your Lenovo sales representative or your technology provider about the use of Lenovo Financial Services. For more information, see the following Lenovo website:

https://www.lenovo.com/us/en/landingpage/lenovo-financial-services/

Related publications and links

For more information, see these resources:

- ThinkSystem SR530 product page
  https://www.lenovo.com/us/en/data-center/servers/racks/ThinkSystem-SR530/p/77XX7SRSR53
- Datasheet for the ThinkSystem SR530:
  https://lenovopress.com/ds0002-lenovo-thinksystem-sr530
- 3D Interactive Tour of the ThinkSystem SR530:
  https://lenovopress.com/lp0670-3d-tour-thinksystem-sr530
- Walkthrough Video for the ThinkSystem SR530:
  https://lenovopress.com/lp0744-thinksystem-sr530-server-video-walkthrough
- User Manuals for the ThinkSystem SR530:
  https://thinksystem.lenovofiles.com/help/topic/7X07/introduction.html?cp=4_2
  - Quick Start Guide
  - Setup Guide
  - Rack Installation Guides
  - Maintenance Manual
  - Messages and Codes Reference
  - UEFI Manual
- Lenovo Data Center Support Downloads - ThinkSystem SR530:
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x07/downloads
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x08/downloads
- Lenovo Hardware Installation & Removal Videos on the ThinkSystem SR530:
  - YouTube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
  - Youku: https://list.youku.com/albumlist/show/id_50437162
- Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com

Related product families

Product families related to this document are the following:

- 2-Socket Rack Servers
- ThinkSystem SR530 Server

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2021. All rights reserved.

This document, LP1045, was created or updated on March 2, 2021.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  http://lenovopress.com/LP1045
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at http://lenovopress.com/LP1045.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
Bootable Media Creator
Flex System
Lenovo Services
RackSwitch
System x®
ThinkSystem
TopSeller
TruDDR4
UpdateXpress System Packs
XClarity®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Hyper-V®, Microsoft®, PowerShell, Windows PowerShell®, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Lenovo ThinkSystem SR530 Server (Xeon SP Gen 2)

Product Guide

Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.

Featuring the second generation of the Intel Xeon Processor Scalable Family (Xeon SP Gen 2), the SR530 server offers a balance of performance, capacity and value. The SR530 server supports up to two processors, up to 768 GB of 2933 MHz TruDDR4 memory, 8x 2.5-inch or 4x 3.5-inch drive bays with an extensive choice of SAS/SATA SSDs and SAS/SATA HDDs, and flexible I/O expansion options with a LOM slot and up to 3x PCIe slots.

The SR530 server offers basic software RAID or advanced hardware RAID protection and a wide range of networking options, including embedded LOM, selectable LOM, ML2, and PCIe network adapters. The next-generation Lenovo XClarity Controller, which is built into the SR530 server, provides advanced service processor control, monitoring, and alerting functions.

The following figure shows the ThinkSystem SR530 server with 3.5-inch front hot-swap drives. Other drive configurations are also available.



Figure 1. Lenovo ThinkSystem SR530 with 3.5-inch hot-swap drives

Did you know?

The SR530 server delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies that can deliver 96% (Titanium) or 94% (Platinum) efficiency at 50% load when connected to a 200 - 240 V AC power source.

The SR530 server is designed to meet ASHRAE A4 standards (up to 45 °C) in select configurations, which enable customers to lower energy costs, while still maintaining world-class reliability.

Key features

The SR530 server offers a balance of processing power, expandability, and cost for small and medium businesses up to the large enterprise. Ease of use and comprehensive systems management tools help make deployment easier and efficient design improves your business environment and helps save operational costs.

Scalability and performance

The SR530 server offers numerous features to boost performance, improve scalability, and reduce costs:

- Improves productivity by offering superior system performance with the second generation of the Intel Xeon Processor Scalable Family with up to 22-core processors, up to 30.25 MB of last level cache (LLC), up to 2933 MHz memory speeds, and up to 10.4 GT/s Ultra Path Interconnect (UPI) links.
    - Support for up to two processors, 44 cores, and 88 threads allows to maximize the concurrent execution of multithreaded applications.
    - Intelligent and adaptive system performance with energy efficient Intel Turbo Boost 2.0 Technology allows CPU cores to run at maximum speeds during peak workloads by temporarily going beyond processor thermal design power (TDP).
    - Intel Hyper-Threading Technology boosts performance for multithreaded applications by enabling simultaneous multithreading within each processor core, up to two threads per core.
    - Intel Virtualization Technology integrates hardware-level virtualization hooks that allow operating system vendors to better utilize the hardware for virtualization workloads.
    - Intel Speed Select Technology provides improvements in server utilization and guaranteed per-core performance service levels with more granular control over processor performance.
    - Intel Deep Learning Boost (Vector Neural Network Instruction set [VNNI]) is designed to deliver significant, more efficient Deep Learning (Inference) acceleration for high-performance Artificial Intelligence (AI) workloads.
    - Intel Advanced Vector Extensions 512 (AVX-512) enable acceleration of enterprise-class and high performance computing (HPC) workloads.
- Helps maximize system performance for data intensive applications with up to 2933 MHz memory speeds and up to 768 GB of memory capacity.
- Offers flexible and scalable internal storage in a 1U rack form factor with up to 8x 2.5-inch drives for performance-optimized configurations or up to 4x 3.5-inch drives for capacity-optimized configurations, providing a wide selection of SAS/SATA HDDs/SSDs.
- Provides I/O scalability with a LOM slot and up to three PCI Express (PCIe) 3.0 I/O expansion slots in a 1U rack form factor.
- Reduces I/O latency and increases overall system performance with Intel Integrated I/O Technology that embeds the PCI Express 3.0 controller into the Intel Xeon Processor Scalable Family.

Availability and serviceability

The SR530 server provides many features to simplify serviceability and increase system uptime:

- Offers protection in the event of a non-correctable memory failure with Single Device Data Correction (SDDC, also known as Chipkill, requires x4-based DIMMs), Adaptive Double Device Data Correction (ADDDC, also known as Redundant Bit Steering [RBS], requires x4-based DIMMs and Intel Xeon Gold or Platinum processors), memory mirroring, and memory rank sparing.
- Provides easy access to upgrades and serviceable parts (such as processors, memory DIMMs, and adapter cards) with tool-less cover removal.
- Offers affordable data protection with software RAID and Simple Swap drives and advanced hardware RAID data redundancy with hot-swap drives.
- Provides availability for applications with redundant hot-swap power supplies and redundant non-hot-swap fans.
- Speeds up troubleshooting tasks to reduce service time with diagnostics built into the XClarity Provisioning Manager.

- Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
- Continuously monitors system parameters, triggers alerts, and performs recovery actions in case of failure to minimize downtime with Built-in XClarity Controller (XCC).
- Provides quick access to system status, firmware, network, health, and alerts information via Virtual Operator Panel from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access.

Manageability and security

Powerful systems management features simplify local and remote management of the SR530 server and deliver enterprise-class data protection:

- Provides advanced service processor control, monitoring, and alerting functions with XClarity Controller, a next generation service processor.
- Improves Unified Extensible Firmware Interface (UEFI) system setup, configuration, updates, simplified error handling, and operating system deployment with the embedded XClarity Provisioning Manager.
- Offers XClarity Essentials software tools that can help you set up, use, and maintain the server.
- Increases uptime, reduces costs, and improves productivity through advanced server management capabilities with Lenovo XClarity Administrator that provides comprehensive hardware management.
- Provides on-the-go monitoring and management of devices in XClarity Administrator from anywhere with the Lenovo XClarity mobile app, which can help improve efficiency and reduce downtime risks.
- Centralizes infrastructure resource management with Lenovo XClarity Integrators for VMware vCenter and Microsoft System Center, extending XClarity Administrator features to virtualization management software tools and enabling users to deploy and manage infrastructure end-to-end.
- Offers advanced cryptographic functionality (such as digital signatures and remote attestation) with an integrated Trusted Platform Module (TPM) or optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC).
- Keeps user data safe with Lenovo Business Vantage, a security software tool suite designed to work with the Trusted Cryptographic Module (available only in PRC).
- Offers enterprise-class data protection with advanced RAID and optional self-encrypting drives.
- Provides faster, stronger encryption with industry-standard AES NI support.
- Helps prevent certain classes of malicious buffer overflow attacks with Intel Execute Disable Bit functionality, when combined with a supporting operating system.
- Enhances security through hardware-based resistance to malicious software attacks with Intel Trusted Execution Technology, allowing an application to run in its own isolated space, protected from all other software running on a system.

Energy efficiency

The SR530 server offers the following energy-efficiency features to save energy, reduce operational costs, increase energy availability, and contribute to the green environment:

- Delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies.
- Enables customers to lower energy costs with design to meet ASHRAE A4 standards in select configurations.
- Reduces power drawn with Intel Intelligent Power Capability that powers individual processor elements on and off as needed.
- Helps reduce power consumption with variable speed fans.
- Helps achieve lower heat output and reduced cooling needs with Lenovo XClarity Energy Manager that provides advanced data center power notification, analysis, and policy-based management.

Components and connectors

The following figure shows the front of the SR530 server with four 3.5-inch drive bays.

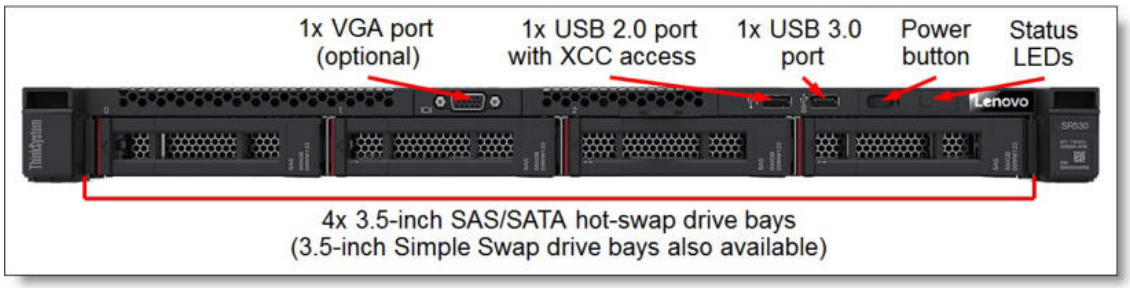


Figure 2. Front view of the SR530: 4x 3.5-inch drive bays

The following figure shows the front of the SR530 server with eight 2.5-inch drive bays.

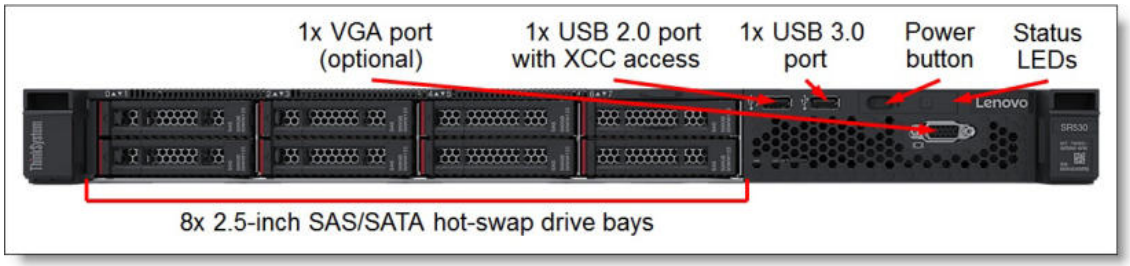


Figure 3. Front view of the SR530: 8x 2.5-inch drive bays

The front of the SR530 server includes the following components:

- Up to 8x 2.5-inch or 4x 3.5-inch hot-swap drive bays, or 4x 3.5-inch Simple Swap drive bays.
- One VGA port (optional).
- One USB 3.0 port.
- One USB 2.0 port with XClarity Controller access.
- Power button.
- Status LEDs.

The following figure shows the rear of the SR530 server with three PCIe low profile slots.

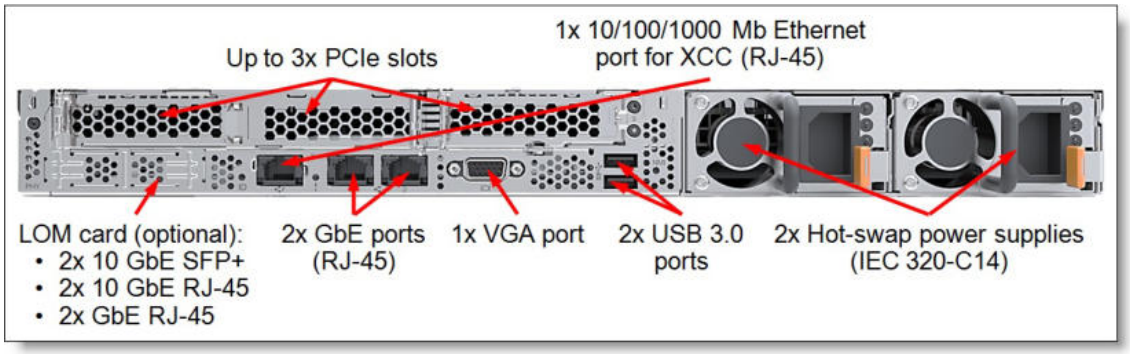


Figure 4. Rear view of the SR530

The rear of the SR530 server includes the following components:

- Up to three PCIe expansion slots (depending on the riser cards selected).
- One LOM card slot.
- One 1 GbE port for XClarity Controller.
- One VGA port.
- Two USB 3.0 ports.
- Up to two hot-swap power supplies.

The following figure shows the locations of key components inside the SR530 server.

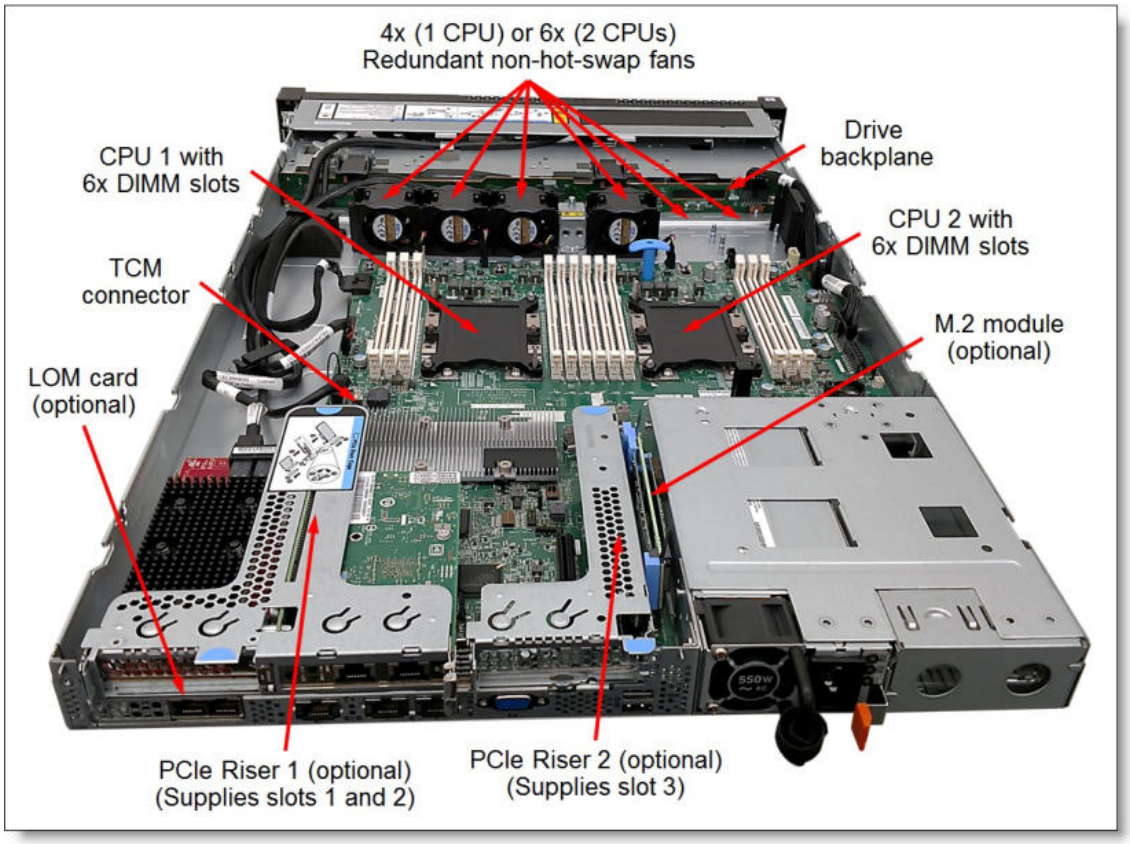


Figure 5. Internal view of the SR530

The following key components are located inside the SR530 server:

- Up to two processors.
- 12 DIMM slots (6 DIMM slots per processor).
- Drive backplanes.
- One M.2 module connector.
- One LOM card connector.
- Two slots for PCIe riser cards.
- One TCM connector.
- Four (one processor) or six (two processors) non-hot-swap system fans.

System specifications

The following table lists the system specifications for the SR530 server.

Table 1. SR530 system specifications

Attribute	Specification
Machine types	7X07 - 1 year warranty 7X08 - 3 year warranty
Form factor	1U rack-mount.
Processor	Up to two Intel Xeon Gen 2 Bronze, Silver, Gold, or Platinum processors: • Up to 22 cores (1.9 GHz core speeds) • Up to 3.8 GHz core speeds (4 cores) • Two UPI links up to 10.4 GT/s each • Up to 30.25 MB cache • Up to 2933 MHz memory speed

Attribute	Specification
Chipset	Intel C622.
Memory	Up to 12 DIMM sockets (6 DIMMs per processor; six memory channels per processor with one DIMM per channel) with support for the following TruDDR4 RDIMM types and capacities: • 8 GB, 16 GB, 32 GB, and 64 GB 2933 MHz. • 16 GB and 32 GB 2666 MHz.
Memory protection	Error correction code (ECC), SDDC (for x4-based memory DIMMs), ADDDC (for x4-based memory DIMMs, requires Intel Xeon Gold or Platinum processors), memory mirroring, memory rank sparing, patrol scrubbing, and demand scrubbing.
Memory capacity	Up to 768 GB with 12x 64 GB RDIMMs (Up to 384 GB per processor).
Drive bays	• 4 LFF SATA Simple Swap drive bays • 4 LFF SAS/SATA hot-swap drive bays • 8 SFF SAS/SATA hot-swap drive bays

Internal storage capacity	• 2.5-inch drives:
	  ◦ 122.88TB using 8x 15.36TB 2.5-inch SAS/SATA SSDs
	  ◦ 19.2TB using 8x 2.4TB 2.5-inch HDDs
	• 3.5-inch drives:
	  ◦ 72TB using 4x 18TB 3.5-inch HDDs
	  ◦ 30.72TB using 4x 7.68TB 3.5-inch SAS/SATA SSDs

Storage controller	6 Gbps SATA
	• Non-RAID: Onboard SATA AHCI
	• RAID 0/1/10/5: Onboard SATA RAID (Intel RSTe)
	
	12 Gbps SAS/6 Gbps SATA RAID
	• RAID 0/1/10/5/50:
	  ◦ RAID 530-8i
	  ◦ RAID 730-8i 1GB Cache
	• RAID 0/1/10/5/50/6/60:
	  ◦ RAID 730-8i 2GB Flash
	  ◦ RAID 930-8i 2GB Flash
	  ◦ RAID 930-16i 4GB or 8GB Flash
	
	12 Gbps SAS/6 Gbps SATA non-RAID: 430-8i HBA

Optical drive bays	None. Support for an external USB DVD RW Optical Disk Drive (SeeOptical drives).

Network interfaces	• 2x Integrated 1 GbE RJ-45 ports (no 10/100 Mb support)
	• Onboard LOM slot for up to two additional 1/10 Gb Ethernet ports:
	  ◦ 2x 1 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE SFP+ ports (no 10/100 Mb support)
	• Optional Mezzanine LOM (ML2) slot for dual-port 10 GbE cards with SFP+ or RJ-45 connectors.
	• 1x RJ-45 10/100/1000 Mb Ethernet systems management port.

I/O expansion slots	Up to three slots depending on the riser cards installed. The slots are as follows: • Slot 1: PCIe 3.0 x8; low profile • Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length • Slot 3: PCIe 3.0 x8 or x16; low profile PCIe x16 slot 3 requires the second processor to be installed.
Ports	• Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. • Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
Cooling	Four (one processor) or six (two processors) non-hot-swap system fans with N+1 redundancy.
Power supply	Up to two redundant hot-swap 550 W or 750 W (100 - 240 V) High Efficiency Platinum or 750 W (200 - 240 V) High Efficiency Titanium AC power supplies. HVDC support (PRC only).

Attribute	Specification
Video	Matrox G200 with 16 MB memory integrated into the XClarity Controller. Maximum resolution is 1920x1200 at 60 Hz with 32 bits per pixel.
Hot-swap parts	Drives (select models) and power supplies.
Systems management	XClarity Controller (XCC) Standard, Advanced, or Enterprise (Pilot 4 chip), proactive platform alerts, XClarity Provisioning Manager, XClarity Essentials, XClarity Administrator, XClarity Integrators for VMware vCenter and Microsoft System Center, XClarity Energy Manager, Capacity Planner.
Security features	Power-on password, administrator's password, secure firmware updates, Trusted Platform Module (TPM) 1.2 or 2.0 (configurable UEFI setting). Optional lockable front bezel. Optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC). Optional Lenovo Business Vantage security software (available only in PRC).
Operating systems	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. See the Operating systems section for specifics.
Warranty	One-year (7X07) or three-year (7X08) customer-replaceable unit (CRU) and onsite limited warranty with 9x5 Next Business Day Parts Delivered.
Service and support	Optional service upgrades are available through Lenovo Services: 2-hour or 4-hour response time, 6-hour or 24-hour committed service repair, warranty extension up to 5 years, 1-year or 2-year post-warranty extensions, YourDrive Your Data, Enterprise Software Support, and Basic Hardware Installation Services.
Dimensions	Width: 435 mm (17.1 in.), height: 43 mm (1.7 in.), depth: 750 mm (29.5 in.). See Physical specifications for details.
Weight	Minimum configuration: 10.2 kg (22.5 lb), maximum: 16 kg (35.3 lb)

Models

ThinkSystem SR530 models can be configured by using the Lenovo Data Center Solution Configurator (DCSC).

Configure-to-order (CTO) models are used to create models with factory-integrated server customizations. For CTO models, two base CTO models are available for the SR530 as listed in the following table, CTO1WW and CTOLWW:

- The CTO1WW base CTO model is for general business and is selectable by choosing **General Purpose** mode in DCSC.
- The CTOLWW base model is intended for High Performance Computing (HPC) and Artificial Intelligence (AI) configurations and solutions, including configurations for Lenovo Scalable Infrastructure (LeSI), and is enabled using either the **HPC & AI LeSI Solutions** mode or **HPC & AI ThinkSystem Hardware** mode in DCSC. CTOLWW configurations can also be built using System x and Cluster Solutions Configurator (x-config).

Preconfigured server models may also be available for the SR530, however these are region-specific; that is, each region may define their own server models, and not all server models are available in every region.

The following table lists the base CTO models of the ThinkSystem SR530 server.

Table 2. Base CTO models

Description	Machine Type/Model General purpose	Machine Type/Model for HPC and AI
ThinkSystem SR530 - 3 year Warranty	7X08CTO1WW	7X08CTOLWW
ThinkSystem SR530 - 1 year Warranty	7X07CTO1WW	7X07CTOLWW

The following table lists the base chassis for CTO models of the SR530 server.

Table 3. Base chassis for CTO models

Feature code	Description
AV0T	ThinkSystem SR530 3.5" Chassis with 4 Bays
AV0S	ThinkSystem SR530 2.5" Chassis with 8 Bays

All models of the SR530 server are shipped with the following items:

- *Rack Installation Guide*
- *Electronic Publications Flyer*

Models table conventions: The model tables shown in this section use the following conventions:

- XClarity Controller: "S" = Standard, "A" = Advanced, "E" = Enterprise.
- Front VGA port: "Y" = Included; "N" = Not included, optional.
- Tool-less Rail Kit: "Y" = Included; "N" = Not included, optional.
- Cable Management Arm (CMA): "Y" = Included; "N" = Not included, optional.
- Power cord:
  - "R1" = 1.5 m C13-C14 rack power cable.
  - "R2" = 2.8 m C13-C14 rack power cable.
  - "L2" = 2.8 m line cord.
  - "N" = Not included; see Power supplies and cables for the ordering information.

The following tables list the models of the SR530 server for the following regions:

- Brazil
- Latin America (except Brazil)
- Europe, Middle East, and Africa (EMEA)
- India
- Hong Kong, Taiwan, Korea
- Japan
- Association of Southeast Asian Nations (ASEAN)
- Australia and New Zealand

Table 4. SR530 server models: Brazil

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Brazil													
7X08A0A1BR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
TopSeller models - Brazil													
7X08100QBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x SATA AHCI	4 / 4 SS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A0A2BR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
7X08A09YBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09ZBR	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0APBR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 5. SR530 server models: Latin America (except Brazil)

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
TopSeller models - Latin America (except Brazil)													
7X08A09WLA	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09XLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0AQLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	Y	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 6. SR530 server models: EMEA

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - EMEA													
7X08A0ACEA	1x 3206R 8C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	R2
7X08A075EA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AZEA	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	None	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	N	R2
7X08A0ADEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AHEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A078EA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A06WEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A07FEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AEEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AJEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A07CEA	1x 4214 12C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AKEA	1x 4214R 12C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A070EA	1x 4216 16C 100W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0ALEA	1x 5218R 20C 125W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 7. SR530 server models: India

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - India													
7X08A08TSG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07USG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A07WSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A084SG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07YSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A079SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06VSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07SSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07JSG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ASG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08PSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A098SG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A077SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A095SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07RSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08VSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08WSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06USG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A094SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A089SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ESG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08KSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 8. SR530 server models: Hong Kong, Taiwan, Korea

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Hong Kong, Taiwan, Korea													
7X08A09CCN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085CN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08100VCN	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	Y	N	Y
7X08A071CN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YCN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09BCN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080CN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CCN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A082CN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09DCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07NCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A088CN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GCN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A087CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08MCN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092CN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06XCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07KCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 9. SR530 server models: Japan

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Japan													
7X08A0AWJP	1x 5218R 20C 125W 2.1GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
TopSeller models - Japan													
7X08A08AJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08DJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08EJP	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07HJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08SJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08QJP	1x 4214 12C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07QJP	1x 4215 8C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07LJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07MJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08HJP	1x 5215 10C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08FJP	1x 5217 8C 115W 3.0GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08YJP	1x 5218 16C 125W 2.3GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A090JP	1x 5220 18C 125W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08UJP	1x 5222 4C 105W 3.8GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A096JP	1x 6230 20C 125W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A0AXJP	1x 3206R 8C 85W 1.9GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AYJP	1x 4210R 10C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AVJP	1x 4214R 12C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 10. SR530 server models: ASEAN

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - ASEAN													
7X08A099SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A086SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A081SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ZSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A083SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A093SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07VSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ESG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RSG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A073SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A097SG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07PSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07TSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09FSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A091SG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 11. SR530 server models: Australia and New Zealand

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Australia and New Zealand (1-year warranty)													
7X07A00VAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	None	No bays / 8 HS SFF	Open bay	Open slot	None	1x 550W	S	Y	Y	N	R2
Relationship models - Australia and New Zealand (3-year warranty)													
7X08A099AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A071AU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YAU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XAU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080AU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A0B0AU	1x 4216 16C 100W 2.1GHz	1x 32GB(x4) 2933MHz	1x RAID 930-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W Platinum	E	Y	Y	N	Y
7X08A07VAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07EAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076AU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BAU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LAU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092AU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A06XAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
TopSeller models - Australia and New Zealand (3-year warranty)													
7X08A09GAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09HAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09LAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09KAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09NAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09MAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09JAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Processors

The SR530 server supports one or two Intel Xeon Bronze, Silver, Gold, or Platinum processors of up to 125 W TDP. The following table lists the specifications of the processors for the SR530 server.

Processor specifications table abbreviations:

- UPI: Ultra Path Interconnect
- TDP: Thermal Design Power
- HT: Hyper-Threading
- TB: Turbo Boost 2.0
- VT-x: Virtualization Technology
- VT-d: Virtualization Technology for Directed I/O
- SST-PP: Speed Select Technology - Performance Profile
- FMA: Fused-Multiply Add (AVX-512)
- RAS: Reliability, Availability, and Serviceability
    - Std: Standard RAS
    - Adv: Advanced RAS

Table 12. Processor specifications

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
Intel Xeon Bronze processors														
3204	6 / 6	1.9 / 1.9 GHz	8.25 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	Std

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
3206R	8 / 8	1.9 / 1.9 GHz	11 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	
Intel Xeon Silver processors														
4208	8 / 16	2.1 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4209T	8 / 16	2.2 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	70 W	Y	Y	Y	Y	N	1	Std
4210	10 / 20	2.2 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4210R	10 / 20	2.4 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4214R	12 / 24	2.4 / 3.5 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214Y	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	Y	1	Std
	10 / 20	2.3 / 3.2 GHz												
	8 / 16	2.4 / 3.2 GHz												
4215	8 / 16	2.5 / 3.5 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4216	16 / 32	2.1 / 3.2 GHz	22 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
Intel Xeon Gold processors														
5215	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	1 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5215L	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	4.5 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5217	8 / 16	3.0 / 3.7 GHz	11 MB	2666 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	1	Adv
5218	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218B	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218R	20 / 40	2.1 / 4.0 GHz	27.5 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218T	16 / 32	2.1 / 3.8 GHz	22 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5220	18 / 36	2.2 / 3.9 GHz	24.75 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220S	18 / 36	2.7 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220T	18 / 36	1.9 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5222	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv
6209U	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	N/A	125 W	Y	Y	Y	Y	N	2	Adv
6222V	20 / 40	1.8 / 3.6 GHz	27.5 MB	2400 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	2	Adv
6226	12 / 24	2.7 / 3.7 GHz	19.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230N	20 / 40	2.3 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230T	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6238T	22 / 44	1.9 / 3.7 GHz	30.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
Intel Xeon Platinum processors														
8253	16 / 32	2.2 / 3.0 GHz	22 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
8256	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv

Configuration notes:

- The Intel Xeon Gold 5218 and 5218B processors have similar specifications; however, they use different silicon designs and cannot be mixed in the same system.
- The processors that support SST-PP offer three distinct operating points that are defined by a core count with a base speed associated with that core count. The operating point is static, it is selected during the boot process and cannot be changed at runtime.

For the SR530 server models that come with one processor, the second processor can be ordered, if required (see the following table for ordering information). The second processor must be of the same model as the first processor. The second processor option includes a processor and a heatsink; two additional system fans are not included and need to be purchased with the second processor (see Cooling for details).

Table 13. Processor options

Description	Part number	Feature code*
Intel Xeon Bronze processors		
SR530/SR570/SR630 Intel Xeon Bronze 3204 6C 85W 1.9GHz Processor w/o FAN	4XG7A37939	B4HU
SR530/SR570/SR630 Intel Xeon Bronze 3206R 8C 85W 1.9GHz Processor w/o FAN	4XG7A37990	B7N3
Intel Xeon Silver processors		
SR530/SR570/SR630 Intel Xeon Silver 4208 8C 85W 2.1GHz Processor w/o FAN	4XG7A37936	B4HT
SR530/SR570/SR630 Intel Xeon Silver 4209T 8C 70W 2.2GHz Processor w/o FAN	4XG7A37945	B4P4
SR530/SR570/SR630 Intel Xeon Silver 4210 10C 85W 2.2GHz Processor w/o FAN	4XG7A37933	B4HS
SR530/SR570/SR630 Intel Xeon Silver 4210R 10C 100W 2.4GHz Processor w/o FAN	4XG7A37988	B7N5
SR530/SR570/SR630 Intel Xeon Silver 4214 12C 85W 2.2GHz Processor w/o FAN	4XG7A37930	B4HR
SR530/SR570/SR630 Intel Xeon Silver 4214R 12C 100W 2.4GHz Processor w/o FAN	4XG7A37987	B7N6
SR530/SR570/SR630 Intel Xeon Silver 4214Y 12/10/8C 85W 2.2GHz Processor w/o FAN	4XG7A37942	B4NW
SR530/SR570/SR630 Intel Xeon Silver 4215 8C 85W 2.5GHz Processor w/o FAN	4XG7A37927	B4HQ
SR530/SR570/SR630 Intel Xeon Silver 4216 16C 100W 2.1GHz Processor w/o FAN	4XG7A37924	B4HP
Intel Xeon Gold processors		
SR530/SR570/SR630 Intel Xeon Gold 5215 10C 85W 2.5GHz Processor w/o FAN	4XG7A37917	B4HN
SR530/SR570/SR630 Intel Xeon Gold 5215L 10C 85W 2.5GHz Processor w/o FAN	4XG7A37911	B4P9
SR530/SR570 Intel Xeon Gold 5217 8C 115W 3.0GHz Processor w/o FAN	4XG7A37921	B4HM
SR530/SR570/SR630 Intel Xeon Gold 5218 16C 125W 2.3GHz Processor w/o FAN	4XG7A37896	B4HL
SR530/SR570/SR630 Intel Xeon Gold 5218B 16C 125W 2.3GHz Processor w/o FAN	4XG7A37959	B6BS
SR530/SR570/SR630 Intel Xeon Gold 5218R 20C 125W 2.1GHz Processor w/o FAN	4XG7A63296	BAZS
SR530/SR570 Intel Xeon Gold 5218T 16C 105W 2.1GHz Processor w/o FAN	4XG7A38017	B4P3
SR530/SR570/SR630 Intel Xeon Gold 5220 18C 125W 2.2GHz Processor w/o FAN	4XG7A37893	B4HK
SR530/SR570/SR630 Intel Xeon Gold 5220S 18C 125W 2.7GHz Processor w/o FAN	4XG7A38018	B6CW
SR530/SR570 Intel Xeon Gold 5220T 18C 105W 1.9GHz Processor w/o FAN	4XG7A38004	B6CQ
SR530/SR570 Intel Xeon Gold 5222 4C 105W 3.8GHz Processor w/o FAN	4XG7A37953	B5S1
Intel Xeon Gold 6209U 20C 125W 2.1GHz Processor	None**	B6CX
SR530/SR570/SR630 Intel Xeon Gold 6222V 20C 115W 1.8GHz Processor w/o FAN	4XG7A38022	B6CV
SR530/SR570/SR630 Intel Xeon Gold 6226 12C 125W 2.7GHz Processor w/o FAN	4XG7A38020	B6CL
SR530/SR570/SR630 Intel Xeon Gold 6230 20C 125W 2.1GHz Processor w/o FAN	4XG7A37890	B4HJ
SR530/SR570 Intel Xeon Gold 6230N 20C 125W 2.3GHz Processor w/o FAN	4XG7A38029	B5RY
SR530/SR570 Intel Xeon Gold 6230T 20C 125W 2.1GHz Processor w/o FAN	4XG7A38007	B6CP
SR530/SR570 Intel Xeon Gold 6238T 22C 125W 1.9GHz Processor w/o FAN	4XG7A37908	B4P2
Intel Xeon Platinum processors		
SR530/SR570/SR630 Intel Xeon Platinum 8253 16C 125W 2.2GHz Processor w/o FAN	4XG7A37899	B5RZ
SR530/SR570 Intel Xeon Platinum 8256 4C 105W 3.8GHz Processor w/o FAN	4XG7A37949	B5S2

* For CTO configurations, the feature code represents a processor, and fans and heatsinks are derived by the configuration tool.
** Factory-installed only; no field upgrade. Supported in the uniprocessor configurations only.

Memory

The SR530 server supports up to 6 TruDDR4 memory RDIMMs when one processor is installed and up to 12 RDIMMs when two processors are installed for a total of up to 768 GB of memory capacity (up to 384 TB per processor). Each processor has six memory channels, and there is a one DIMM per channel.

Lenovo TruDDR4 memory uses the highest-quality components sourced from Tier 1 DRAM suppliers and only memory that meets strict requirements is selected. It is compatibility tested and tuned on every ThinkSystem server to maximize performance and reliability.

TruDDR4 memory has a unique signature programmed into the DIMM, which enables Lenovo servers to verify whether the memory installed is qualified and supported. Lenovo qualified and supported TruDDR4 memory is covered by Lenovo warranty, and service and support provided worldwide.

The following memory protection technologies are supported by the processor's integrated memory controllers:

- ECC
- SDDC (for x4-based memory DIMMs)
- ADDDC (for x4-based memory DIMMs; Gold and Platinum processors only)
- Memory mirroring
- Memory rank sparing
- Patrol scrubbing
- Demand scrubbing

The following table lists memory options available for the SR530 server.

Table 14. Memory options

Description	Part number	Feature code	Maximum quantity*
RDIMMs - 2933 MHz			
ThinkSystem 8GB TruDDR4 2933MHz (1Rx8 1.2V) RDIMM	4ZC7A08706	B4H1	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (1Rx4 1.2V) RDIMM	4ZC7A08707	B4LY	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (2Rx8 1.2V) RDIMM	4ZC7A08708	B4H2	6 / 12
ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08709	B4H3	6 / 12
ThinkSystem 64GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08710	B4H4	6 / 12
RDIMMs - 2666 MHz			
ThinkSystem 16GB TruDDR4 2666 MHz (1Rx4 1.2V) RDIMM	7X77A01302	AUNB	6 / 12
ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM	7X77A01303	AUNC	6 / 12
ThinkSystem 32GB TruDDR4 2666 MHz (2Rx4 1.2V) RDIMM	7X77A01304	AUND	6 / 12

* The maximum quantity shown is with one processor / two processors.

Configuration notes:

- All RDIMMs in the server operate at the same speed, which is determined as the lowest value of:
  - RDIMM rated speed (2666 MHz or 2933 MHz).
  - Memory speed supported by the specific processor (2133 MHz, 2400 MHz, 2666 MHz, or 2933 MHz).

  Note: Maximum memory speed can be achieved when Max performance mode is enabled in UEFI.
- Mixing RDIMMs of different ranks (single- or dual-rank), DRAM chip types (x4 or x8), speeds (2666 MHz or 2933 MHz), and capacities (8 GB, 16 GB, 32 GB, or 64 GB) is supported in the independent channel mode (the default operational mode).
- For server configurations with memory protection, the following rules apply:
  - Single Device Data Correction (SDDC) works only in the independent channel mode and supports only x4-based memory DIMMs.
  - Adaptive Double Device Data Correction (ADDDC) works with x4-based memory DIMMs and requires two DIMM ranks per channel, Intel Xeon Gold or Platinum processors, and the Closed Page memory access mode.
  - If memory mirroring is used, then DIMMs must be installed in quantities of 2 or 4 per processor for mirroring across two memory channels, or in quantities of 3 or 6 per processor for mirroring across three memory channels. Mixing two- and three-channel mirroring in the server is allowed (one processor uses two-channel mirroring, and another processor uses three-channel mirroring). All DIMMs in the server must be identical in type and size.
  - If memory rank sparing is used, then a minimum of two ranks must be installed per populated channel (a least one dual-rank or quad-rank DIMM; single-rank DIMMs are not supported). With rank sparing, one rank in each populated channel is reserved as spare memory for other ranks on the same channel. All DIMMs in the server must be identical in type and size.
  - SDDC, memory mirroring, and memory rank sparing modes are mutually exclusive. Only one operational memory mode can be enabled on the server.

Internal storage

The SR530 server supports the following internal drive bay configurations:

1. 4 LFF SATA Simple Swap drive bays
2. 4 LFF SAS/SATA hot-swap drive bays
3. 8 SFF SAS/SATA hot-swap drive bays

In addition, the SR530 server models can be configured with one or two internal M.2 SATA SSDs. The server also supports configurations without drive bays.

The following figure shows the internal drive bay configurations.

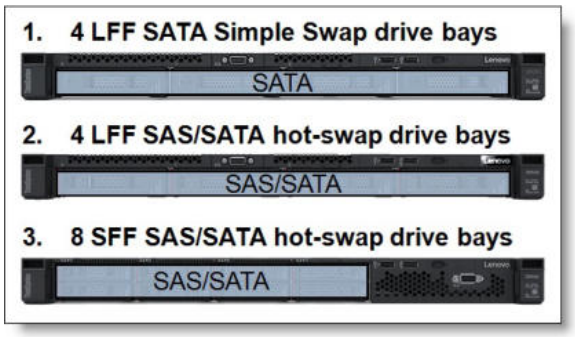


Figure 6. Internal drive bay configurations

The following table lists the internal storage options for the SR530 server.

Table 15. Internal storage options

Description	Part number	Feature code	Maximum quantity
Factory-installed backplane kits			
ThinkSystem 1U 3.5" SATA/SAS 4-Bay Backplane	None*	AUW8	1
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane	None*	AUWB	1
Backplane kit field upgrade options			
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane Kit	7XH7A05896	None**	1
M.2 enablement kits			
ThinkSystem M.2 Enablement Kit	7Y37A01092	AUMU	1
ThinkSystem M.2 with Mirroring Enablement Kit	7Y37A01093	AUMV	1

* These backplane kits can be factory-installed in standard or custom (CTO or Special Bid) models, and they might not have an option part number assigned.
** Field upgrade only; used for upgrading models without any drive bays to 8x 2.5" SAS/SATA hot-swap drive bays.

M.2 Enablement Kit configuration notes:

- The M.2 Enablement Kit (7Y37A01092) supports one M.2 SATA SSD which is connected to the SATA port on the Intel Platform Controller Hub (PCH).
- The M.2 with Mirroring Enablement Kit (7Y37A01093) is connected to the Intel PCH via the PCIe link, and the kit supports two M.2 SATA SSDs that can be configured in a RAID-1 or RAID-0 drive group, or they can operate as two separate drives.

The following tables list supported internal storage configurations with the SAS/SATA backplanes.

Table 16. Internal storage configurations

Drive bay configuration	Backplane kit type and quantity		Storage controller type and quantity*
	4x 3.5" SATA/SAS	8x 2.5" SATA/SAS	
4x 3.5" chassis (Feature code AV0T)			
4x 3.5-in. SATA Simple Swap	0	0	Onboard AHCI (non-RAID) / Intel RSTe (RAID) (4)
4x 3.5-in. SAS/SATA hot-swap	1	0	1x RAID 530-8i/730-8i 1GB (4)
			1x RAID 730-8i 2GB/930-8i (4)
			1x 430-8i HBA (4)
8x 2.5" chassis (Feature code AV0S)			
8x 2.5-in. SAS/SATA hot-swap	0	1	1x RAID 530-8i/730-8i 1GB (8)
			1x RAID 730-8i 2GB/930-8i/930-16i (8)
			1x 430-8i HBA (8)

* The number in brackets (x) specifies the quantity of drive bays connected to each of the controllers.

Configuration note: Models without any drive bays are based on the 8x 2.5" chassis (feature code AV0S), and they support adding drive bays by using the 2.5" 8-drive backplane kit (7XH7A05896).

Controllers for internal storage

The following table lists the storage controllers and options for internal storage of the SR530 server.

Table 17. RAID controllers and HBAs for internal storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
6 Gbps SATA controllers				
Onboard AHCI (non-RAID) / Intel RSTe (RAID)	Onboard*	Onboard*	1	-
12 Gb SAS/SATA RAID controllers				
ThinkSystem RAID 530-8i PCIe 12Gb Adapter	7Y37A01082	AUNG	1	1
ThinkSystem RAID 730-8i 1GB Cache PCIe 12Gb Adapter	7Y37A01083	AUNH	1	1
ThinkSystem RAID 730-8i 2GB Flash PCIe 12Gb Adapter	4Y37A09722	B4RQ	1	1
ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter	7Y37A01084	AUNJ	1	1
ThinkSystem RAID 930-16i 4GB Flash PCIe 12Gb Adapter	7Y37A01085	AUNK	1	1
ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter	4Y37A09721	B31E	1	1
12 Gb SAS/SATA non-RAID HBAs				
ThinkSystem 430-8i SAS/SATA 12Gb HBA	7Y37A01088	AUNL	1	1

* The onboard SATA controller integrated into the Intel C622 Platform Controller Hub (PCH) supports non-RAID (JBOD) AHCI mode or a hardware-assist, software RAID feature (Intel Rapid Storage Technology Enterprise [RSTe]).

Configuration note: Low profile SAS RAID controllers and HBAs for internal storage are supported in the PCIe x8 slot 1 supplied by the riser card 1.

The following table summarizes features of supported SAS/SATA storage controllers.

Table 18. Storage controller features and specifications (LP = Low profile, FHHL = Full-height half-length)

Feature	Intel RSTe	RAID 530-8i	RAID 730-8i 1GB	RAID 730-8i 2GB	RAID 930-8i	RAID 930-16i	430-8i HBA
Form factor	Onboard	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP
SAS controller	None	SAS3408	SAS3108	SAS3108	SAS3508	SAS3516	SAS3408
Host interface	PCH	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	6 Gb SATA	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	8	8	8	16	8
Connector type	SATA x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4
Number of connectors	2	2	2	2	2	4	2
Drive interface	SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD	HDD, SSD, SED	HDD, SSD	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED*
Hot-swap drive support	No	Yes	Yes	Yes	Yes	Yes	Yes
Number of drives	8	8	8	8	8	16^	8
RAID levels	0/1/10/5	0/1/10/5/50	0/1/10/5/50	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	None
JBOD mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cache	None	None	1 GB	2 GB	2 GB	4 GB; 8 GB	None
Cache protection	None	None	None	Flash backup (Included)	Flash backup (Included)	Flash backup (Included)	None
SED key management (SafeStore)	No	Yes	No	Yes	Yes	Yes	No
SSD I/O acceleration (FastPath)	No	Yes	No	Yes	Yes	Yes	No
SSD Caching (CacheCade Pro 2.0)	No	No	No	No	No**	No**	No
Consistency check	Yes	Yes	Yes	Yes	Yes	Yes	No
Patrol read	Yes	Yes	Yes	Yes	Yes	Yes	No
Online capacity expansion	Yes	Yes	Yes	Yes	Yes	Yes	No
Online RAID level migration	Yes	Yes	Yes	Yes	Yes	Yes	No
Global Hot Spare	Yes	Yes	Yes	Yes	Yes	Yes	No
Auto-rebuild	Yes	Yes	Yes	Yes	Yes	Yes	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
^ Up to 8 drives is supported by the RAID 930-16i in the SR530 server.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

Important: The onboard Intel RSTe is not supported by virtualization hypervisors, including VMware vSphere (ESXi), Linux KVM, Xen, and Microsoft Hyper-V.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Drives for internal storage

The following tables list the hard disk drive and solid-state drive options for the internal disk storage of the server.

2.5-inch hot-swap drives:

- 2.5-inch hot-swap 12 Gb SAS HDDs
- 2.5-inch hot-swap 6 Gb SATA HDDs
- 2.5-inch hot-swap 12 Gb SAS SSDs
- 2.5-inch hot-swap 6 Gb SATA SSDs

3.5-inch hot-swap drives:

- 3.5-inch hot-swap 12 Gb SAS HDDs
- 3.5-inch hot-swap 6 Gb SATA HDDs
- 3.5-inch hot-swap 12 Gb SAS SSDs
- 3.5-inch hot-swap 6 Gb SATA SSDs

Simple-swap drives:

- 3.5-inch simple-swap 6 Gb SATA HDDs

M.2 drives:

- M.2 SATA drives

M.2 drive support: The use of M.2 drives requires an additional adapter as described in the Internal storage section.

Table 19. 2.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00024	AULY	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00025	AULZ	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00026	AUM0	ThinkSystem 2.5" 900GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00027	AUM1	ThinkSystem 2.5" 1.2TB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00028	AUM2	ThinkSystem 2.5" 1.8TB 10K SAS 12Gb Hot Swap 512e HDD	8
7XB7A00069	B0YS	ThinkSystem 2.5" 2.4TB 10K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00021	AULV	ThinkSystem 2.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00022	AULW	ThinkSystem 2.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00023	AULX	ThinkSystem 2.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00034	AUM6	ThinkSystem 2.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00035	AUM7	ThinkSystem 2.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
2.5-inch hot-swap SED HDDs - 12 Gb SAS 10K			
7XB7A00030	AUM4	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD SED	8
7XB7A00031	AUM5	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD SED	8

Table 20. 2.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00036	AUUE	ThinkSystem 2.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	8
7XB7A00037	AUUJ	ThinkSystem 2.5" 2TB 7.2K SATA 6Gb Hot Swap 512e HDD	8

Table 21. 2.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17062	B8HU	ThinkSystem 2.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17063	B8J4	ThinkSystem 2.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17064	B8JD	ThinkSystem 2.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17065	B8JA	ThinkSystem 2.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13654	B4A1	ThinkSystem 2.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13655	B4A2	ThinkSystem 2.5" PM1645 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A38175	B91A	ThinkSystem 2.5" PM1643a 960GB Entry SAS 12Gb Hot Swap SSD	8
4XB7A38176	B91B	ThinkSystem 2.5" PM1643a 1.92TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17054	B91C	ThinkSystem 2.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17055	B91D	ThinkSystem 2.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17056	BC4R	ThinkSystem 2.5" PM1643a 15.36TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A13645	B4A7	ThinkSystem 2.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	8

Table 22. 2.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17087	B8J1	ThinkSystem 2.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17088	B8HY	ThinkSystem 2.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17089	B8J6	ThinkSystem 2.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17090	B8JE	ThinkSystem 2.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17091	B8J7	ThinkSystem 2.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13633	B49L	ThinkSystem 2.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13634	B49M	ThinkSystem 2.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13635	B49N	ThinkSystem 2.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13636	B49P	ThinkSystem 2.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13637	B49Q	ThinkSystem 2.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10237	B488	ThinkSystem 2.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10239	B48A	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10240	B48B	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10241	B48C	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			

Part number	Feature	Description	Maximum supported
4XB7A38271	BCTC	ThinkSystem 2.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38272	BCTD	ThinkSystem 2.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38273	BCTE	ThinkSystem 2.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38274	BCTF	ThinkSystem 2.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38275	BCTG	ThinkSystem 2.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17075	B8HV	ThinkSystem 2.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17076	B8JM	ThinkSystem 2.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17077	B8HP	ThinkSystem 2.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17078	B8J5	ThinkSystem 2.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17079	B8JP	ThinkSystem 2.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17080	B8J2	ThinkSystem 2.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38185	B9AC	ThinkSystem 2.5" 5210 960GB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38144	B7EW	ThinkSystem 2.5" 5210 1.92TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38145	B7EX	ThinkSystem 2.5" 5210 3.84TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38146	B7EY	ThinkSystem 2.5" 5210 7.68TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A10247	B498	ThinkSystem 2.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10248	B499	ThinkSystem 2.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10249	B49A	ThinkSystem 2.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13622	B49B	ThinkSystem 2.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13623	B49C	ThinkSystem 2.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10195	B34H	ThinkSystem 2.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10196	B34J	ThinkSystem 2.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10197	B34K	ThinkSystem 2.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10198	B34L	ThinkSystem 2.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10199	B34M	ThinkSystem 2.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10200	B4D2	ThinkSystem 2.5" PM883 7.68TB Entry SATA 6Gb Hot Swap SSD	8
7SD7A05740	B0Z0	ThinkSystem 2.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10155	B2X4	ThinkSystem 2.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10157	B2X6	ThinkSystem 2.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	8

Table 23. 3.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00063	B1JJ	ThinkSystem 3.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	4
3.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00038	AUU2	ThinkSystem 3.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00039	AUU3	ThinkSystem 3.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00040	AUUC	ThinkSystem 3.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00041	AUU4	ThinkSystem 3.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00042	AUU5	ThinkSystem 3.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00043	AUU6	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00044	AUU7	ThinkSystem 3.5" 6TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00045	B0YR	ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00046	AUUG	ThinkSystem 3.5" 10TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00067	B117	ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13906	B496	ThinkSystem 3.5" 14TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13911	B7EZ	ThinkSystem 3.5" 16TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A38266	BCFP	ThinkSystem 3.5" 18TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap SED HDDs - 12 Gb NL SAS			
7XB7A00047	AUUH	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD FIPS	4

Table 24. 3.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00049	AUUF	ThinkSystem 3.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00050	AUUD	ThinkSystem 3.5" 2TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00051	AUU8	ThinkSystem 3.5" 4TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00052	AUUA	ThinkSystem 3.5" 6TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00053	AUU9	ThinkSystem 3.5" 8TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00054	AUUB	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00068	B118	ThinkSystem 3.5" 12TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13907	B497	ThinkSystem 3.5" 14TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13914	B7F0	ThinkSystem 3.5" 16TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A38130	BCFH	ThinkSystem 3.5" 18TB 7.2K SATA 6Gb Hot Swap 512e HDD	4

Table 25. 3.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17066	B8HT	ThinkSystem 3.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17043	B8JN	ThinkSystem 3.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17067	B8JK	ThinkSystem 3.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17068	B8JG	ThinkSystem 3.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A13658	B4A4	ThinkSystem 3.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A17058	B91E	ThinkSystem 3.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A17059	BEVK	ThinkSystem 3.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A13649	B4A8	ThinkSystem 3.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	4

Table 26. 3.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17096	B8JL	ThinkSystem 3.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17097	B8JF	ThinkSystem 3.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17098	B8J0	ThinkSystem 3.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17099	B8HR	ThinkSystem 3.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17100	B8HX	ThinkSystem 3.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13639	B49R	ThinkSystem 3.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13640	B49S	ThinkSystem 3.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13641	B49T	ThinkSystem 3.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13642	B49U	ThinkSystem 3.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13643	B49V	ThinkSystem 3.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10242	B48D	ThinkSystem 3.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10244	B48F	ThinkSystem 3.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10245	B48G	ThinkSystem 3.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10246	B48H	ThinkSystem 3.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			
4XB7A38276	BCTH	ThinkSystem 3.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38277	BCTJ	ThinkSystem 3.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38278	BCTK	ThinkSystem 3.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38279	BCTL	ThinkSystem 3.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38281	BCTM	ThinkSystem 3.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17081	B8JB	ThinkSystem 3.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17082	B8J9	ThinkSystem 3.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17083	B8JC	ThinkSystem 3.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17084	B8HZ	ThinkSystem 3.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17085	B8HQ	ThinkSystem 3.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17086	B8J3	ThinkSystem 3.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Part number	Feature	Description	Maximum supported
4XB7A13625	B49D	ThinkSystem 3.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13626	B49E	ThinkSystem 3.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13627	B49F	ThinkSystem 3.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13628	B49G	ThinkSystem 3.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13629	B49H	ThinkSystem 3.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17176	B6TM	ThinkSystem 3.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17177	B6TN	ThinkSystem 3.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17178	B6TP	ThinkSystem 3.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17179	B6JY	ThinkSystem 3.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17180	B6JZ	ThinkSystem 3.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	4
7SD7A05735	B0Z5	ThinkSystem 3.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10160	B2X9	ThinkSystem 3.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10162	B2XB	ThinkSystem 3.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Table 27. 3.5-inch simple-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch simple-swap HDDs - 6 Gb NL SATA			
7XB7A00055	AUZS	ThinkSystem 1TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00056	AUZT	ThinkSystem 2TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00057	AUZU	ThinkSystem 4TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00058	AXC7	ThinkSystem 6TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00059	AXC6	ThinkSystem 8TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00060	AXC8	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Simple Swap 512e HDD	4

Table 29. M.2 SATA drives

Part number	Feature	Description	Maximum supported
M.2 SSDs - 6 Gb SATA - Entry (<3 DWPD)			
7N47A00129	AUUL	ThinkSystem M.2 32GB SATA 6Gbps Non-Hot Swap SSD	2
7N47A00130	AUUV	ThinkSystem M.2 128GB SATA 6Gbps Non-Hot Swap SSD	2
7SD7A05703	B11V	ThinkSystem M.2 5100 480GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17071	B8HS	ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17073	B919	ThinkSystem M.2 5300 480GB SATA 6Gbps Non-Hot Swap SSD	2

Optical drives

The server supports the external USB optical drive listed in the following table.

Table 30. External optical drive

Part number	Feature code	Description
7XA7A05926	AVV8	ThinkSystem External USB DVD RW Optical Disk Drive

The drive is based on the Lenovo Slim DVD Burner DB65 drive and supports the following formats: DVD-RAM, DVD-RW, DVD+RW, DVD+R, DVD-R, DVD-ROM, CD-RW, CD-R, CD-ROM.

I/O expansion

The SR530 server supports one LOM card slot and up to three PCIe slots with different riser cards installed into two riser sockets on the system planar (one riser socket supports installation of one riser card).

The slot form factors are as follows:

- LOM card slot
- Slot 1: PCIe 3.0 x8; low profile
- Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length
- Slot 3: PCIe 3.0 x8 or x16; low profile

Configuration notes:

- PCIe x16 slot 3 requires the second processor to be installed.
- The COM Port Upgrade Kit is installed in place of one of the PCIe slots 1, 2, or 3.

The locations of the PCIe slots are shown in the following figure.

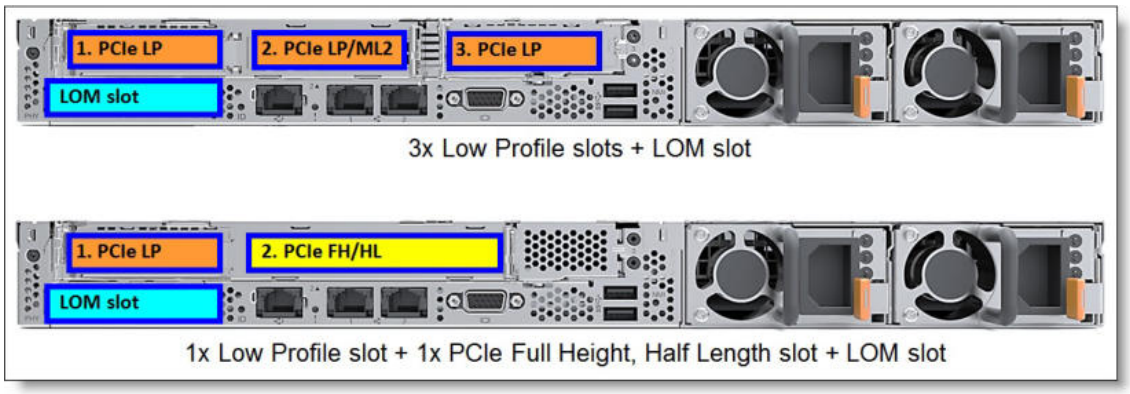


Figure 7. Slot locations

Riser 1 supplies slots 1 and 2, and Riser 2 supplies slot 3. The slots that are available for use depend on the number of riser cards that are installed and whether the second processor is installed, as shown in the following table.

Table 31. Slots available for use

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
None	None	LOM	-
None	PCIe x8	LOM, 3	-
None	PCIe x16	LOM	3
PCIe x8/x16 or PCIe x8/x8ML2	None	LOM, 1, 2	-
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x8	LOM, 1, 2, 3	-

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x16	LOM, 1, 2	3

The following table lists available PCIe riser card options.

Table 32. PCIe riser cards and miscellaneous options

Description	Part number	Feature code	Maximum quantity
x8 Riser Card 1 options (Riser card 1 supplies slots 1 and 2)			
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+LP Riser 1 Kit	7XH7A02682	AUWC	1
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+FH Riser 1 Kit	7XH7A05893	None*	1
ThinkSystem SR530/SR570 x8/x8ML2 PCIe LP+LP Riser 1 Kit	7XH7A05892	AV0X	1
Riser Card 2 option (Riser card 2 supplies slot 3)			
ThinkSystem SR530/SR570/SR630 x16 PCIe LP Riser 2 Kit	7XH7A02685	AUWA	1
ThinkSystem SR530/SR570 x8 PCIe LP Riser 2 Kit	7XH7A05891	AV0W	1
Serial port upgrade kit			
ThinkSystem COM Port Upgrade Kit	7Z17A02577	AUSL	1

* The LP+FH Riser 1 can be factory-installed by selecting the feature codes AUWC (LP+LP Riser 1) and AUWS (LP+FH Bracket).

The COM Port Upgrade Kit, part number 7Z17A02577, is used for mounting the external serial port on the rear of the SR530. This option includes the bracket and the cable. The COM Port option is mounted in place of one of the PCIe slots 1, 2, or 3.

Network adapters

The SR530 server has two onboard 1 GbE ports (no 10/100 Mb support) and up to two additional onboard 1/10 GbE network ports (no 10/100 Mb support) with optional LOM cards. Onboard ports and LOM cards use the Intel Ethernet Connection X722 1/10 GbE technology integrated into the Intel C622 Platform Controller Hub (PCH). The server also supports ML2 adapters that are installed in the custom ML2 slot provided by an ML2 riser card. The LOM cards support direct connectivity to the XClarity Controller via the Network Controller Sideband Interface (NSCI) for out-of-band systems management.

Note: ML2 network adapters do not support NSCI when used in the SR530 server.

The integrated Intel Ethernet Connection X722 has the following features:

- Two 1 Gb Ethernet ports (no 10/100 Mb Ethernet support)
- Two 1/10 Gb Ethernet capable ports (no 10/100 Mb Ethernet support)
- NIC Teaming (load balancing and failover)
- Data Center Bridging
- iWARP (RDMA over IP)
- VMDq and SR-IOV virtualization (10 Gb speeds only, 4 PFs, 128 VFs per device)
- IEEE 802.1q Virtual Local Area Networks (VLANs)
- NVGRE, VXLAN, IPinGRE, and MACinUDP network virtualization
- IEEE 802.1Qbg Edge Virtual Bridging
- TCP, IP, and UDP checksum offload
- Large Send Offload (LSO) and Generic Send Offload (GSO)
- Receive Side Scaling (RSS) for TCP and UDP traffic
- Jumbo frames up to 9.5 Kbytes

The following table lists the network adapters that are supported with the SR530 server.

Table 33. Network adapters

Description	Part number	Feature code	Max qty	I/O slots supported
LOM cards - 1 Gb Ethernet				
ThinkSystem 1Gb 2-port RJ45 LOM	7ZT7A00544	AUKG	1	LOM slot
LOM cards - 10 Gb Ethernet				
ThinkSystem 10Gb 2-port Base-T LOM	7ZT7A00548	AUKL	1	LOM slot
ThinkSystem 10Gb 2-port SFP+ LOM	7ZT7A00546	AUKJ	1*	LOM slot
ML2 adapters - 10 Gb Ethernet				
Broadcom NX-E ML2 10Gb 2-Port Base-T Ethernet Adapter	7ZT7A00497	AUKQ	1	2 (ML2)
Emulex VFA5.2 ML2 Dual Port 10GbE SFP+ Adapter	00AG560	AT7U	1*	2 (ML2)
Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	01CV770	AU7Z	1*	2 (ML2)
Intel X710-DA2 ML2 2x10GbE SFP+ Adapter	00JY940	ATRH	1*	2 (ML2)
PCIe Low Profile adapters - 1 Gb Ethernet				
Broadcom 5720 1GbE RJ45 2-Port PCIe Ethernet Adapter	7ZT7A00482	AUZX	3	1, 2, 3
Broadcom 5719 1GbE RJ45 4-Port PCIe Ethernet Adapter	7ZT7A00484	AUZV	3	1, 2, 3
ThinkSystem I350-F1 PCIe 1Gb 1-Port SFP Ethernet Adapter	7ZT7A00533	AUZZ	3	1, 2, 3
ThinkSystem I350-T2 PCIe 1Gb 2-Port RJ45 Ethernet Adapter	7ZT7A00534	AUZY	3	1, 2, 3
ThinkSystem I350-T4 PCIe 1Gb 4-Port RJ45 Ethernet Adapter	7ZT7A00535	AUZW	3	1, 2, 3
PCIe Low Profile adapters - 10 Gb Ethernet				
Broadcom 57416 10GBASE-T 2-Port PCIe Ethernet Adapter	7ZT7A00496	AUKP	3	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ PCIe Adapter	00AG570	AT7S	3*	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	00AG580	AT7T	3*	1, 2, 3
Intel X550-T2 Dual Port 10GBase-T Adapter	00MM860	ATPX	3	1, 2, 3
Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter	7ZT7A00537	AUKX	3*	1, 2, 3
QLogic QL41134 PCIe 10Gb 4-Port Base-T Ethernet Adapter	4XC7A08225	B31G	3	1, 2, 3
PCIe Full Height adapters - 10 Gb Ethernet				
Emulex OCe14104B-NX PCIe 10Gb 4-Port SFP+ Ethernet Adapter	7ZT7A00493	AUKN	1*	2
PCIe Low Profile adapters - 25 Gb Ethernet				
Broadcom 57412 10/25GbE SFP28 1-Port PCIe Ethernet Adapter	7ZT7A00505	AUKS	3*	1, 2, 3
Broadcom 57414 10/25GbE SFP28 2-port PCIe Ethernet Adapter	4XC7A08238	B5T0	3*	1, 2, 3
PCIe Low Profile adapters - Omni-Path				
Intel OPA 100 Series Single-port PCIe 3.0 x16 HFA	00WE027	AU0B	1 / 2#*	2, 3

The maximum quantity shown is with one processor / two processors.
* The adapter comes without transceivers or cables; for ordering transceivers or cables, see the adapter product guide

Configuration notes:

- ML2 network adapters are supported in the ML2 x8 slot 2 supplied by the x8/x8ML2 Riser Card 1 (7XH7A05892).
- PCIe full-height network adapters are supported in the full-height PCIe x16 slot 2 supplied by the PCIe x8/x16 LP+FH Riser Card 1 (7XH7A05893).
- Omni-Path adapters are supported in the low profile or full-height PCIe x16 slots supplied by the riser cards 1 and 2.
- PCIe Low Profile network adapters (except Omni-Path adapters) are supported in the low profile and full-height PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

- Some adapters require supported transceivers or DAC cables to be purchased for the adapter. The maximum number of transceivers or cables that are supported per adapter equals the quantity of the adapter ports, and all adapter ports must have the same type of the transceiver or cable selected.

For more information, see the list of Product Guides in the Ethernet Adapters category:
http://lenovopress.com/servers/options/ethernet#rt=product-guide

SAS adapters for external storage

The following table lists SAS RAID controllers and HBAs for external storage attachments that are supported by the SR530 server.

Table 34. SAS RAID adapters and HBAs for external storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
12 Gbps SAS RAID adapters				
ThinkSystem RAID 930-8e 4GB Flash PCIe 12Gb Adapter	7Y37A01087	AUNQ	2	1, 2, 3
12 Gbps SAS HBAs				
ThinkSystem 430-8e SAS/SATA 12Gb HBA	7Y37A01090	AUNR	2	1, 2, 3
ThinkSystem 430-16e SAS/SATA 12Gb HBA	7Y37A01091	AUNN	2	1, 2, 3

Configuration notes:

- Low profile SAS RAID controllers and HBAs for external storage are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.
- The total quantity of the RAID 730-8i 2GB, RAID 930-8i, RAID 930-16i, and RAID 930-8e controllers in a supported combination in the server must not exceed 2 (up to 2 supercapacitors can be mounted in the server).

The following table summarizes features of supported RAID controllers and HBAs for external storage.

Table 35. Features and specifications of the RAID controllers and HBAs for external storage

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
Form factor	PCIe LP	PCIe LP	PCIe LP
SAS controller chip	SAS3516	SAS3408	SAS3416
Host interface	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	16
Connector type	SFF-8644 x4	SFF-8644 x4	SFF-8644 x4
Number of connectors	2	2	4
Drive interface	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD, SSD, SED	HDD, SSD, SED*	HDD, SSD, SED*
Hot-swap drive support	Yes	Yes	Yes
Number of devices	240	1024	1024
RAID levels	0/1/10/5/50/6/60	None	None
JBOD mode	Yes	Yes	Yes
Cache	4 GB	None	None
Cache protection	Flash backup (Included)	None	None
SED key management (SafeStore)	Yes	No	No
SSD I/O acceleration (FastPath)	Yes	No	No

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
SSD Caching (CacheCade Pro 2.0)	No**	No	No
Consistency check	Yes	No	No
Patrol read	Yes	No	No
Online capacity expansion	Yes	No	No
Online RAID level migration	Yes	No	No
Global Hot Spare	Yes	No	No
Auto-rebuild	Yes	No	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Fibre Channel host bus adapters

The following table lists Fibre Channel HBAs supported by the SR530 server.

Table 36. Fibre Channel HBAs

Description	Part number	Feature code	Maximum quantity	I/O slots supported
16 Gb Fibre Channel - PCIe				
Emulex 16Gb Gen6 FC Single-port HBA	01CV830	ATZU	3	1, 2, 3
Emulex 16Gb Gen6 FC Dual-port HBA	01CV840	ATZV	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Single-port HBA	01CV750	ATZB	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Dual-port HBA	01CV760	ATZC	3	1, 2, 3
8 Gb Fibre Channel - PCIe (available only in PRC and Asia Pacific)				
Emulex LPe12002-M8-L PCIe 8Gb 2-Port SFP+ FC HBA	4XC7A08221	B0X0	3	1, 2, 3
Emulex LPe12000-M8-L PCIe 8Gb 1-Port SFP+ FC HBA	4XC7A08220	B0WZ	3	1, 2, 3

Configuration note: FC HBAs are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

For more information, see the list of Product Guides in the Host bus adapters category:
http://lenovopress.com/servers/options/hba#rt=product-guide

Cooling

The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.

The following table shows additional cooling options.

Table 37. Cooling options

Description	Part number	Feature code	Maximum quantity
ThinkSystem SR530 FAN Option Kit	4F17A12354	AV0N	1

Configuration note: The SR530 FAN Option Kit (4F17A12354) includes two system fans that are required for field upgrades that add a second processor to the server. If two processors are selected in the initial server configurations, two fans for the second processor are derived by the configurator.

Power supplies and cables

The SR530 server supports up to two redundant power supplies and is capable of N+N redundancy depending on the configuration. A second power supply can be added to the models that come with one power supply. The following table lists the power supply options.

Table 38. Power supplies

Description	Part number	Feature code	Maximum quantity
ThinkSystem 550W (230V/115V) Platinum Hot-Swap Power Supply	7N67A00882	AVV6	2
ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply	7N67A00883	AVV7	2
ThinkSystem 750W (230V) Titanium Hot-Swap Power Supply	7N67A00884	AVV5	2

Configuration notes:

- Minimum of 1 and maximum of 2 power supplies per system.
- If 2 are installed, power supplies must be identical.
- Power supplies support AC (Worldwide) and HVDC (PRC only) power sources.

Important: The Standalone Solution Configuration Tool (SSCT) and Lenovo Data Center Solution Configurator (DCSC) power supply selection rules allow a subset of possible configurations due to power restrictions. Configurations that cannot be built in SSCT or DCSC due to power restrictions may still be supported. To verify support and ensure that the right power supply is chosen for optimal performance, you should always validate your server configuration using the latest version of the Lenovo Capacity Planner: http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

The SR530 server ship standard with or without a power cord (model dependent). A hot-swap power supply option ships without a power cord. The following table lists the rack power cables and line cords that can be ordered for the SR530 server.

Table 39. Power cables

Description	Part number	Feature code
Rack power cables		
1.0m, 10A/125-250V, C13 to IEC 320-C14 Rack Power Cable	00Y3043	A4VP
1.5m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7937	6201
2.0m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08369	6570
2.8m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08366	6311

Description	Part number	Feature code
2.8m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08370	6400
2.8m, 10A/100-250V, C13 to IEC 320-C20 Rack Power Cable	39Y7938	6204
4.3m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7932	6263
4.3m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08371	6583
Line cords		
Argentina 2.8m, 10A/250V, C13 to IRAM 2073 Line Cord	39Y7930	6222
Argentina 4.3m, 10A/250V, C13 to IRAM 2073 Line Cord	81Y2384	6492
Australia/New Zealand 2.8m, 10A/250V, C13 to AS/NZS 3112 Line Cord	39Y7924	6211
Australia/New Zealand 4.3m, 10A/250V, C13 to AS/NZS 3112 Line Cord	81Y2383	6574
Brazil 2.8m, 10A/250V, C13 to NBR 14136 Line Cord	69Y1988	6532
Brazil 4.3m, 10A/250V, C13 to NBR14136 Line Cord	81Y2387	6404
China 1.8m, 10A/250V, C13 to GB 2099.1 Line Cord	4L67A69954	6361
China 2.8m, 10A/250V, C13 to GB 2099.1 Line Cord	39Y7928	6210
China 4.3m, 10A/250V, C13 to GB 2099.1 Line Cord	81Y2378	6580
Denmark 2.8m, 10A/250V, C13 to DK2-5a Line Cord	39Y7918	6213
Denmark 4.3m, 10A/250V, C13 to DK2-5a Line Cord	81Y2382	6575
Europe 2.8m, 10A/250V, C13 to CEE7-VII Line Cord	39Y7917	6212
Europe 4.3m, 10A/250V, C13 to CEE7-VII Line Cord	81Y2376	6572
India 2.8m, 10A/250V, C13 to IS 6538 Line Cord	39Y7927	6269
India 4.3m, 10A/250V, C13 to IS 6538 Line Cord	81Y2386	6567
Israel 2.8m, 10A/250V, C13 to SI 32 Line Cord	39Y7920	6218
Israel 4.3m, 10A/250V, C13 to SI 32 Line Cord	81Y2381	6579
Italy 2.8m, 10A/250V, C13 to CEI 23-16 Line Cord	39Y7921	6217
Italy 4.3m, 10A/250V, C13 to CEI 23-16 Line Cord	81Y2380	6493
Japan 2.8m, 12A/125V, C13 to JIS C-8303 Line cord	46M2593	6314
Japan 2.8m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08357	5472
Japan 4.3m, 12A/125V, C13 to JIS C-8303 Line Cord	39Y7926	6335
Japan 4.3m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08362	6495
Korea 2.8m, 12A/250V, C13 to KS C8305 Line Cord	39Y7925	6219
Korea 4.3m, 12A/250V, C13 to KS C8305 Line Cord	81Y2385	6494
South Africa 2.8m, 10A/250V, C13 to SABS 164 Line Cord	39Y7922	6214
South Africa 4.3m, 10A/250V, C13 to SABS 164 Line Cord	81Y2379	6576
Switzerland 2.8m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	39Y7919	6216
Switzerland 4.3m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	81Y2390	6578
Taiwan 2.8m, 10A/125V, C13 to CNS 10917-3 Line Cord	23R7158	6386
Taiwan 2.8m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2375	6317
Taiwan 2.8m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2374	6402
Taiwan 4.3m, 10A/125V, C13 to CNS 10917-3 Line Cord	4L67A08363	AX8B
Taiwan 4.3m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2389	6531
Taiwan 4.3m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2388	6530
United Kingdom 2.8m, 10A/250V, C13 to BS 1363/A Line Cord	39Y7923	6215
United Kingdom 4.3m, 10A/250V, C13 to BS 1363/A Line Cord	81Y2377	6577
United States 2.8m, 10A/125V, C13 to NEMA 5-15P Line Cord	90Y3016	6313

Description	Part number	Feature code
United States 2.8m, 10A/250V, C13 to NEMA 6-15P Line Cord	46M2592	A1RF
United States 2.8m, 13A/125V, C13 to NEMA 5-15P Line Cord	00WH545	6401
United States 4.3m, 10A/125V, C13 to NEMA 5-15P Line Cord	4L67A08359	6370
United States 4.3m, 10A/250V, C13 to NEMA 6-15P Line Cord	4L67A08361	6373
United States 4.3m, 13A/125V, C13 to NEMA 5-15P Line Cord	4L67A08360	AX8A

Systems management

The SR530 supports the following systems management tools:

- Lenovo XClarity Controller
- Lenovo XClarity Provisioning Manager
- Lenovo XClarity Essentials
- Lenovo XClarity Administrator
- Lenovo XClarity Integrators
- Lenovo XClarity Energy Manager
- Lenovo Capacity Planner

Lenovo XClarity Controller

The SR530 server contains Lenovo XClarity Controller (XCC), which provides advanced service-processor control, monitoring, and alerting functions. XClarity Controller offers three functional levels: Standard, Advanced, and Enterprise.

By default, the SR530 server includes XClarity Controller Standard features, and it can be upgraded to Advanced or Enterprise functionality by using the Features on Demand (FoD) upgrades.

XClarity Controller Standard offers the following capabilities:

- Gathering and viewing system information and inventory
- Monitoring system status and health
- Alerting and notifications
- Event logging
- Configuring network connectivity
- Configuring security
- Updating system firmware
- Configuring server settings and devices
- Real-time power usage monitoring
- Remotely controlling server power (Power on, Power off, Restart)
- Managing FoD activation keys
- Redirecting serial console via IPMI
- Capturing the video display contents when an operating system hang condition is detected

XClarity Controller Advanced Upgrade adds the following functionality to the Standard features:

- Remotely viewing video with the following graphics resolutions:
  - Up to 1600x1200 with up to 23 bits per pixel; or
  - Up to 1920x1200 with up to 15 bits per pixel
- Remotely accessing the server using the keyboard and mouse from a remote client
- Remotely deploying an operating system
- Syslog alerting
- Redirecting serial console via SSH
- Displaying graphics for real-time and historical power usage data and temperature

XClarity Controller Enterprise Upgrade adds the following functionality to the Advanced features:

- Capping power usage
- Mapping the ISO and image files located on the local client as virtual drives for use by the server
- Mounting the remote ISO and image files via HTTPS, SFTP, CIFS, and NFS
- Collaborating across up to six users of the virtual console
- Controlling quality and bandwidth usage

The XClarity Controller provides remote server management through industry-standard interfaces:

- Intelligent Platform Management Interface (IPMI) Version 2.0
- Simple Network Management Protocol (SNMP) Version 3
- Common Information Model (CIM)
- Data Center Manageability Interface (DCMI) Version 1.5
- Redfish REpresentational State Transfer (REST) API
- Web browser with HTML5 support
- Command-line interface
- Virtual Operator Panel with XClarity Mobile App via the front USB port with XClarity Controller access

Virtual Operator Panel provides quick access to system status, firmware, network, health, and alerts information. With proper authentication, it also allows to configure systems management and network settings and to control system power (Power on, Power off, Restart). The Virtual Operator Panel can be accessed from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access (See Components and connectors).

Note: Depending on the system settings, the front USB port can be assigned to XClarity Controller for management functions, or to the system as a regular USB 2.0 port, or switched between two functions by using the system ID button.

IPMI via the Ethernet port (IPMI over LAN) is supported, however it is disabled by default. For CTO orders you can specify whether you want to the feature enabled or disabled in the factory, using the feature codes listed in the following table.

Table 40. IPMI-over-LAN settings

Part number	Feature code	Description
CTO only	B7XZ	Disable IPMI-over-LAN (default)
CTO only	B7Y0	Enable IPMI-over-LAN

The following table lists the XClarity Controller FoD upgrades.

Table 41. XClarity Controller FoD upgrades

Description	Part number	Feature code	Maximum quantity
ThinkSystem XClarity Controller Standard to Advanced Upgrade	4L47A09132	AVUT	1
ThinkSystem XClarity Controller Standard to Enterprise Upgrade	None*	AUPW	1
ThinkSystem XClarity Controller Advanced to Enterprise Upgrade	4L47A09133	None**	1

* Factory-installed only.
** Field upgrade only.

Configuration notes:

- For factory-installed upgrades, either Standard to Advanced Upgrade (feature AVUT) or Standard to Enterprise Upgrade (feature AUPW) can be selected, but not both.
- For field upgrades, the Advanced to Enterprise Upgrade (4L47A09133) requires the Standard to Advanced Upgrade to be activated on the server previously with either the factory-installed feature AVUT or field upgrade 4L47A09132.

Lenovo XClarity Provisioning Manager

Lenovo XClarity Provisioning Manager is a UEFI-embedded GUI application that combines the functions of configuring system setup settings, configuring RAID, and updating applications and firmware. It also enables you to install the supported operating systems and associated device drivers, run diagnostics, and collect service data.

Lenovo XClarity Provisioning Manager has the following features:

- Automatic hardware detection
- Collecting and viewing system inventory information
- Configuring UEFI system setup settings
- Updating the system firmware
- Configuring RAID by using the RAID Setup Wizard or Advanced mode
- Installing an operating system and device drivers automatically or manually
- Running diagnostics and collecting service data

Lenovo XClarity Essentials

Lenovo offers the following XClarity Essentials software tools that can help you set up, use, and maintain the server at no additional cost:

- Lenovo XClarity Essentials OneCLI
  OneCLI is a collection of server management tools that utilize a command line interface program to manage firmware, hardware, and operating systems. It provides functions to collect full system health information (including health status), configure system setting, and update system firmware and drivers.
- Lenovo XClarity Essentials UpdateXpress
  The UpdateXpress tool is a standalone GUI application for firmware and device driver updates that enables you to maintain your server firmware and device drivers up-to-date and help you avoid unnecessary server outages. The tool acquires and deploys individual updates and UpdateXpress System Packs (UXSPs) which are integration-tested bundles.
- Lenovo XClarity Essentials Bootable Media Creator
  The Bootable Media Creator (BOMC) tool is used to create bootable media for offline firmware update.

For more information and downloads, visit the Lenovo XClarity Essentials web page:
http://support.lenovo.com/us/en/documents/LNVO-center

Lenovo XClarity Administrator

Lenovo XClarity is a centralized systems management solution that helps administrators deliver infrastructure faster. This solution integrates easily with Lenovo x86 servers, RackSwitch switches, and DS Series storage, providing automated agent-less discovery, monitoring, firmware updates, configuration management, and bare metal deployment of operating systems and hypervisors across multiple servers.

Lenovo XClarity Administrator is an optional software component for the SR530 server which can be downloaded and used at no charge to discover and monitor the SR530 and manage firmware upgrades for them.

If software support is required for Lenovo XClarity Administrator, or Lenovo XClarity Administrator premium features (such as configuration management and operating system deployment) are required, or both, Lenovo XClarity Pro software subscription should be ordered. Lenovo XClarity Pro is licensed on a per managed system basis, that is, each managed Lenovo system requires a license.

The following table lists the geo-specific Lenovo XClarity software license options.

Table 42. Lenovo XClarity software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Pro, per Managed Endpoint w/1 Yr SW S&S	00MT201	00MT207	1
Lenovo XClarity Pro, per Managed Endpoint w/3 Yr SW S&S	00MT202	00MT208	1
Lenovo XClarity Pro, per Managed Endpoint w/5 Yr SW S&S	00MT203	00MT209	1

* NA = North America; AP = Asia Pacific
** EMEA = Europe, Middle East, Africa; LA = Latin America

Lenovo XClarity Administrator offers the following standard features that are available at no charge:

- Auto-discovery and monitoring of Lenovo x86 servers, RackSwitch switches, Flex System chassis, and DS Series storage systems
- Firmware updates and compliance enforcement
- External alerts and notifications via SNMP traps, syslog remote logging, and e-mail
- Secure connections to managed endpoints
- NIST 800-131A or FIPS 140-2 compliant cryptographic standards between the management solution and managed endpoints
- Integration into existing higher level management systems such as cloud automation and orchestration tools through REST APIs, providing extensive external visibility and control over hardware resources
- An intuitive, easy-to-use GUI
- Scripting with Windows PowerShell, providing command-line visibility and control over hardware resources

Lenovo XClarity Administrator offers the following premium features that require an optional Pro license:

- Pattern-based configuration management that allows to define configurations once and apply repeatedly without errors when deploying new servers or redeploying existing servers without disrupting the fabric
- Bare-metal deployment of operating systems and hypervisors to streamline infrastructure provisioning

For more information, refer to the Lenovo XClarity Administrator Product Guide:
http://lenovopress.com/tips1200

Lenovo XClarity Integrators

Lenovo offers at no charge (if software support is required, a Lenovo XClarity Pro software subscription license should be ordered) two software plug-in modules, Lenovo XClarity Integrators, to manage physical infrastructure from leading external virtualization management software tools from Microsoft and VMware:

- Lenovo XClarity Integrator for Microsoft System Center
- Lenovo XClarity Integrator for VMware vCenter

Lenovo XClarity Integrators offer the following additional features:

- Ability to discover, manage, and monitor Lenovo server hardware from VMware vCenter or Microsoft System Center
- Deployment of firmware updates and configuration patterns to Lenovo x86 rack servers and Flex System from the virtualization management tool
- Non-disruptive server maintenance in clustered environments that reduces workload downtime by dynamically migrating workloads from affected hosts during rolling server updates or reboots
- Greater service level uptime and assurance in clustered environments during unplanned hardware events by dynamically triggering workload migration from impacted hosts when impending hardware failures are predicted

For more information, refer to the Lenovo XClarity Integrators web page:
http://www3.lenovo.com/us/en/data-center/software/systems-management/xclarity-integrators

Lenovo XClarity Energy Manager

Lenovo XClarity Energy Manager provides a stand-alone, web-based agent-less power management console that provides real time data and enables you to observe, plan and manage power and cooling for Lenovo servers. Using built-in intelligence, it identifies server power consumption trends and ideal power settings and performs cooling analysis so that you can define and optimize power-saving policies.

Lenovo XClarity Energy Manager offers the following capabilities:

- Monitors room, row, rack, and device levels in the data center
- Reports vital server information, such as power, temperature and resource utilization
- Monitors inlet temperature to locate hot spots, reducing the risk of data or device damage
- Provides finely-grained controls to limit platform power in compliance with IT policy
- Generates alerts when a user-defined threshold is reached

Lenovo XClarity Energy Manager is an optional software component for the SR530 server that is licensed on a per managed node basis, that is, each managed server requires a license. The 1-node Energy Manager license is included in the XClarity Controller Enterprise upgrade.

To manage systems without XClarity Controller Enterprise licenses, a node license pack should be purchased. The following table lists the geo-specific Lenovo XClarity Energy Manager software license options.

Table 43. Lenovo XClarity Energy Manager software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Energy Manager, 1 Node w/ 1 Yr S&S	01DA225	01DA228	1

* NA = North America; AP = Asia Pacific.
** EMEA = Europe, Middle East, Africa; LA = Latin America.

For more information, refer to the Lenovo XClarity Energy Manager web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lxem

Lenovo Capacity Planner

Lenovo Capacity Planner is a power consumption evaluation tool that enhances data center planning by enabling IT administrators and pre-sales professionals to understand various power characteristics of racks, servers, and other devices. Capacity Planner can dynamically calculate the power consumption, current, British Thermal Unit (BTU), and volt-ampere (VA) rating at the rack level, improving the planning efficiency for large-scale deployments.

For more information, refer to the Capacity Planner web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

Security

The SR530 server offers the following security features:

- Power-on password
- Administrator's password
- Secure firmware updates
- Onboard Trusted Platform Module (TPM) version 1.2 or 2.0 (configurable UEFI system setting)
- Trusted Cryptographic Module (TCM) (optional; available in PRC only)
- Nationz Trusted Platform Module v2.0 (optional; available in PRC only)
- Lockable front bezel (optional)
- Security Key Lifecycle Manager (SKLM) encryption key management for SEDs - FoD upgrade (optional)
- Lenovo Business Vantage security software (optional; available in PRC only)

The server is NIST SP 800-147B compliant.

The following table lists the security options that are available for the SR530 server.

Table 44. Security options

Description	Part number	Feature code	Maximum quantity
Lockable front bezel			
ThinkSystem 1U Security Bezel	7Z17A02581	AUWR	1
Trusted Cryptographic Module (PRC only)			
ThinkSystem Trusted Cryptographic Module	None*	AVKE	1
Trusted Platform Module (PRC only)			
ThinkSystem Nationz Trusted Platform Module v2.0	None*	B22N	1
Security Key Lifecycle Manager - FoD (United States, Canada, Asia Pacific, and Japan)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00D9998	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00D9999	AS6C	1
Security Key Lifecycle Manager - FoD (Latin America, Europe, Middle East, and Africa)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00FP648	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00FP649	AS6C	1

* Factory-installed only; no field upgrade.

Lenovo Business Vantage is a security software tool suite (available only in PRC) designed to work with the TCM or Nationz TPM for enhanced security, to keep user data safe, and to erase confidential data completely from a drive.

Lenovo Business Vantage provides the following features:

- Encrypts files to ensure data safety by using the TCM or Nationz TPM.
- Erases confidential data from a hard disk.
- Prohibits unauthorized access to the USB port of devices.
- Encrypts files to ensure data security on a USB storage device.

For more information, refer to the Lenovo Business Vantage web page:
http://support.lenovo.com.cn/lenovo/wsi/es/es.html

Rack installation

The following table lists the rack installation options that are available for the SR530 server.

Table 45. Rack installation options

Description	Part number	Feature code	Maximum quantity
4-post rail kits			
ThinkSystem Tool-less Slide Rail	7M27A05702	AXCA	1
ThinkSystem Tool-less Slide Rail Kit with 1U CMA	7M27A05701	AXCB	1
ThinkSystem Screw-in Slide Rail	4M17A07274	AXFN	1
ThinkSystem Screw-in Slide Rail Kit with 1U CMA	4M17A07281	B0TE	1
ThinkSystem Tool-less Friction Rail	4M17A07273	AXFM	1
Cable management arm (CMA) upgrade			
ThinkSystem 1U CMA Upgrade Kit for Tool-less Slide Rail	7M27A05699	None^	1*
ThinkSystem 1U CMA Upgrade Kit for Screw-in Slide Rail	4M17A07276	AXFP	1**
Front VGA port			
ThinkSystem SR530/SR630 Front VGA Connector (for 3.5" models)	None***	AUWU	1
ThinkSystem SR530/SR570/SR630 Front VGA Connector Upgrade Kit (for 2.5" models)	7Z17A02579	AUWW	1

^ Field upgrade only.
* The CMA Upgrade Kit for Tool-less Slide Rail is supported with the Tool-less Slide Rail (7M27A05702) only.
** The CMA Upgrade Kit for Screw-in Slide Rail is supported with the Screw-in Slide Rail (4M17A07274) only.
*** Factory-installed only; no field upgrade.

The following table summarizes the rail kit features and specifications.

Table 46. Rail kit features and specifications summary

Feature	Tool-less Slide Rail		Screw-in Slide Rail		Tool-less Friction Rail
	Without CMA	With CMA	Without CMA	With CMA	
Part number	7M27A05702	7M27A05701	4M17A07274	4M17A07281	4M17A07273
CMA	7M27A05699	Included	4M17A07276	Included	No support
Rail length	730 mm (28.74 in.)	807 mm (31.8 in.)	836.8 mm (32.9 in.)	836.8 mm (32.9 in.)	728.1 mm (28.7 in.)
Rail type	Full-out slide (ball bearing)		Full-out slide (ball bearing)		Half-out slide (friction)
Tool-less installation	Yes		No		Yes
In-rack server maintenance	Yes		Yes		No
1U PDU support	Yes		Yes		Yes
0U PDU support	Limited*		Limited*		Limited**
Rack type	IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant
Mounting holes	Square or round		Square, round, or threaded		Square or round
Mounting flange thickness	2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)
Distance between front and rear mounting flanges^	609.6 mm (24 in.) – 863.6 mm (34 in.)		609.6 mm (24 in.) – 812.8 mm (32 in.)		609.6 mm (24 in.) – 863.6 mm (34 in.)

* If a 0U PDU is used, the rack cabinet must be at least 1100 mm (43.31 in.) deep if no CMA is used, or at least 1200 mm (47.24 in.) deep if a CMA is used.
** If a 0U PDU used, the rack must be at least 1000 mm (39.37 in.) deep.
^ Measured when mounted on the rack, from the front surface of the front mounting flange to the rear most point of the rail.

Operating systems

The server supports the following operating systems:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 8.1
- Red Hat Enterprise Linux 8.2
- Red Hat Enterprise Linux 8.3
- SUSE Linux Enterprise Server 12 SP4
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 12 Xen SP4
- SUSE Linux Enterprise Server 12 Xen SP5
- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Server 15 SP1
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 15 Xen
- SUSE Linux Enterprise Server 15 Xen SP1
- SUSE Linux Enterprise Server 15 Xen SP2
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2

For a complete list of supported, certified and tested operating systems, plus additional details and links to relevant web sites, see the Operating System Interoperability Guide: https://lenovopress.com/osig#servers=sr530-7x07-7x08-sp-gen-2

For configure-to-order configurations, the server can be preloaded with VMware ESXi installed on M.2 cards. Ordering information is listed in the following table.

Table 47. VMware ESXi preload

Part number	Feature code	Description
CTO only	B3VW	VMware ESXi 6.5 U2 (Factory Installed)
CTO only	B6U0	VMware ESXi 6.5 U3 (factory installed)
CTO only	B3VX	VMware ESXi 6.7 (Factory Installed)
CTO only	B4XA	VMware ESXi 6.7 U1 (Factory Installed)
CTO only	B6U1	VMware ESXi 6.7 U2 (factory installed)
CTO only	B88T	VMware ESXi 6.7 U3 (factory installed)
CTO only	BBZG	VMware ESXi 7.0 (Factory Installed)
CTO only	BE5E	VMware ESXi 7.0 U1 (Factory Installed)

Physical specifications

The SR530 has the following overall physical dimensions, excluding components that extend outside the standard chassis, such as EIA flanges, front security bezel (if any), and power supply handles:

- Width: 435 mm (17.1 inches)
- Height: 43 mm (1.7 inches)

- Depth: 750 mm (29.5 inches)

The following table lists the detailed dimensions. See the figure below for the definition of each dimension.

Table 48. Detailed dimensions

Dimension	Description
482 mm	X_a = Width, to the outsides of the front EIA flanges
435 mm	X_b = Width, to the rack rail mating surfaces
435 mm	X_c = Width, to the outer most chassis body feature
43 mm	Y_a = Height, from the bottom of chassis to the top of the chassis
715 mm	Z_a = Depth, from the rack flange mating surface to the rearmost I/O port surface
716 mm	Z_b = Depth, from the rack flange mating surface to the rearmost feature of the chassis body
744 mm	Z_c = Depth, from the rack flange mating surface to the rearmost feature such as power supply handle
35 mm	Z_d = Depth, from the forwardmost feature on front of EIA flange to the rack flange mating surface
47 mm	Z_e = Depth, from the front of security bezel (if applicable) or forwardmost feature to the rack flange mating surface

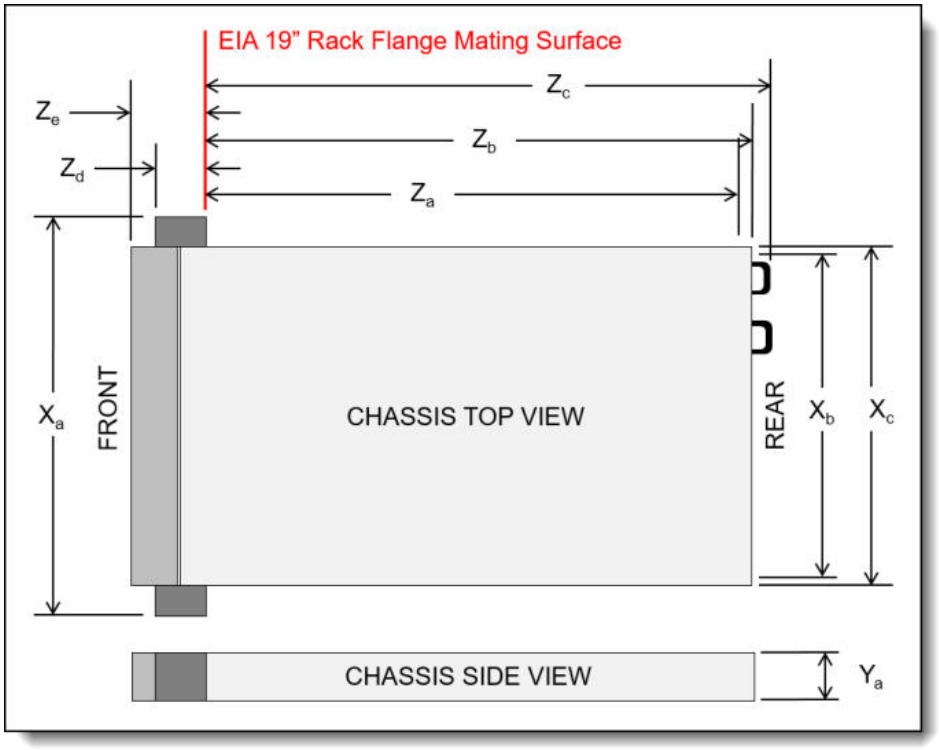


Figure 8. Server dimensions

The shipping dimensions (cardboard packaging) of the SR530 are as follows:

- Width: 587 mm (23.1 inches)
- Height: 225 mm (8.9 inches)
- Depth: 998 mm (39.3 inches)

The SR530 server has the following weight:

- Minimum configuration: 10.2 kg (22.5 lb)
- Maximum configuration: 16.0 kg (35.3 lb)

Operating environment

The SR530 server complies with ASHRAE class A2 specifications. The server performance might be impacted when the operating temperature is outside the ASHRAE A2 specifications. Depending on the hardware configuration, some server models comply with ASHRAE class A3 and class A4 specifications. To comply with ASHRAE class A3 and class A4 specifications, the server models must meet the following hardware configuration requirements at the same time:

- Two power supplies must be installed
- No system fan failure

The SR530 server is supported in the following environment:

- Air temperature:
  - Operating:
    - ASHRAE Class A4: 5 °C - 45 °C (41 °F - 113 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 125-m (410-ft) increase in altitude
    - ASHRAE Class A3: 5 °C - 40 °C (41 °F - 104 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 175-m (574-ft) increase in altitude
    - ASHRAE Class A2: 10 °C - 35 °C (50 °F - 95 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 300-m (984-ft) increase in altitude
  - Non-operating: 5 °C - 45 °C (41 °F - 113 °F)
  - Storage: -40 °C - +60 °C (-40 °F - 140 °F)
- Maximum altitude: 3,050 m (10,000 ft)
- Humidity:
  - Operating:
    - ASHRAE Class A4: 8% - 90% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A3: 8% - 85% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A2: 8% - 80% (non-condensing); maximum dew point: 21 °C (70 °F)
  - Storage: 8% - 90% (non-condensing)
- Electrical:
  - 100 - 127 (nominal) V AC; 50 Hz / 60 Hz
  - 200 - 240 (nominal) V AC; 50 Hz / 60 Hz
  - 180 - 300 V DC (HVDC; supported in PRC only)
- Acoustics:
  - Minimum configuration:
    - Operating: 5.0 bels
    - Idle: 4.5 bels
  - Maximum configuration:
    - Operating: 5.5 bels
    - Idle: 5.2 bels
- Vibration:
  - Operating: 0.21 G rms at 5 Hz to 500 Hz for 15 minutes across 3 axes
  - Non-operating: 1.04 G rms at 2 Hz to 200 Hz for 15 minutes across 6 surfaces
- Shock:
  - Operating: 15 G for 3 milliseconds in each direction (positive and negative X, Y, and Z axes)
  - Non-operating:
    - 12 kg - 22 kg: 50 G for 152 in./sec velocity change across 6 surfaces
    - 23 kg - 31 kg: 35 G for 152 in./sec velocity change across 6 surfaces

The following table lists the maximum system power load, rated inlet current, and system heat output based on the power supply and source voltage.

Table 49. Rated system power, inlet current, and system heat output

Power supply	Source voltage	Maximum power load per system (two power supplies)	Rated current per inlet	System heat output
550 W Platinum	100 - 127 V AC	722 W	6.2 A	2463 BTU/hour
	200 - 240 V AC	704 W	3 A	2402 BTU/hour
	180 - 300 V DC	702 W	2.5 A	2395 BTU/hour
750 W Platinum	100 - 127 V AC	984 W	8.4 A	3357 BTU/hour
	200 - 240 V AC	958 W	4.1 A	3269 BTU/hour
	180 - 300 V DC	958 W	3.5 A	3269 BTU/hour
750 W Titanium	200 - 240 V AC	949 W	4.1 A	3238 BTU/hour
	180 - 300 V DC	948 W	3.5 A	3235 BTU/hour

Warranty and support

The SR530 server has a one-year (7X07) or three-year (Machine Type 7X08) warranty.

The standard warranty terms are customer-replaceable unit (CRU) and onsite (for field-replaceable units FRUs only) with standard call center support during normal business hours and 9x5 Next Business Day Parts Delivered.

Lenovo's additional support services provide a sophisticated, unified support structure for your data center, with an experience consistently ranked number one in customer satisfaction worldwide. Available offerings include:

- **Premier Support**

  Premier Support provides a Lenovo-owned customer experience and delivers direct access to technicians skilled in hardware, software, and advanced troubleshooting, in addition to the following:

  - Direct technician-to-technician access through a dedicated phone line
  - 24x7x365 remote support
  - Single point of contact service
  - End to end case management
  - Third-party collaborative software support
  - Online case tools and live chat support
  - On-demand remote system analysis
- **Warranty Upgrade (Preconfigured Support)**

  Services are available to meet the on-site response time targets that match the criticality of your systems.

  - 3, 4, or 5 years of service coverage
  - 1-year or 2-year post-warranty extensions
  - **Foundation Service**: 9x5 service coverage with next business day onsite response. YourDrive YourData is an optional extra (see below).
  - **Essential Service:** 24x7 service coverage with 4-hour onsite response or 24-hour committed repair (available only in select countries). Bundled with YourDrive YourData.
  - **Advanced Service:** 24x7 service coverage with 2-hour onsite response or 6-hour committed repair (available only in select countries). Bundled with YourDrive YourData.

- **Managed Services**

  Lenovo Managed Services provides continuous 24x7 remote monitoring (plus 24x7 call center availability) and proactive management of your data center using state-of-the-art tools, systems, and practices by a team of highly skilled and experienced Lenovo services professionals.

  Quarterly reviews check error logs, verify firmware & OS device driver levels, and software as needed. We'll also maintain records of latest patches, critical updates, and firmware levels, to ensure you systems are providing business value through optimized performance.

- **Technical Account Management (TAM)**

  A Lenovo Technical Account Manager helps you optimize the operation of your data center based on a deep understanding of your business. You gain direct access to your Lenovo TAM, who serves as your single point of contact to expedite service requests, provide status updates, and furnish reports to track incidents over time. In addition, your TAM will help proactively make service recommendations and manage your service relationship with Lenovo to make certain your needs are met.

- **Enterprise Server Software Support**

  Enterprise Software Support is an additional support service providing customers with software support on Microsoft, Red Hat, SUSE, and VMware applications and systems. Around the clock availability for critical problems plus unlimited calls and incidents helps customers address challenges fast, without incremental costs. Support staff can answer troubleshooting and diagnostic questions, address product comparability and interoperability issues, isolate causes of problems, report defects to software vendors, and more.

- **YourDrive YourData**

  Lenovo's YourDrive YourData is a multi-drive retention offering that ensures your data is always under your control, regardless of the number of drives that are installed in your Lenovo server. In the unlikely event of a drive failure, you retain possession of your drive while Lenovo replaces the failed drive part. Your data stays safely on your premises, in your hands. The YourDrive YourData service can be purchased in convenient bundles and is optional with Foundation Service. It is bundled with Essential Service and Advanced Service.

- **Health Check**

  Having a trusted partner who can perform regular and detailed health checks is central to maintaining efficiency and ensuring that your systems and business are always running at their best. Health Check supports Lenovo-branded server, storage, and networking devices, as well as select Lenovo-supported products from other vendors that are sold by Lenovo or a Lenovo-Authorized Reseller.

Examples of region-specific warranty terms are second or longer business day parts delivery or parts-only base warranty.

If warranty terms and conditions include onsite labor for repair or replacement of parts, Lenovo will dispatch a service technician to the customer site to perform the replacement. Onsite labor under base warranty is limited to labor for replacement of parts that have been determined to be field-replaceable units (FRUs). Parts that are determined to be customer-replaceable units (CRUs) do not include onsite labor under base warranty.

If warranty terms include parts-only base warranty, Lenovo is responsible for delivering only replacement parts that are under base warranty (including FRUs) that will be sent to a requested location for self-service. Parts-only service does not include a service technician being dispatched onsite. Parts must be changed at customer's own cost and labor and defective parts must be returned following the instructions supplied with the spare parts.

Lenovo Service offerings are region-specific. Not all preconfigured support and upgrade options are available in every region. For information about Lenovo service upgrade offerings that are available in your region, refer to the following resources:

- Service part numbers in Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com/#/services
- Lenovo Services Availability Locator
  http://lenovolocator.com/

For service definitions, region-specific details, and service limitations, please refer to the following documents:

- Lenovo Statement of Limited Warranty for Data Center Group (DCG) Servers and System Storage
  http://pcsupport.lenovo.com/us/en/solutions/ht503310
- Lenovo Data Center Services Agreement
  http://support.lenovo.com/us/en/solutions/ht116628

Services

Lenovo Services is a dedicated partner to your success. Our goal is to reduce your capital outlays, mitigate your IT risks, and accelerate your time to productivity.

Note: Some service options may not be available in all countries. For more information, go to https://www.lenovo.com/systems/services. For information about Lenovo service upgrade offerings that are available in your region, contact your local Lenovo sales representative or business partner.

Here's a more in-depth look at what we can do for you:

- **Asset Recovery Services**

  Asset Recovery Services (ARS) helps customers recover the maximum value from their end-of-life equipment in a cost-effective and secure way. On top of simplifying the transition from old to new equipment, ARS mitigates environmental and data security risks associated with data center equipment disposal. Lenovo ARS is a cash-back solution for equipment based on its remaining market value, yielding maximum value from aging assets and lowering total cost of ownership for your customers. For more information, see the ARS page, https://lenovopress.com/lp1266-reduce-e-waste-and-grow-your-bottom-line-with-lenovo-ars.

- **Assessment Services**

  An Assessment helps solve your IT challenges through an onsite, multi-day session with a Lenovo technology expert. We perform a tools-based assessment which provides a comprehensive and thorough review of a company's environment and technology systems. In addition to the technology based functional requirements, the consultant also discusses and records the non-functional business requirements, challenges, and constraints. Assessments help organizations like yours, no matter how large or small, get a better return on your IT investment and overcome challenges in the ever-changing technology landscape.

- **Design Services**

  Professional Services consultants perform infrastructure design and implementation planning to support your strategy. The high-level architectures provided by the assessment service are turned into low level designs and wiring diagrams, which are reviewed and approved prior to implementation. The implementation plan will demonstrate an outcome-based proposal to provide business capabilities through infrastructure with a risk-mitigated project plan.

- **Basic Hardware Installation**

  Lenovo experts can seamlessly manage the physical installation of your server, storage, or networking hardware. Working at a time convenient for you (business hours or off shift), the technician will unpack and inspect the systems on your site, install options, mount in a rack cabinet, connect to power and network, check and update firmware to the latest levels, verify operation, and dispose of the packaging, allowing your team to focus on other priorities.

- **Deployment Services**

  When investing in new IT infrastructures, you need to ensure your business will see quick time to value with little to no disruption. Lenovo deployments are designed by development and engineering teams who know our Products & Solutions better than anyone else, and our technicians own the process from delivery to completion. Lenovo will conduct remote preparation and planning, configure & integrate systems, validate systems, verify and update appliance firmware, train on administrative tasks, and provide post-deployment documentation. Customer's IT teams leverage our skills to enable IT staff to transform with higher level roles and tasks.

- **Integration, Migration, and Expansion Services**

  Move existing physical & virtual workloads easily, or determine technical requirements to support increased workloads while maximizing performance. Includes tuning, validation, and documenting ongoing run processes. Leverage migration assessment planning documents to perform necessary migrations.

Regulatory compliance

The ThinkSystem SR530 server conforms to the following regulations:

- United States: FCC Part 15, Class A; UL 60950-1
- Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1
- Mexico: NOM-19
- Argentina: IEC60950-1
- European Union: CE Mark (EN55022 Class A, IEC/EN60950-1, EN55024, EN61000-3-2, EN61000-3-3)
- Germany: TUV-GS (IEC/EN 60950-1, EK1-ITB2000)
- Russia, Kazakhstan, Belarus: EAC (TR CU 004/2011, TR CU 020/2011)
- China: CCC GB4943.1, GB9254 Class A, GB17625.1
- India: BIS
- Japan: VCCI, Class A
- Taiwan: BSMI CNS13438, Class A; CNS14336-1
- Korea: KN22, Class A; KN24
- Australia/New Zealand: AS/NZS CISPR 22 Class A
- Reduction of Hazardous Substances (ROHS)
- Energy Star 3.0 (excluding configurations with Bronze 3204, Gold 5222, or Platinum 8256 processors)

Note: For more information on the Energy Star 3.0 certification, refer to the *Energy Star 3.0 Certifications for ThinkSystem Servers* publication:
http://lenovopress.com/lp1230

External drive enclosures

The server supports attachment to external drive enclosures using a RAID controller with external ports or a SAS host bus adapter. Adapters supported by the server are listed in the SAS adapters for external storage section.

Note: Information provided in this section is for ordering reference purposes only. For the operating system and adapter support details, refer to the interoperability matrix for a particular storage enclosure that can be found on the Lenovo Data Center Support web site:
http://datacentersupport.lenovo.com

Table 50. External drive enclosures

Description	Part number		
	Worldwide	Japan	PRC
Lenovo Storage D1212 LFF Disk Expansion with Dual SAS IO Modules	4587A11	4587A1J	4587A1C
Lenovo Storage D1224 SFF Disk Expansion with Dual SAS IO Modules	4587A31	4587A3J	4587A3C
Lenovo Storage D3284 4TB x 84 HD Expansion Enclosure	641311F		
Lenovo Storage D3284 6TB x 84 HD Expansion Enclosure	641312F		
Lenovo Storage D3284 8TB x 84 HD Expansion Enclosure	641313F		
Lenovo Storage D3284 10TB x 84 HD Expansion Enclosure	641314F		

For details about supported drives, adapters, and cables, see the following Lenovo Press Product Guides:

- Lenovo Storage D1212 and D1224
  http://lenovopress.com/lp0512
- Lenovo Storage D3284
  http://lenovopress.com/lp0513

External storage systems

Lenovo offers the ThinkSystem DE Series and ThinkSystem DM Series external storage systems for high-performance storage. See the DE Series and DM Series product guides for specific controller models, expansion enclosures and configuration options:

- ThinkSystem DE Series Storage
  https://lenovopress.com/storage/thinksystem/de-series#rt=product-guide
- ThinkSystem DM Series Storage
  https://lenovopress.com/storage/thinksystem/dm-series#rt=product-guide

External backup units

The following table lists the external backup options that are offered by Lenovo.

Table 51. External backup options

Part number	Description
External RDX USB drives	
4T27A10725	ThinkSystem RDX External USB 3.0 Dock
External SAS tape backup drives	
6160S6E	IBM TS2260 Tape Drive Model H6S
6160S7E	IBM TS2270 Tape Drive Model H7S
6160S8E	IBM TS2280 Tape Drive Model H8S
External SAS tape backup autoloaders	
6171S5R	IBM TS2900 Tape Autoloader w/LTO5 HH SAS
6171S6R	IBM TS2900 Tape Autoloader w/LTO6 HH SAS
6171S7R	IBM TS2900 Tape Autoloader w/LTO7 HH SAS
External tape backup libraries	
6741A1F	IBM TS4300 3U Tape Library-Base Unit
6741A3F	IBM TS4300 3U Tape Library-Expansion Unit
Full High 8 Gb Fibre Channel for TS4300	
01KP954	LTO 8 FH Fibre Channel Drive
01KP938	LTO 7 FH Fibre Channel Drive
01KP935	LTO 6 FH Fibre Channel Drive
Half High 8 Gb Fibre Channel for TS4300	
01KP952	LTO 8 HH Fibre Channel Drive
01KP936	LTO 7 HH Fibre Channel Drive
01KP933	LTO 6 HH Fibre Channel Drive
Half High 6 Gb SAS for TS4300	
01KP953	LTO 8 HH SAS Drive
01KP937	LTO 7 HH SAS Drive
01KP934	LTO 6 HH SAS Drive

For more information, see the list of Product Guides in the Backup units category:
https://lenovopress.com/servers/options/backup

Fibre Channel SAN switches

Lenovo offers the ThinkSystem DB Series of Fibre Channel SAN switches and directors for high-performance storage expansion. See the DB Series product guides for models and configuration options:

- ThinkSystem DB Series SAN Switches and Directors: https://lenovopress.com/storage/switches/rack#rt=product-guide

Rack cabinets

The following table lists the supported rack cabinets.

Table 52. Rack cabinets

Part number	Description
7D2B0001WW / 7D2N0001WW	12U 1200mm Deep Micro Datacenter Rack
7D2C0001WW / 7D2P0001WW	18U 1200mm Deep Micro Datacenter Rack
93072RX	25U Standard Rack
93072PX	25U Static S2 Standard Rack
93634PX	42U 1100mm Dynamic Rack
93634EX	42U 1100mm Dynamic Expansion Rack
93604PX	42U 1200mm Deep Dynamic Rack
93614PX	42U 1200mm Deep Static Rack
93084EX	42U Enterprise Expansion Rack
93084PX	42U Enterprise Rack
93074RX	42U Standard Rack

For specifications about these racks, see the Lenovo Rack Cabinet Reference, available from: https://lenovopress.com/lp1287-lenovo-rack-cabinet-reference

For more information, see the list of Product Guides in the Rack cabinets category: https://lenovopress.com/servers/options/racks

KVM switches and consoles

The following table lists the supported KVM consoles, keyboards, and KVM switches.

Table 53. Console keyboards

Part number	Description
Console keyboards	
7ZB7A05469	ThinkSystem Keyboard w/ Int. Pointing Device USB - Arabic 253 RoHS v2
7ZB7A05468	ThinkSystem Keyboard w/ Int. Pointing Device USB - Belg/UK 120 RoHS v2
7ZB7A05206	ThinkSystem Keyboard w/ Int. Pointing Device USB - Czech 489 RoHS v2
7ZB7A05207	ThinkSystem Keyboard w/ Int. Pointing Device USB - Danish 159 RoHS v2
7ZB7A05208	ThinkSystem Keyboard w/ Int. Pointing Device USB - Dutch 143 RoHS v2
7ZB7A05210	ThinkSystem Keyboard w/ Int. Pointing Device USB - Fr/Canada 445 RoHS v2
7ZB7A05209	ThinkSystem Keyboard w/ Int. Pointing Device USB - French 189 RoHS v2
7ZB7A05211	ThinkSystem Keyboard w/ Int. Pointing Device USB - German 129 RoHS v2
7ZB7A05212	ThinkSystem Keyboard w/ Int. Pointing Device USB - Greek 219 RoHS v2
7ZB7A05213	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hebrew 212 RoHS v2
7ZB7A05214	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hungarian 208 RoHS v2

Part number	Description
7ZB7A05215	ThinkSystem Keyboard w/ Int. Pointing Device USB - Italian 141 RoHS v2
7ZB7A05216	ThinkSystem Keyboard w/ Int. Pointing Device USB - Japanese 194 RoHS v2
7ZB7A05217	ThinkSystem Keyboard w/ Int. Pointing Device USB - Korean 413 RoHS v2
7ZB7A05218	ThinkSystem Keyboard w/ Int. Pointing Device USB - LA Span 171 RoHS v2
7ZB7A05219	ThinkSystem Keyboard w/ Int. Pointing Device USB - Norwegian 155 RoHS v2
7ZB7A05220	ThinkSystem Keyboard w/ Int. Pointing Device USB - Polish 214 RoHS v2
7ZB7A05221	ThinkSystem Keyboard w/ Int. Pointing Device USB - Portuguese 163 RoHS v2
7ZB7A05222	ThinkSystem Keyboard w/ Int. Pointing Device USB - Russian 441 RoHS v2
7ZB7A05223	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovak 245 RoHS v2
7ZB7A05231	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovenian 234 RoHS v2
7ZB7A05224	ThinkSystem Keyboard w/ Int. Pointing Device USB - Spanish 172 RoHS v2
7ZB7A05225	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swed/Finn 153 RoHS v2
7ZB7A05226	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swiss F/G 150 RoHS v2
7ZB7A05227	ThinkSystem Keyboard w/ Int. Pointing Device USB - Thai 191 RoHS v2
7ZB7A05467	ThinkSystem Keyboard w/ Int. Pointing Device USB - Trad Chinese/US 467 RoHS v2
7ZB7A05228	ThinkSystem Keyboard w/ Int. Pointing Device USB - Turkish 179 RoHS v2
7ZB7A05229	ThinkSystem Keyboard w/ Int. Pointing Device USB - UK Eng 166 RoHS v2
7ZB7A05470	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Eng 103P RoHS v2
7ZB7A05230	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Euro 103P RoHS v2
ThinkSystem Digital and Analog KVM Console switches and cables	
1754D1T	ThinkSystem Digital 2x1x16 KVM Switch (DVI video output port)
1754A1T	ThinkSystem Analog 1x8 KVM Switch (DVI video output port)
4X97A11108	ThinkSystem VGA to DVI Conversion Cable
4X97A11109	ThinkSystem Single-USB Conversion Cable for Digital KVM
4X97A11107	ThinkSystem Dual-USB Conversion Cable for Digital KVM
4X97A11106	ThinkSystem USB Conversion Cable for Analog KVM
GCM and LCM Console switches and cables	
1754D2X	Global 4x2x32 Console Manager (GCM32)
1754D1X	Global 2x2x16 Console Manager (GCM16)
1754A2X	Local 2x16 Console Manager (LCM16)
1754A1X	Local 1x8 Console Manager (LCM8)
43V6147	Single Cable USB Conversion Option (UCO)
39M2895	USB Conversion Option (4 Pack UCO)
46M5383	Virtual Media Conversion Option Gen2 (VCO2)
46M5382	Serial Conversion Option (SCO)

For more information, see the list of Product Guides in the KVM Switches and Consoles category:
http://lenovopress.com/servers/options/kvm

Power distribution units

The following table lists the power distribution units (PDUs) that are offered by Lenovo.

Table 54. Power distribution units

Part number	Description
0U Basic PDUs	
00YJ776	0U 36 C13/6 C19 24A/200-240V 1 Phase PDU with NEMA L6-30P line cord
00YJ777	0U 36 C13/6 C19 32A/200-240V 1 Phase PDU with IEC60309 332P6 line cord
00YJ778	0U 21 C13/12 C19 32A/200-240V/346-415V 3 Phase PDU with IEC60309 532P6 line cord
00YJ779	0U 21 C13/12 C19 48A/200-240V 3 Phase PDU with IEC60309 460P9 line cord
Switched and Monitored PDUs	
00YJ780	0U 20 C13/4 C19 Switched and Monitored 32A/200-240V/1Ph PDU w/ IEC60309 332P6 line cord
00YJ781	0U 20 C13/4 C19 Switched and Monitored 24A/200-240V/1Ph PDU w/ NEMA L6-30P line cord
00YJ782	0U 18 C13/6 C19 Switched / Monitored 32A/200-240V/346-415V/3Ph PDU w/ IEC60309 532P6 cord
00YJ783	0U 12 C13/12 C19 Switched and Monitored 48A/200-240V/3Ph PDU w/ IEC60309 460P9 line cord
46M4003	1U 9 C19/3 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
46M4004	1U 12 C13 Switched and Monitored DPI PDU (without line cord)
46M4005	1U 12 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
Ultra Density Enterprise PDUs (9x IEC 320 C13 + 3x IEC 320 C19 outlets)	
71762NX	Ultra Density Enterprise C19/C13 PDU Module (without line cord)
71763NU	Ultra Density Enterprise C19/C13 PDU 60A/208V/3ph with IEC 309 3P+Gnd line cord
C13 Enterprise PDUs (12x IEC 320 C13 outlets)	
39M2816	DPI C13 Enterprise PDU+ (without line cord)
39Y8941	DPI Single Phase C13 Enterprise PDU (without line cord)
C19 Enterprise PDUs (6x IEC 320 C19 outlets)	
39Y8948	DPI Single Phase C19 Enterprise PDU (without line cord)
39Y8923	DPI 60A 3 Phase C19 Enterprise PDU with IEC 309 3P+G (208 V) fixed line cord
Front-end PDUs (3x IEC 320 C19 outlets)	
39Y8938	DPI 30amp/125V Front-end PDU with NEMA L5-30P line cord
39Y8939	DPI 30amp/250V Front-end PDU with NEMA L6-30P line cord
39Y8934	DPI 32amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8940	DPI 60amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8935	DPI 63amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
NEMA PDUs (6x NEMA 5-15R outlets)	
39Y8905	DPI 100-127V PDU with Fixed NEMA L5-15P line cord
Line cords for PDUs that ship without a line cord	
40K9611	DPI 32a Line Cord (IEC 309 3P+N+G)
40K9612	DPI 32a Line Cord (IEC 309 P+N+G)
40K9613	DPI 63a Cord (IEC 309 P+N+G)
40K9614	DPI 30a Line Cord (NEMA L6-30P)
40K9615	DPI 60a Cord (IEC 309 2P+G)
40K9617	DPI Australian/NZ 3112 Line Cord
40K9618	DPI Korean 8305 Line Cord

For more information, see the Lenovo Press documents in the PDU category:
https://lenovopress.com/servers/options/pdu

Uninterruptible power supply units

The following table lists the uninterruptible power supply (UPS) units that are offered by Lenovo.

Table 55. Uninterruptible power supply units

Part number	Description
55941AX	RT1.5kVA 2U Rack or Tower UPS (100-125VAC)
55941KX	RT1.5kVA 2U Rack or Tower UPS (200-240VAC)
55942AX	RT2.2kVA 2U Rack or Tower UPS (100-125VAC)
55942KX	RT2.2kVA 2U Rack or Tower UPS (200-240VAC)
55943AX	RT3kVA 2U Rack or Tower UPS (100-125VAC)
55943KX	RT3kVA 2U Rack or Tower UPS (200-240VAC)
55945KX	RT5kVA 3U Rack or Tower UPS (200-240VAC)
55946KX	RT6kVA 3U Rack or Tower UPS (200-240VAC)
55948KX	RT8kVA 6U Rack or Tower UPS (200-240VAC)
55949KX	RT11kVA 6U Rack or Tower UPS (200-240VAC)
55948PX	RT8kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55949PX	RT11kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55943KT†	ThinkSystem RT3kVA 2U Standard UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55943LT†	ThinkSystem RT3kVA 2U Long Backup UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55946KT†	ThinkSystem RT6kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)
5594XKT†	ThinkSystem RT10kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)

† Only available in China and countries in the Asia Pacific region.

For more information, see the list of Product Guides in the UPS category:
https://lenovopress.com/servers/options/ups

Lenovo Financial Services

Lenovo Financial Services reinforces Lenovo's commitment to deliver pioneering products and services that are recognized for their quality, excellence, and trustworthiness. Lenovo Financial Services offers financing solutions and services that complement your technology solution anywhere in the world.

We are dedicated to delivering a positive finance experience for customers like you who want to maximize your purchase power by obtaining the technology you need today, protect against technology obsolescence, and preserve your capital for other uses.

We work with businesses, non-profit organizations, governments and educational institutions to finance their entire technology solution. We focus on making it easy to do business with us. Our highly experienced team of finance professionals operates in a work culture that emphasizes the importance of providing outstanding customer service. Our systems, processes and flexible policies support our goal of providing customers with a positive experience.

We finance your entire solution. Unlike others, we allow you to bundle everything you need from hardware and software to service contracts, installation costs, training fees, and sales tax. If you decide weeks or months later to add to your solution, we can consolidate everything into a single invoice.

Our Premier Client services provide large accounts with special handling services to ensure these complex transactions are serviced properly. As a premier client, you have a dedicated finance specialist who manages your account through its life, from first invoice through asset return or purchase. This specialist develops an in-depth understanding of your invoice and payment requirements. For you, this dedication provides a high-quality, easy, and positive financing experience.

For your region specific offers please ask your Lenovo sales representative or your technology provider about the use of Lenovo Financial Services. For more information, see the following Lenovo website:

https://www.lenovo.com/us/en/landingpage/lenovo-financial-services/

Related publications and links

For more information, see these resources:

- ThinkSystem SR530 product page
  https://www.lenovo.com/us/en/data-center/servers/racks/ThinkSystem-SR530/p/77XX7SRSR53
- Datasheet for the ThinkSystem SR530:
  https://lenovopress.com/ds0002-lenovo-thinksystem-sr530
- 3D Interactive Tour of the ThinkSystem SR530:
  https://lenovopress.com/lp0670-3d-tour-thinksystem-sr530
- Walkthrough Video for the ThinkSystem SR530:
  https://lenovopress.com/lp0744-thinksystem-sr530-server-video-walkthrough
- User Manuals for the ThinkSystem SR530:
  https://thinksystem.lenovofiles.com/help/topic/7X07/introduction.html?cp=4_2
  - Quick Start Guide
  - Setup Guide
  - Rack Installation Guides
  - Maintenance Manual
  - Messages and Codes Reference
  - UEFI Manual
- Lenovo Data Center Support Downloads - ThinkSystem SR530:
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x07/downloads
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x08/downloads
- Lenovo Hardware Installation & Removal Videos on the ThinkSystem SR530:
  - YouTube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
  - Youku: https://list.youku.com/albumlist/show/id_50437162
- Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com

Related product families

Product families related to this document are the following:

- 2-Socket Rack Servers
- ThinkSystem SR530 Server

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2021. All rights reserved.

This document, LP1045, was created or updated on March 2, 2021.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  http://lenovopress.com/LP1045
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at http://lenovopress.com/LP1045.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
Bootable Media Creator
Flex System
Lenovo Services
RackSwitch
System x®
ThinkSystem
TopSeller
TruDDR4
UpdateXpress System Packs
XClarity®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Hyper-V®, Microsoft®, PowerShell, Windows PowerShell®, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Lenovo

ThinkSystem SR530
Maintenance Manual



Machine Types: 7X07 and 7X08

Note

Before using this information and the product it supports, be sure to read and understand the safety information and the safety instructions, which are available at:
http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html

In addition, be sure that you are familiar with the terms and conditions of the Lenovo warranty for your server, which can be found at:
http://datacentersupport.lenovo.com/warrantylookup

Tenth Edition (May 2020)

© Copyright Lenovo 2017, 2020.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Safety iii
Safety inspection checklist iv

Chapter 1. Introduction 1
Specifications 2
Firmware updates 7
Configuring the LAN over USB interface manually 10
Installing the LAN over USB Windows device driver 10
Tech Tips 11
Security advisories 11
Power on the server 11
Power off the server 11

Chapter 2. Server components 13
Front view 13
Operator information panel 15
Rear view 17
Rear view LEDs 21
System board components 23
System board switches and jumpers 25
System board LEDs 27
Internal cable routing 28
VGA connector 29
Front I/O assembly 31
RAID super capacitor module 32
Backplanes 33
Parts list 36
Power cords 39

Chapter 3. Hardware replacement procedures 41
Installation Guidelines 41
System reliability guidelines 42
Working inside the server with the power on . . 43
Handling static-sensitive devices 43
Rack latches replacement 44
Remove the rack latches 44
Install the rack latches 46
Security bezel replacement 48
Remove the security bezel 48
Install the security bezel 50
Top cover replacement 52
Remove the top cover 52
Install the top cover 54
Air baffle replacement 55
Remove the air baffle 55
Install the air baffle 57
RAID super capacitor module replacement 58
Remove a RAID super capacitor module . . . 58
Install a RAID super capacitor module 60
System fan replacement 62
Remove a system fan 62
Install a system fan 64
Front I/O assembly replacement 65
Remove the front I/O assembly 65
Install the front I/O assembly 66
Hot-swap drive backplane replacement 67
Remove the backplane for four 3.5-inch hot-swap drives 67
Install the backplane for four 3.5-inch hot-swap drives 68
Remove the backplane for eight 2.5-inch hot-swap drives 69
Install the backplane for eight 2.5-inch hot-swap drives 70
Simple-swap drive backplate assembly replacement 71
Remove the simple-swap drive backplate assembly 71
Install the simple-swap drive backplate assembly 72
Hot-swap drive replacement 73
Remove a hot-swap drive 73
Install a hot-swap drive 74
Simple-swap drive replacement 76
Remove a simple-swap drive 76
Install a simple-swap drive 78
Memory module replacement 79
Remove a memory module 79
Memory module installation rules 80
Install a memory module 85
CMOS battery replacement 87
Remove the CMOS battery 87
Install the CMOS battery 89
TCM/TPM adapter replacement (for Chinese Mainland only) 90
Remove the TCM/TPM adapter (for Chinese Mainland only) 90
Install the TCM/TPM adapter (for Chinese Mainland only) 91
Hot-swap power supply replacement 93
Remove a hot-swap power supply 93
Install a hot-swap power supply 99

© Copyright Lenovo 2017, 2020

PCIe adapter replacement 105
Remove a PCIe adapter 105
Install a PCIe adapter 106
Riser card replacement 107
Remove a riser card 107
Install a riser card 109
M.2 backplane and M.2 drive replacement 111
Remove the M.2 backplane and M.2 drive . . . 111
Adjust the retainer on the M.2 backplane . . . 113
Install the M.2 backplane and M.2 drive 114
Serial port module replacement 117
Remove the serial port module 117
Install the serial port module 119
LOM adapter replacement 121
Remove the LOM adapter 121
Install the LOM adapter 122
Processor and heat sink replacement 123
Remove a processor and heat sink 123
Install a processor and heat sink 126
System board replacement 131
Remove the system board 131
Install the system board 134
Update the Universal Unique Identifier (UUID) 135
Update the DMI/SMBIOS data 137
Enable TPM/TCM 139
Enable UEFI Secure Boot 142
Complete the parts replacement 143

Chapter 4. Problem determination 145

Event logs 145
General problem determination procedures 147
Resolving suspected power problems 147
Resolving suspected Ethernet controller problems 148
Troubleshooting by symptom 148
Power on and power off problems 149
Memory problems 150
Hard disk drive problems 151
Monitor and video problems 153
Keyboard, mouse, or USB-device problems 154
Optional-device problems 155
Serial-device problems 157
Intermittent problems 157
Power problems 158
Network problems 158
Observable problems 159
Software problems 161

Appendix A. Getting help and technical assistance 163

Before you call 163
Collecting service data 164
Contacting Support 165

Appendix B. Notices 167

Trademarks 168
Important notes 168
Particulate contamination 168
Telecommunication regulatory statement 169
Electronic emission notices 169
Taiwan BSMI RoHS declaration 170
Taiwan import and export contact information . . . 170

Index 171

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information （安全信息）。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

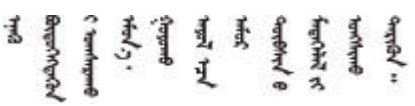
A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.



Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

© Copyright Lenovo 2017, 2020

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

ཐོན་རྫས་འདི་བདེ་སྤྱོད་མ་བྱས་གོང་། ·སྐྱོན་ཐྱི་ཡིད་གཟབ་ བྱ་འདྲ་མིན་ཡོད་པའི་འོད་སྣེར་བལྟ་དགོས།

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun.

.مەزكۇر مەھسۇلاتنى ئورنىتىشتىن بۇرۇن بىخەتەرلىك ئۇچۇرلىرىنى ئوقۇپ چىقىڭ

Youq mwngz yungh canjbinj neix gaxgonq, itdingh aeu doeg aen canjbinj soengq cungj vahgangj ancien siusik.

Safety inspection checklist

Use the information in this section to identify potentially unsafe conditions with your server. As each machine was designed and built, required safety items were installed to protect users and service technicians from injury.

CAUTION:
This equipment must be installed or serviced by trained personnel, as defined by the NEC, IEC 62368-1 & IEC 60950-1, the standard for Safety of Electronic Equipment within the Field of Audio/Video, Information Technology and Communication Technology. Lenovo assumes you are qualified in the servicing of equipment and trained in recognizing hazards energy levels in products. Access to the equipment is by the use of a tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

Important: Electrical grounding of the server is required for operator safety and correct system function. Proper grounding of the electrical outlet can be verified by a certified electrician.

Use the following checklist to verify that there are no potentially unsafe conditions:

1. Make sure that the power is off and the power cord is disconnected.
2. Check the power cord.
   - Make sure that the third-wire ground connector is in good condition. Use a meter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and the frame ground.
   - Make sure that the power cord is the correct type.

     To view the power cords that are available for the server:

     a. Go to:

        http://dcsc.lenovo.com/#/

     b. In the Customize a Model pane:

        1) Click **Select Options/Parts for a Model**.
        2) Enter the machine type and model for your server.

c. Click the Power tab to see all line cords.

- Make sure that the insulation is not frayed or worn.

3. Check for any obvious non-Lenovo alterations. Use good judgment as to the safety of any non-Lenovo alterations.
4. Check inside the server for any obvious unsafe conditions, such as metal filings, contamination, water or other liquid, or signs of fire or smoke damage.
5. Check for worn, frayed, or pinched cables.
6. Make sure that the power-supply cover fasteners (screws or rivets) have not been removed or tampered with.

© Copyright Lenovo 2017, 2020

Chapter 1. Introduction

The ThinkSystem™ SR530 is a general-purpose dual-socket 1U rack server that is great for various IT workloads, include web hosting, entry cloud, and virtualization. It is ideal for small and medium-size business (SMB) customers to run many kinds of applications by offering the latest technology to support multi-core processors, faster memory speed, flexible input/output (I/O) options and tiered system management.

The server comes with a limited warranty. For details about the warranty, see:
https://support.lenovo.com/us/en/solutions/ht503310

For details about your specific warranty, see:
http://datacentersupport.lenovo.com/warrantylookup

Identifying your server

When you contact Lenovo for help, the machine type and serial number information helps support technicians to identify your server and provide faster service.

The machine type and serial number are on the ID label on the right rack latch in the front of the server.

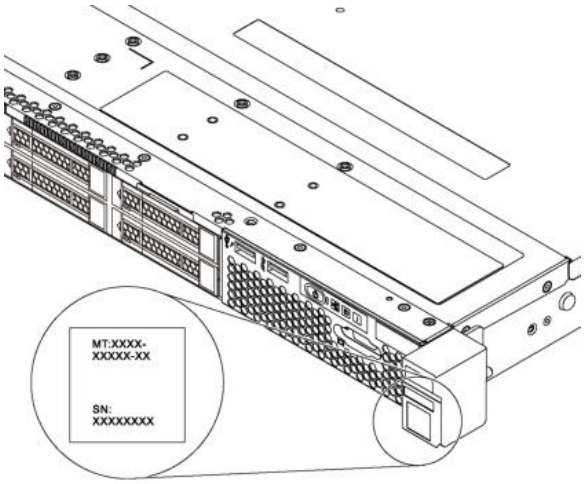


Figure 1. Location of the ID label

© Copyright Lenovo 2017, 2020

XClarity Controller network access label

The XClarity® Controller network access label is attached on the top side of the pull-out information tab. After you get the server, peel the XClarity Controller network access label away and store it in a safe place.

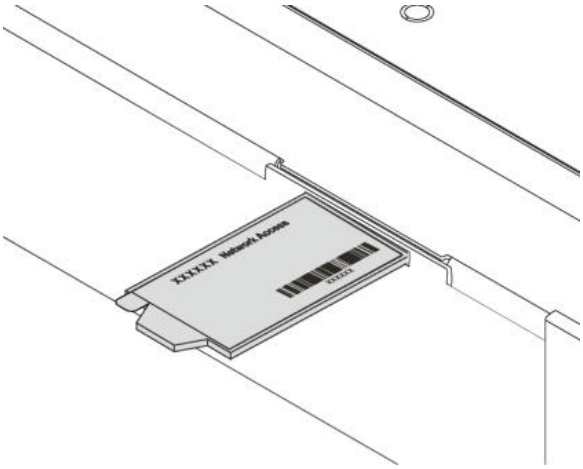


Figure 2. Location of the XClarity Controller network access label

Quick response code

The system service label, which is on the top cover, provides a quick response (QR) code for mobile access to service information. Scan the QR code with a mobile device and a QR code reader application to get quick access to the Lenovo Service web site for this server. The Lenovo Service Information Web site provides additional information for parts installation and replacement videos, and error codes for server support.

The following illustration shows the QR code: https://support.lenovo.com/p/servers/sr530



Figure 3. QR code

Specifications

The following information is a summary of the features and specifications of the server. Depending on the model, some features might not be available, or some specifications might not apply.

Table 1. Server specifications

Specification	Description
Dimension	• Form factor: 1U • Height: 43.0 mm (1.7 inches) • Width: – With rack latches: 482.0 mm (19.0 inches) – Without rack latches: 434.4 mm (17.1 inches) • Depth: 778.3 mm (30.7 inches) **Note:** The depth is measured with rack latches and power supply installed, but without security bezel installed.
Weight	Up to 16.0 kg (35.3 lb), depending on your configuration
Processor (depending on the model)	• Up to two Intel® Xeon® Scalable Processors – Designed for Land Grid Array (LGA) 3647 socket – Scalable up to 20 cores For a list of supported processors, see: http://www.lenovo.com/us/en/serverproven/
Memory	For 1st Generation Intel Xeon Scalable Processor (SP Gen 1) : • Minimum: 8 GB • Maximum: – 384 GB using registered DIMMs (RDIMMs) – 768 GB using load-reduced DIMMs (LRDIMMs) • Type (depending on the model): – TruDDR4 2666, single-rank or dual-rank, 8 GB/16 GB/32 GB RDIMMs – TruDDR4 2666, quad-rank, 64 GB LRDIMMs • Slots: 12 slots For 2nd Generation Intel Xeon Scalable Processor (SP Gen 2): • Minimum: 8 GB • Maximum: 768 GB • Type (depending on the model): – TruDDR4 2666, single-rank or dual-rank, 16 GB/32 GB RDIMMs – TruDDR4 2933, single-rank or dual-rank, 8 GB/16 GB/32 GB/64 GB RDIMMs • Slots: 12 slots **Note:** Operating speed and total memory capacity depend on the processor model and UEFI settings. For a list of supported memory, see: http://www.lenovo.com/us/en/serverproven/

Table 1. Server specifications (continued)

Specification	Description
Internal drives	Drives supported by your server vary by model. • Up to four 3.5-inch hot-swap SAS/SATA drives • Up to four 3.5-inch simple-swap SATA drives • Up to eight 2.5-inch hot-swap SAS/SATA drives • Up to two M.2 drives
PCIe slots	Depending on the server model, your server supports up to three PCIe slots. For more information about the PCIe slots, see “Rear view” on page 17.
Input/Output (I/O) features	• Front panel: – One VGA connector* – One XClarity Controller USB connector – One USB 3.0 connector • Rear panel: – One VGA connector – Two USB 3.0 connectors – Two Ethernet connectors (RJ-45) – One XClarity Controller network connector – Two Ethernet connectors on the LOM adapter* – One serial port* * Available on some models
RAID adapters (depending on the model)	• A RAID 530-8i SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 10, and 50 • A RAID 730-8i 1G Cache SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 10, and 50 • A RAID 730-8i 2G Flash SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 6, 10, 50, and 60 • A RAID 930-8i or 930-16i SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 6, 10, 50, and 60 • A RAID 930-8e SAS/SATA adapter that supports JBOD mode and RAID levels 0, 1, 5, 6, 10, 50, and 60 **Notes:** • RAID 730-8i 1G Cache SAS/SATA adapter is not available for North America. • RAID 530-8i SAS/SATA adapter cannot be mixed with RAID 730-8i 1G Cache SAS/SATA adapter. • RAID 730-8i 2G Flash SAS/SATA adapter cannot be mixed with RAID 730-8i 1G Cache SAS/SATA adapter or RAID 930- 8i SAS/SATA adapter. • A RAID super capacitor module must be installed if the RAID 930-8i or 930-16i SAS/SATA adapter, RAID 930-8e SAS/SATA adapter, or RAID 730-8i 2G Flash SAS/SATA adapter is installed.

Table 1. Server specifications (continued)

Specification	Description
System fans	• One processor: four system fans • Two processors: six system fans **Note:** If your server is installed with one processor, four system fans (fan 1 to fan 4) are adequate to provide proper cooling. However, you must keep the locations for fan 5 and fan 6 occupied by fan fillers to ensure proper airflow.
Power supplies	Up to two hot-swap power supplies for redundancy support. • 550-watt ac 80 PLUS Platinum • 750-watt ac 80 PLUS Platinum • 750-watt ac 80 PLUS Titanium
Acoustical noise emissions	• Sound power levels, idle – 4.5 bels, minimum – 4.6 bels, typical – 5.2 bels, maximum • Sound power levels, operating – 5.0 bels, minimum – 5.1 bels, typical – 5.5 bels, maximum **Notes:** • These sound power levels are measured in controlled acoustical environments according to procedures specified by ISO 7779 and are reported in accordance with ISO 9296. • The declared acoustic noise levels are based on specified configurations, which may change slightly depending on configuration/conditions.
Electrical input	• Sine-wave input (50–60 Hz) required • Input voltage low range – Minimum: 100 V ac – Maximum: 127 V ac • Input voltage high range: – Minimum: 200 V ac – Maximum: 240 V ac **Note:** For server models with 750-watt ac 80 PLUS Titanium power supplies, the 100–127 V ac input voltage is not supported. **CAUTION:** • **240 V dc input (input range: 180-300 V dc) is supported in Chinese Mainland ONLY. Power supply with 240 V dc input cannot support hot plugging power cord function. Before removing the power supply with dc input, please turn off server or disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the power cord.** • **In order for the ThinkSystem products to operate error free in both a DC or AC electrical environment, a TN-S earthing system which complies to 60364-1 IEC 2005 standard has to be present or installed.**

Table 1. Server specifications (continued)

Specification	Description
Minimal configuration for debugging	• One processor in processor socket 1 • One DIMM in slot 3 • One power supply • One HDD or M.2 (If OS installation is needed for debugging) • Four system fans (fan 1 to fan 4)
Environment	The server is supported in the following environment: • Air temperature: – Operating: – ASHRAE class A2: 10–35°C (50–95°F); when the altitude exceeds 900 m (2953 ft), the maximum ambient temperature value decreases by 1°C (1.8°F) with every 300 m (984 ft) of altitude increase. – ASHRAE class A3: 5–40°C (41–104°F); when the altitude exceeds 900 m (2953 ft), the maximum ambient temperature value decreases by 1°C (1.8°F) with every 175 m (574 ft) of altitude increase. – ASHRAE class A4: 5–45°C (41–113°F); when the altitude exceeds 900 m (2953 ft), the maximum ambient temperature value decreases by 1°C (1.8°F) with every 125 m (410 ft) of altitude increase. – Server off: 5–45°C (41–113°F) – Shipping or storage: -40–60°C (-40–140°F) • Maximum altitude: 3050 m (10 000 ft) • Relative humidity (non-condensing): – Operating: – ASHRAE class A2: 8%–80%; maximum dew point: 21°C (70°F) – ASHRAE class A3: 8%–85%; maximum dew point: 24°C (75°F) – ASHRAE class A4: 8%–90%; maximum dew point: 24°C (75°F) – Shipping or storage: 8%–90% • Particulate contamination **Attention:** Airborne particulates and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the server. For information about the limits for particulates and gases, see “Particulate contamination” on page 168. **Notes:** Your server complies with ASHRAE class A2 specifications. The server performance might be impacted when the operating temperature is outside the ASHRAE A2 specifications. Depending on the hardware configuration, some server models comply with ASHRAE class A3 and class A4 specifications. To comply with ASHRAE class A3 and class A4 specifications, the server models must meet the following hardware configuration requirements at the same time: • Two power supplies must be installed. • No system fan fails.

Important information about EU ecodesign requirements

To meet the EU ecodesign requirements for energy-related products (ErP) Lot 9, your server must meet the following requirements:

- Minimum memory: 16 GB
- For server configured with one processor, these processors are not supported: Intel Xeon 3104, 3106, 3204, 4108, 4109T, 4110, 4112, 5122, 5222, 8156, and 8256.

Firmware updates

Several options are available to update the firmware for the server.

You can use the tools listed here to update the most current firmware for your server and the devices that are installed in the server.

Note: Lenovo typically releases firmware in bundles called UpdateXpress System Packs (UXSPs). To ensure that all of the firmware updates are compatible, you should update all firmware at the same time. If you are updating firmware for both the Lenovo XClarity Controller and UEFI, update the firmware for Lenovo XClarity Controller first.

Best practices related to updating firmware is available at the following location:

http://lenovopress.com/LP0656

Important terminology

- **In-band update**. The installation or update is performed using a tool or application within an operating system that is executing on the server's core CPU.
- **Out-of-band update**. The installation or update is performed by the Lenovo XClarity Controller collecting the update and then directing the update to the target subsystem or device. Out-of-band updates have no dependency on an operating system executing on the core CPU. However, most out-of-band operations do require the server to be in the S0 (Working) power state.
- **On-Target update.** The installation or update is initiated from an Operating System executing on the server's operating system.
- **Off-Target update.** The installation or update is initiated from a computing device interacting directly with the server's Lenovo XClarity Controller.
- **UpdateXpress System Packs (UXSPs)**. UXSPs are bundled updates designed and tested to provide the interdependent level of functionality, performance, and compatibility. UXSPs are server machine-type specific and are built (with firmware and device driver updates) to support specific Windows Server, Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) operating system distributions. Machine-type-specific firmware-only UXSPs are also available.

See the following table to determine the best Lenovo tool to use for installing and setting up the firmware:

Note: The server UEFI settings for option ROM must be set to **Auto** or **UEFI** to update firmware using Lenovo XClarity Administrator or Lenovo XClarity Essentials. For more information, see the following Tech Tip:

https://datacentersupport.lenovo.com/us/en/solutions/ht506118

Tool	In-band update	Out-of-band update	On-target update	Off-target update	Graphical user interface	Command-line interface	Supports UXSPs
Lenovo XClarity Provisioning Manager Limited to core system firmware only.	√			√	√		√
Lenovo XClarity Controller Supports core system firmware and most advanced I/O option firmware updates		√		√	√	√	
Lenovo XClarity Essentials OneCLI Supports all core system firmware, I/O firmware, and installed operating system driver updates	√	√				√	√
Lenovo XClarity Essentials UpdateXpress Supports all core system firmware, I/O firmware, and installed operating system driver updates	√	√			√		√
Lenovo XClarity Essentials Bootable Media Creator Supports core system firmware and I/O firmware updates. You can update the Microsoft Windows operating system, but device drivers are not included on the bootable image	√				√	√	√
Lenovo XClarity Administrator Supports core system firmware and I/O firmware updates	√	√		√	√		

The latest firmware can be found at the following site:

http://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr530/7X07/downloads

- **Lenovo XClarity Provisioning Manager**

  From Lenovo XClarity Provisioning Manager, you can update the Lenovo XClarity Controller firmware, the UEFI firmware, and the Lenovo XClarity Provisioning Manager software.

Note: By default, the Lenovo XClarity Provisioning Manager Graphical User Interface is displayed when you press F1. If you have changed that default to be the text-based system setup, you can bring up the Graphical User Interface from the text-based system setup interface.

Additional information about using Lenovo XClarity Provisioning Manager to update firmware is available at:

http://sysmgt.lenovofiles.com/help/topic/LXPM/platform_update.html

- **Lenovo XClarity Controller**

  If you need to install a specific update, you can use the Lenovo XClarity Controller interface for a specific server.

  Notes:

  – To perform an in-band update through Windows or Linux, the operating system driver must be installed and the Ethernet-over-USB (sometimes called LAN over USB) interface must be enabled.

    Additional information about configuring Ethernet over USB is available at:

    http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_configuringUSB.html

  – If you update firmware through the Lenovo XClarity Controller, make sure that you have downloaded and installed the latest device drivers for the operating system that is running on the server.

  Specific details about updating firmware using Lenovo XClarity Controller are available at:

  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_manageserverfirmware.html

- **Lenovo XClarity Essentials OneCLI**

  Lenovo XClarity Essentials OneCLI is a collection of command line applications that can be used to manage Lenovo servers.Its update application can be used to update firmware and device drivers for your servers. The update can be performed within the host operating system of the server (in-band) or remotely through the BMC of the server (out-of-band).

  Specific details about updating firmware using Lenovo XClarity Essentials OneCLI is available at:

  http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_c_update.html

- **Lenovo XClarity Essentials UpdateXpress**

  Lenovo XClarity Essentials UpdateXpress provides most of OneCLI update functions through a graphical user interface (GUI). It can be used to acquire and deploy UpdateXpress System Pack (UXSP) update packages and individual updates. UpdateXpress System Packs contain firmware and device driver updates for Microsoft Windows and for Linux.

  You can obtain Lenovo XClarity Essentials UpdateXpress from the following location:

  https://datacentersupport.lenovo.com/solutions/lnvo-xpress

- **Lenovo XClarity Essentials Bootable Media Creator**

  You can use Lenovo XClarity Essentials Bootable Media Creator to create bootable media that is suitable for applying firmware updates, running preboot diagnostics, and deploying Microsoft Windows operating systems.

  You can obtain Lenovo XClarity Essentials BoMC from the following location:

  https://datacentersupport.lenovo.com/solutions/lnvo-bomc

- **Lenovo XClarity Administrator**

If you are managing multiple servers using the Lenovo XClarity Administrator, you can update firmware for all managed servers through that interface. Firmware management is simplified by assigning firmware-compliance policies to managed endpoints. When you create and assign a compliance policy to managed endpoints, Lenovo XClarity Administrator monitors changes to the inventory for those endpoints and flags any endpoints that are out of compliance.

Specific details about updating firmware using Lenovo XClarity Administrator are available at:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/update_fw.html

Configuring the LAN over USB interface manually

To perform a firmware update through the operating system using Lenovo XClarity Essentials OneCLI, the Lenovo XClarity Controller must be configured to use the LAN over USB interface. The firmware update package attempts to perform the setup automatically, if needed. If the automatic setup fails or if you prefer to set up the LAN over USB manually, use one of the following procedures.

Additional information about using the Lenovo XClarity Controller to enable LAN over USB is available at:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_configuringUSB.html

Installing the LAN over USB Windows device driver

When you install a Windows operating system, there might be an unknown RNDIS device in the Device Manager. Lenovo provides a Windows INF file that identifies this device.

Complete the following steps to install `ibm_rndis_server_os.inf`:

Note: You only have to perform these steps if the compute node is running a Windows operating system and the `ibm_rndis_server_os.inf` file has not been previously installed. The file only has to be installed once. It is required by Windows operating systems to detect and use the LAN over USB functionality.

Step 1. Click **Administrative Tools → Computer Management → Device Manager** and find the RNDIS Device. Click **Properties → Driver → Reinstall driver**. Point the server to the `\Windows\inf` directory where it can find the `ibm_rndis_server_os.inf` file and install the device.

Step 2. Click **Administrative Tools → Device Manager**. Right-click **Network adapters** and select **Scan for hardware changes**. A small pop-up confirms that the Ethernet device is found and installed. The New Hardware Wizard starts automatically.

Step 3. When you are prompted `Can Windows connect to Windows Update to search for software?`, select **No, not this time**. Click **Next** to continue.

Step 4. When you are prompted `What do you want the wizard to do?`, select **Install from a list or specific location (Advanced)**. Click **Next** to continue.

Step 5. When you are prompted `Please choose your search and installation options`, select **Don't search. I will choose the driver to install**. Click **Next** to continue.

Step 6. When you are prompted `Select a hardware type, and then click Next`, select **Network adapters**. Click **Next** to continue.

Step 7. When you are prompted with the statement `Completing the Found New Hardware Wizard`, click **Finish**. A new local area connection appears. If the message `This connection has limited or no connectivity` is displayed, ignore this message.

Step 8. Return to the Device Manager. **Lenovo USB Remote NDIS Network Device** appears under **Network Adapters**.

Step 9. Use the Lenovo XClarity Controller interface to view or set the IP address for the LAN adapter.

Additional information about using the Lenovo XClarity Controller to configure LAN over USB is available at:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_configuringUSB.html

Tech Tips

Lenovo continually updates the support Web site with the latest tips and techniques that you can use to solve issues that you might have with your server. These Tech Tips (also called retain tips or service bulletins) provide procedures to work around issues related to the operation of your server.

To find the Tech Tips available for your server:

1. Go to http://datacentersupport.lenovo.com and navigate to the support page for your server.
2. Click **Documentation** from the navigation pane.

   Follow the on-screen instructions to choose the category for the problem that you are having.

Security advisories

Lenovo is committed to developing products and services that adhere to the highest security standards in order to protect our customers and their data. When potential vulnerabilities are reported, it is the responsibility of the Lenovo Product Security Incident Response Team (PSIRT) to investigate and provide information to our customers so they may put mitigation plans in place as we work toward providing solutions.

The list of current advisories is available at the following location:
https://datacentersupport.lenovo.com/product_security/home

Power on the server

After the server performs a short self-test (power status LED flashes quickly) when connected to input power, it enters a standby state (power status LED flashes once per second).

The server can be turned on (power status LED on) in any of the following ways:

- You can press the power button.
- The server can restart automatically after a power interruption.
- The server can respond to remote power-on requests sent to the Lenovo XClarity Controller.

For information about powering off the server, see “Power off the server” on page 11.

Power off the server

The server remains in a standby state when it is connected to a power source, allowing the Lenovo XClarity Controller to respond to remote power-on requests. To remove all power from the server (power status LED off), you must disconnect all power cables.

To place the server in a standby state (power status LED flashes once per second):

Note: The Lenovo XClarity Controller can place the server in a standby state as an automatic response to a critical system failure.

- Start an orderly shutdown using the operating system (if supported by your operating system).
- Press the power button to start an orderly shutdown (if supported by your operating system).

- Press and hold the power button for more than 4 seconds to force a shutdown.

When in a standby state, the server can respond to remote power-on requests sent to the Lenovo XClarity Controller. For information about powering on the server, see “Power on the server” on page 11.

Chapter 2. Server components

Use the information in this section to learn about each of the components associated with your server.

Front view

The front view of the server varies by the model.

- Front view of server models with 3.5-inch drive bays
- Front view of server models with 2.5-inch drive bays

The following illustrations show the front views of server models with hot-swap drives. Depending on the model, your server might look slightly different the illustrations.

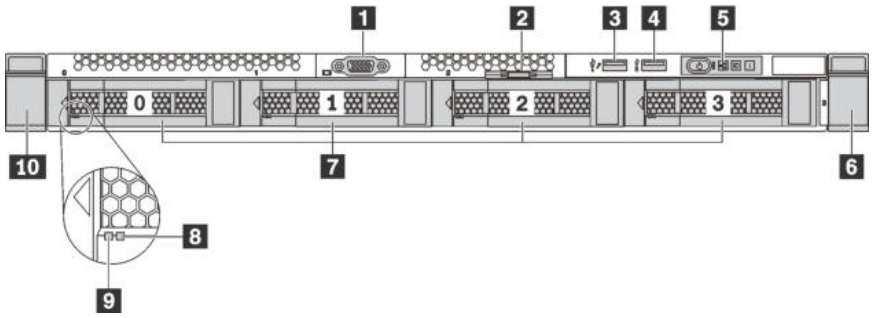


Figure 4. Front view of server models with 3.5-inch drive bays

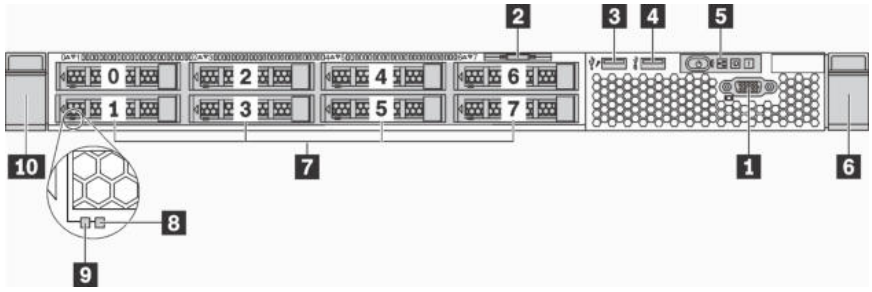


Figure 5. Front view of server models with 2.5-inch drive bays

Table 2. Components on the front of the server

Callout	Callout
1 VGA connector (available on some model)	2 Pull-out information tab
3 XClarity Controller USB connector	4 USB 3.0 connector
5 Operator information panel	6 Rack latch (right)
7 Drive bays	8 Drive status LED (yellow)
9 Drive activity LED (green)	10 Rack latch (left)

1 VGA connector (available on some models)

© Copyright Lenovo 2017, 2020

Used to attach a high-performance monitor, a direct-drive monitor, or other devices that use a VGA connector.

2 Pull-out information tab

The Lenovo XClarity Controller network access label is attached on the pull-out information tab.

3 XClarity Controller USB connector

Depending on the setting, this connector supports USB 2.0 function, XClarity Controller management function, or both.

- If the connector is set for USB 2.0 function, you can attach a device that requires a USB 2.0 connection, such as a keyboard, a mouse, or a USB storage device.
- If the connector is set for XClarity Controller management function, you can attach a mobile device installed with the application to run XClarity Controller event logs.
- If the connector is set to have both functions, you can press the ID button for three seconds to switch between the two functions.

4 USB 3.0 connector

Attach a USB-compatible device, such as a USB keyboard, USB mouse, or USB storage device.

5 Operator information panel

For information about the controls and status LEDs on the operator information panel, see “Operator information panel” on page 15.

6 10 Rack latches

If your server is installed in a rack, you can use the rack latches to help you slide the server out of the rack. You also can use the latches and screws to secure the server in the rack so that the server cannot slide out, especially in vibration-prone areas. For more information, refer to the *Rack Installation Guide* that comes with your rail kit.

7 Drive bays

The number of the installed drives in your server varies by model. When you install drives, follow the order of the drive bay numbers.

The EMI integrity and cooling of the server are protected by having all drive bays occupied. The vacant drive bays must be occupied by drive fillers.

8 Drive status LED

9 Drive activity LED

Each hot-swap drive has two LEDs.

Drive LED	Status	Description
8 Drive status LED (right)	Solid yellow	The drive has an error.
	Blinking yellow (blinking slowly, about one flash per second)	The drive is being rebuilt.
	Blinking yellow (blinking rapidly, about four flashes per second)	The RAID controller is locating the drive.
9 Drive activity LED (left)	Solid green	The drive is powered but not active.
	Blinking green	The drive is active.

Operator information panel

The operator information panel of the server provides controls and LEDs.

The following illustration shows the operator information panel of the server.

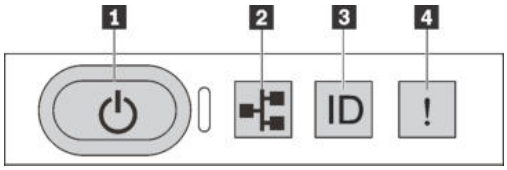


Figure 6. Operator information panel

Table 3. Components on the operator information panel

Callout	Callout
1 Power button with power status	2 Network activity
3 System ID button with ID	4 System error

1 Power button with power status

You can press the power button to power on the server when you finish setting up the server. You also can hold the power button for several seconds to power off the server if you cannot shut down the server from the operating system. The power status helps you to determine the current power status.

Status	Color	Description
Solid on	Green	The server is on and running.
Slow blinking (about one flash per second)	Green	The server is off and is ready to be powered on (standby state).
Fast blinking (about four flashes per second)	Green	The server is off, but the XClarity Controller is initializing, and the server is not ready to be powered on.
Off	None	There is no ac power applied to the server.

2 Network activity LED

Compatibility of the NIC adapter and the network activity LED.

NIC adapter	Network activity LED
LOM adapter	Support
ML2 NIC adapter	Support
PCIe NIC adapter	Not support

The network activity LED on the operator information panel helps you identify the network connectivity and activity.

Status	Color	Description
On	Green	The server is connected to a network.
Blinking	Green	The network is connected and active.
Off	None	The server is disconnected from the network.

3 System ID button with ID LED

Use this system ID button and the blue system ID LED to visually locate the server. A system ID LED is also located on the rear of the server. Each time you press the system ID button, the state of both the system ID LEDs changes. The LEDs can be changed to on, blinking, or off. You can also use the Lenovo XClarity Controller or a remote management program to change the state of the system ID LEDs to assist in visually locating the server among other servers.

If the XClarity Controller USB connector is set to have both the USB 2.0 function and XClarity Controller management function, you can press the ID button for three seconds to switch between the two functions.

4 System error LED

Status	Color	Description	Action
On	Yellow	An error has been detected on the server. Causes might include but not limited to the following errors: • The temperature of the server reached the non-critical temperature threshold. • The voltage of the server reached the non-critical voltage threshold. • A fan has been detected to be running at low speed. • A fan has been removed. • The power supply has a critical error. • The power supply is not connected to the power.	Check the event log to determine the exact cause of the error. For information about troubleshooting, see “Troubleshooting by symptom” on page 148 .
Off	None	The server is off or the server is on and is working correctly.	None.

Rear view

The rear of the server provides access to several components, including the power supplies, PCIe adapters, serial port, and Ethernet connectors.

- “Rear view of server models with three PCIe slots” on page 17
- “Rear view of server models with two PCIe slots” on page 19

Rear view of server models with three PCIe slots

The following illustration shows the rear view of server models with three PCIe slots. Depending on the model, your server might look slightly different from the illustrations in this topic.

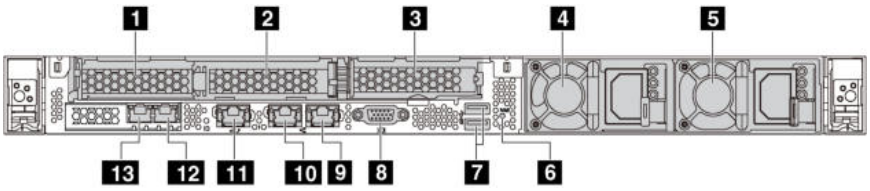


Figure 7. Rear view of server models with three PCIe slots

Table 4. Connectors on the rear of the server

Callout	Callout
1 PCIe slot 1 on riser 1 assembly	2 PCIe slot 2 on riser 1 assembly
3 PCIe slot 3 on riser 2 assembly	4 Power supply 1
5 Power supply 2 (available on some models)	6 NMI button
7 USB 3.0 connectors	8 VGA connector
9 Ethernet connector 2 (RJ-45)	10 Ethernet connector 1 (RJ-45)
11 XClarity Controller network connector	12 Ethernet connector 2 on the LOM adapter (available on some models)
13 Ethernet connector 1 on the LOM adapter (available on some models)	

1 2 PCIe slots on riser 1 assembly

Your server supports two types of riser cards for riser 1 assembly.

- Type 1
  - Slot 1: PCIe x16 (x8, x4, x1), low-profile
  - Slot 2: PCIe x16 (x16, x8, x4, x1), low-profile
- Type 2
  - Slot 1: PCIe x16 (x8, x4, x1), low-profile
  - Slot 2: ML2 x8 (x8, x4, x1), low-profile

3 PCIe slot on riser 2 assembly

Your server supports two types of riser cards for riser 2 assembly.

- Type 1: PCIe x16 (x8, x4, x1), low-profile

- Type 2: PCIe x16 (x16, x8, x4, x1), low-profile

  Note: Type 2 is supported only when two processors are installed.

4 Power supply 1

5 Power supply 2 (available on some models)

The hot-swap redundant power supplies help you avoid significant interruption to the operation of the system when a power supply fails. You can purchase a power supply option from Lenovo and install the power supply to provide power redundancy without turning off the server.

On each power supply, there are three status LEDs near the power cord connector. For information about the LEDs, see “Rear view LEDs” on page 21.

6 NMI button

Press this button to force a nonmaskable interrupt (NMI) to the processor. By this way, you can blue screen the server and take a memory dump. You might have to use a pen or the end of a straightened paper clip to press the button.

7 USB 3.0 connectors (2)

Attach a USB-compatible device, such as a USB keyboard, USB mouse, or USB storage device.

8 VGA connector

Used to attach a high-performance monitor, a direct-drive monitor, or other devices that use a VGA connector.

9 Ethernet connector 2

10 Ethernet connector 1

Used to attach an Ethernet cable for a LAN. Each Ethernet connector has two status LEDs to help you identify the Ethernet connectivity and activity. For information about the LEDs, see “Rear view LEDs” on page 21.

Ethernet connector 1 can be set as XClarity Controller network connector. To set Ethernet connector 1 as XClarity Controller network connector, start Setup utility, go to **BMC Settings → Network Settings → Network Interface Port** and select **Shared**. Then, go to **Shared NIC on** and select **Onboard Port 1**.

11 XClarity Controller network connector

Used to attach an Ethernet cable to manage the system using XClarity Controller.

12 Ethernet connector 2 on the LOM adapter

13 Ethernet connector 1 on the LOM adapter

The LOM adapter provides two extra Ethernet connectors for network connections.

Ethernet connector 1 on the LOM adapter can be set as XClarity Controller network connector. To set the Ethernet connector as XClarity Controller network connector, start Setup utility, go to **BMC Settings → Network Settings → Network Interface Port** and select **Shared**. Then, go to **Shared NIC on** and select **PHY Card**.

Rear view of server models with two PCIe slots

The following illustrations show the rear view of the server models with two PCIe slots. Depending on the model, your server might look slightly different from the illustrations in this topic.

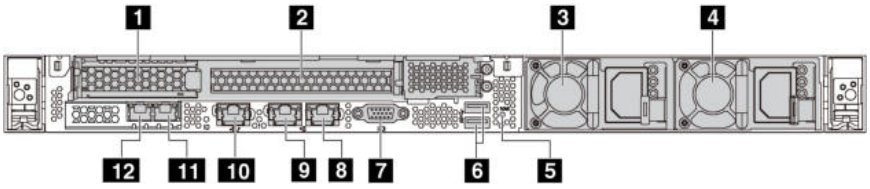


Figure 8. Rear view of server models with two PCIe slots

Table 5. Connectors on the rear of the server

Callout	Callout
1 PCIe slot 1 on riser 1 assembly	2 PCIe slot 2 on riser 1 assembly
3 Power supply 1	4 Power supply 2 (available on some models)
5 NMI button	6 USB 3.0 connectors
7 VGA connector	8 Ethernet connector 2 (RJ-45)
9 Ethernet connector 1 (RJ-45)	10 XClarity Controller network connector
11 Ethernet connector 2 on the LOM adapter (available on some models)	12 Ethernet connector 1 on the LOM adapter (available on some models)

1 2 PCIe slots on riser 1 assembly

Your server supports two types of riser cards for riser 1 assembly.

- Type 1
  - Slot 1: PCIe x16 (x8, x4, x1), low-profile
  - Slot 2: PCIe x16 (x16, x8, x4, x1), full-height, half-length
- Type 2
  - Slot 1: PCIe x16 (x8, x4, x1), low-profile
  - Slot 2: ML2 x8 (x8, x4, x1), low-profile adapter with full-height bracket

3 Power supply 1

4 Power supply 2 (available on some models)

The hot-swap redundant power supplies help you avoid significant interruption to the operation of the system when a power supply fails. You can purchase a power supply option from Lenovo and install the power supply to provide power redundancy without turning off the server.

On each power supply, there are three status LEDs near the power cord connector. For information about the LEDs, see “Rear view LEDs” on page 21.

5 NMI button

Press this button to force a nonmaskable interrupt (NMI) to the processor. By this way, you can blue screen the server and take a memory dump. You might have to use a pen or the end of a straightened paper clip to press the button.

6 USB 3.0 connectors (2)

Attach a USB-compatible device, such as a USB keyboard, USB mouse, or USB storage device.

7 VGA connector

Used to attach a high-performance monitor, a direct-drive monitor, or other devices that use a VGA connector.

8 Ethernet connector 2

9 Ethernet connector 1

Used to attach an Ethernet cable for a LAN. Each Ethernet connector has two status LEDs to help you identify the Ethernet connectivity and activity. For information about the LEDs, see “Rear view LEDs” on page 21.

Ethernet connector 1 can be set as XClarity Controller Network connector. To set Ethernet connector 1 as XClarity Controller Network connector, start Setup utility, go to **BMC Settings → Network Settings → Network Interface Port** and select **Shared**. Then, go to **Shared NIC on** and select **Onboard Port 1**.

10 XClarity Controller network connector

Used to attach an Ethernet cable to manage the system using XClarity Controller.

11 Ethernet connector 2 on the LOM adapter

12 Ethernet connector 1 on the LOM adapter

The LOM adapter provides two extra Ethernet connectors for network connections.

Ethernet connector 1 on the LOM adapter can be set as XClarity Controller Network connector. To set the Ethernet connector as XClarity Controller Network connector, start Setup utility, go to **BMC Settings → Network Settings → Network Interface Port** and select **Shared**. Then, go to **Shared NIC on** and select **PHY Card**.

Rear view LEDs

The rear of the server provides system ID LED, system error LED, network LEDs, and power supply LEDs.

The following illustration shows the LEDs on the rear view of server models with three PCIe slots. The LEDs on the rear view of server models with two PCIe slots are the same.

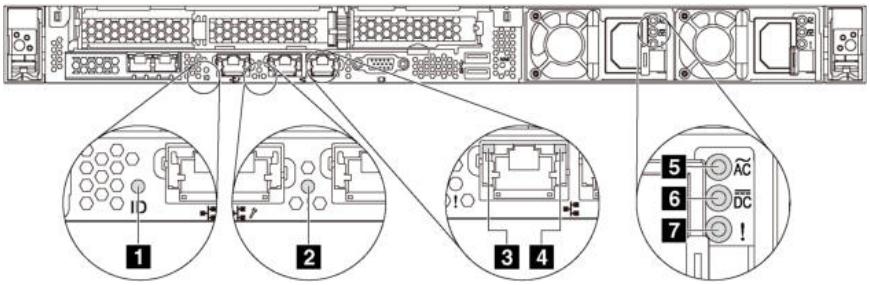


Figure 9. Rear view LEDs

Table 6. LEDs on the rear view of the server

Callout	Callout
1 System ID LED	2 System error LED
3 Ethernet link LED	4 Ethernet activity LED
5 Power input LED	6 Power output LED
7 Power supply error LED	

1 System ID LED

The blue system ID LED helps you to visually locate the server. A system ID LED is also located on the front of the server. Each time you press the system ID button, the state of both the system ID LEDs changes. The LEDs can be changed to on, blinking, or off. You can also use the Lenovo XClarity Controller or a remote management program to change the state of the system ID LEDs to assist in visually locating the server among other servers.

2 System error LED

The system error LED helps you to determine if there are any system errors. For details, see “System error LED” on page 16.

3 Ethernet link LED

4 Ethernet activity LED

Each Ethernet connector has two status LEDs.

Ethernet status LED	Color	Status	Description
3 Ethernet link LED	Green	On	Network link is established.
	None	Off	Network link is disconnected.
4 Ethernet activity LED	Green	Blinking	Network link is connected and active.
	None	Off	The server is disconnected from a LAN.

5 6 7 Power supply LEDs

Each hot-swap power supply has three status LEDs.

LED	Description
5 Power input LED	• Green: The power supply is connected to the ac power source. • Off: The power supply is disconnected from the ac power source.
6 Power output LED	• Green: The server is on and the power supply is working normally. • Blinking green: The power supply is in the zero-output mode (standby). When the server power load is low, one of the installed power supplies enters into the standby state while the other one delivers the entire load. When the power load increases, the standby power supply will switch to active state to provide sufficient power to the system. To disable zero-output mode, start the Setup utility, go to **System Settings → Power → Zero Output** and select **Disable**. If you disable the zero-out mode, both power supplies will be in the active state. • Off: The server is powered off, or the power supply is not working properly. If the server is powered on but the LED is off, replace the power supply.
7 Power supply error LED	• Yellow: The power supply has failed. To resolve the issue, replace the power supply. • Off: The power supply is working normally

System board components

The illustration in this section shows the component locations on the system board.

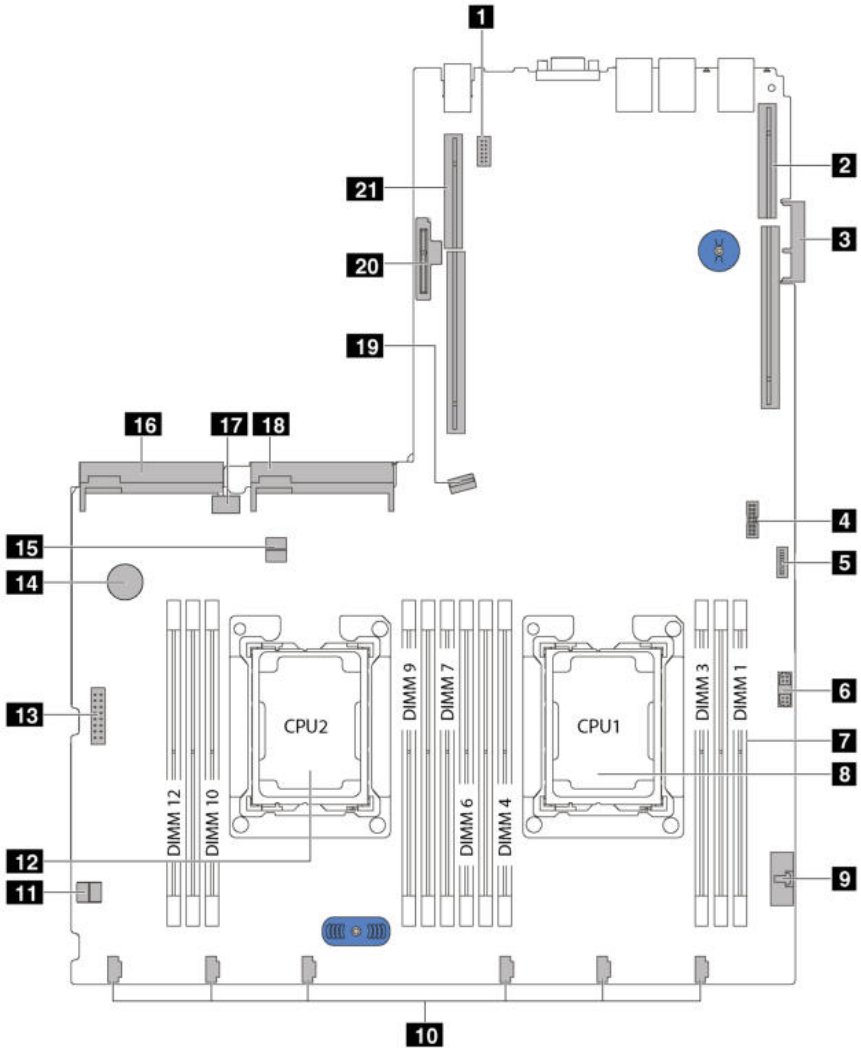


Figure 10. System board components

Callout	Callout
1 Serial-port-module connector	2 Riser 1 slot
3 LOM adapter connector	4 TCM[1]/TPM[2] connector (for Chinese Mainland only)
5 Front USB connector	6 Front VGA connector
7 DIMM slots	8 Processor 1 socket
9 Operator-information-panel connector	10 System fan connectors
11 Cable retainer	12 Processor 2 socket
13 Backplane power connector	14 CMOS battery
15 Cable retainer	16 Power supply 2 connector

Callout	Callout
17 Internal USB connector	18 Power supply 1 connector
19 SATA 0-3 connector	20 M.2 module slot
21 Riser 2 slot	

Notes:

- [1] Trusted Cryptography Module
- [2] Trusted Platform Module

System board switches and jumpers

The following illustration shows the location of the switches and jumpers on the server.

Note: If there is a clear protective sticker on the top of the switch blocks, you must remove and discard it to access the switches.

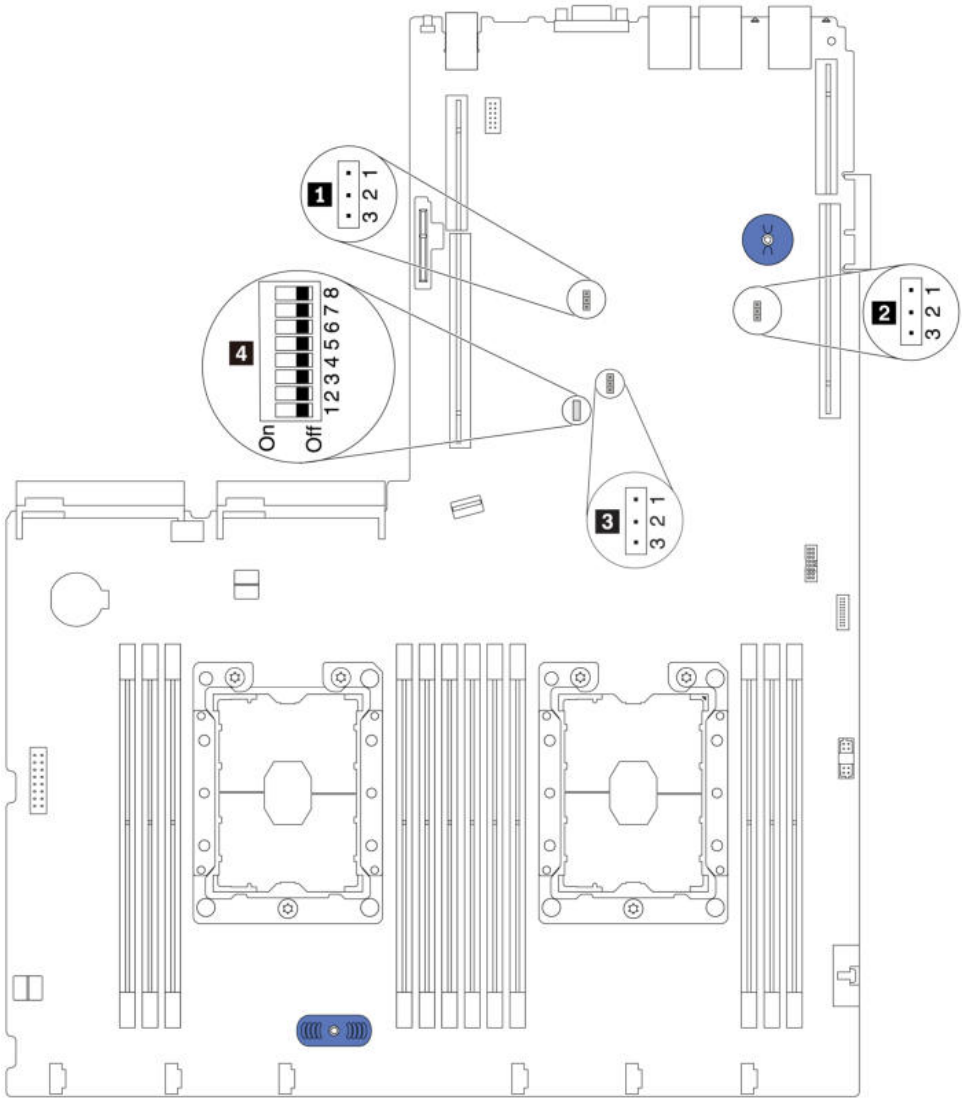


Figure 11. System-board switches and jumpers

Table 7. Jumpers and switches on the system board

Jumper/Switch name	Jumper/Switch number	Jumper/Switch setting
1 TPM/TCM physical presence jumper	JP6	• Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: TPM/TCM physical presence is asserted.
2 Clear CMOS jumper	JP3	• Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: Clear the real-time clock (RTC) registry.
3 ME firmware security override	JP8	• Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: Enable Flash security override. **Note:** For debug only.
4 SW6 switch block	SW6 (including switches 1, 2, 3, 4, 5, 6, 7, and 8)	All the switches are in the **Off** position by default. • Switches 1, 6, and 8: Reserved. • Switch 2: Override power-on password switch. Changing position of this switch overrides the power-on password. Changing position of this switch does not affect the administrator password.
4 Power permission	SW6 (switch 7)	The default position is Off. Changing this switch to the On position enables Power On.
4 Force XCC reset	SW6 (switch 4)	The default position is Off. Changing this switch to the On position resets the Lenovo XClarity Controller.
4 Force XCC update	SW6 (switch 3)	The default position is Off. Changing this switch to the On position forces the Lenovo XClarity Controller to update to the latest version.

Important:

- Before you move the switches and jumpers, turn off the server. Then, disconnect all power cords and external cables. Do not open your server or attempt any repair before reading and understanding the following information:
  - http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html
  - “Handling static-sensitive devices” on page 43
- Any system-board switch or jumper block that is not shown in the illustrations in this document are reserved.

System board LEDs

The following illustrations show the light-emitting diodes (LEDs) on the system board.

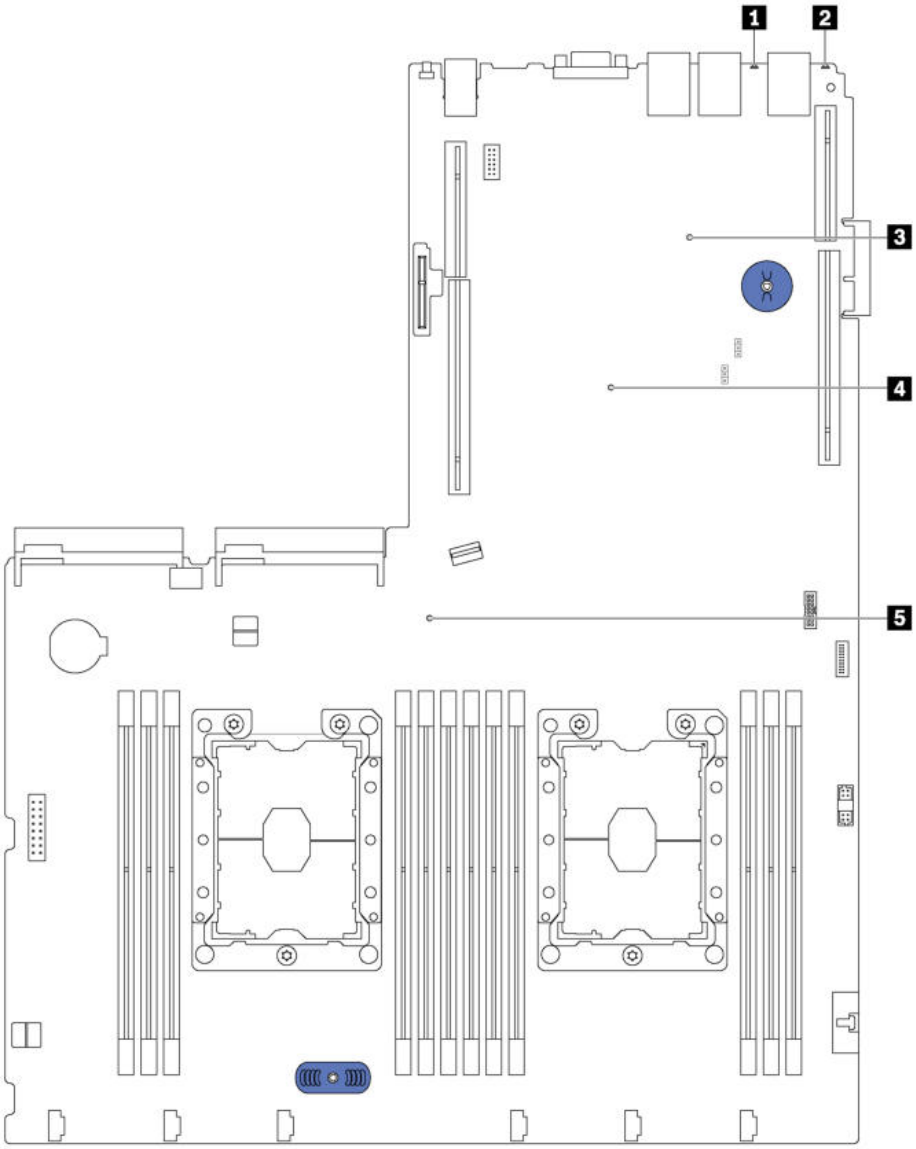


Figure 12. System board LEDs

Table 8. LEDs on the system board

Callout	Callout
1 System error LED	2 System ID LED
3 XClarity Controller heartbeat LED	4 Field-Programmable Gate Array (FPGA) error LED
5 System power LED	

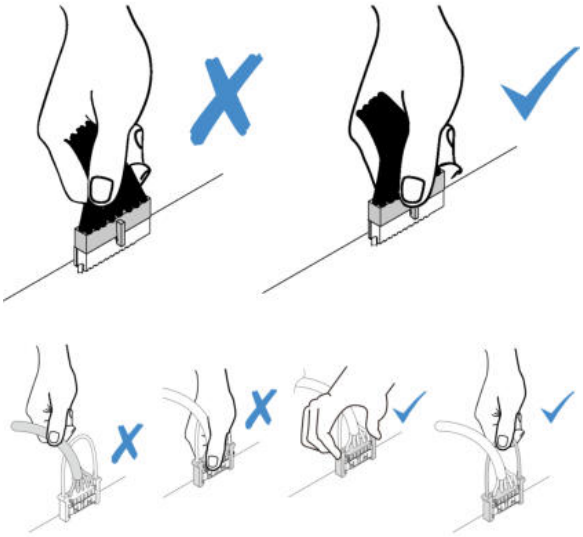
Internal cable routing

Some of the components in the server have internal cables and cable connectors.

To connect cables, observe the following guidelines:

- Power off the server before you connect or disconnect any internal cables.
- See the documentation that comes with any external devices for additional cabling instructions. It might be easier for you to route cables before you connect the devices to the server.
- Cable identifiers of some cables are printed on the cables that come with the server and optional devices. Use these identifiers to connect the cables to the correct connectors.
- Ensure that the relevant cables pass through the cable clips.

Note: Disengage all latches, release tabs, or locks on cable connectors when you disconnect cables from the system board. Failing to release them before removing the cables will damage the cable sockets on the system board, which are fragile. Any damage to the cable sockets might require replacing the system board.



VGA connector

Use this section to understand the cable routing for the video graphic adapter (VGA) connector.

Note: The VGA connector is available on some models.

Server models with 3.5-inch drive bays

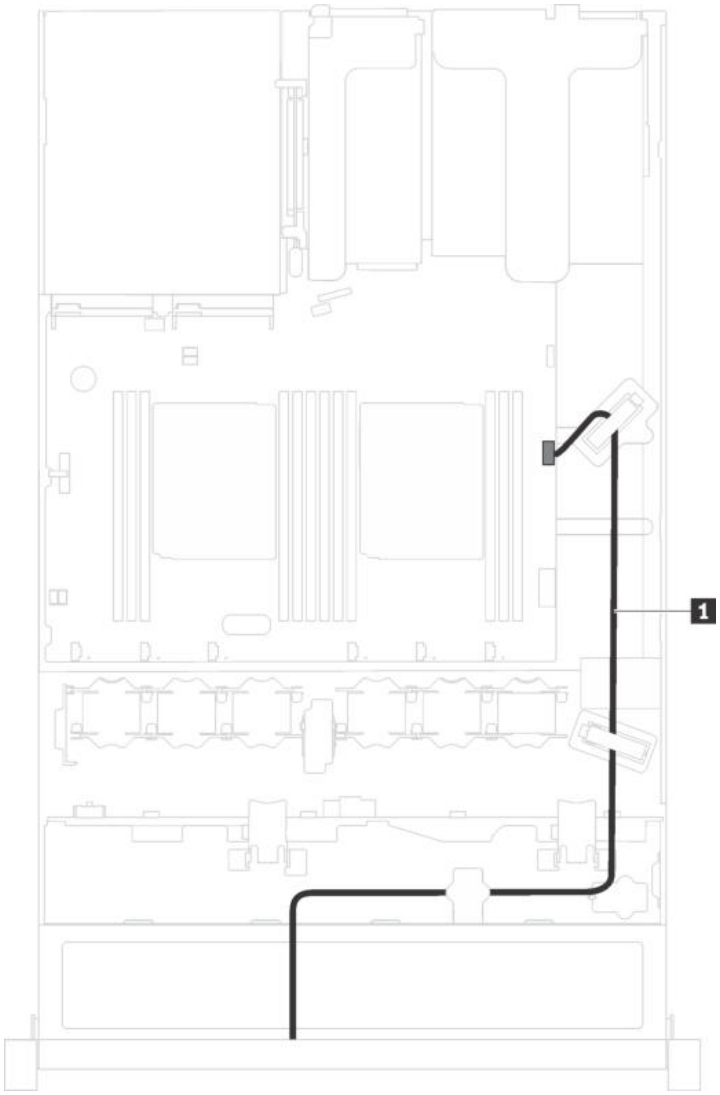


Figure 13. VGA connector cable routing

From	To
1 VGA cable	Front VGA connector on the system board

Server models with 2.5-inch drive bays

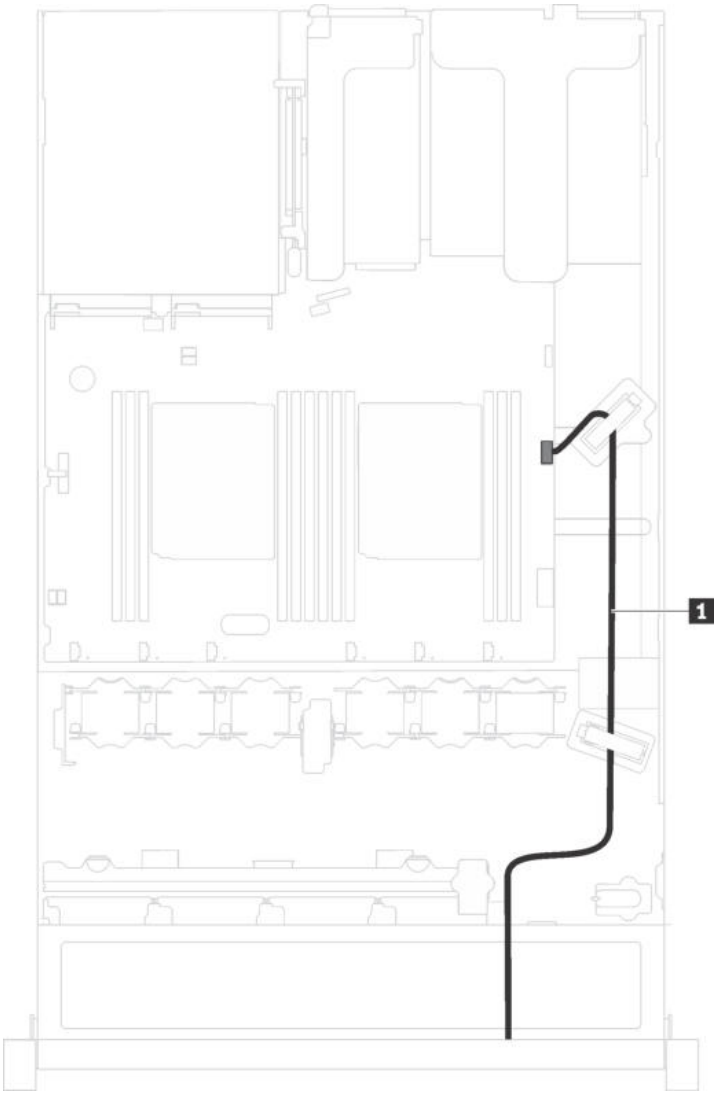


Figure 14. VGA connector cable routing

From	To
1 VGA cable	Front VGA connector on the system board

Front I/O assembly

Use this section to understand the cable routing for the front I/O assembly.

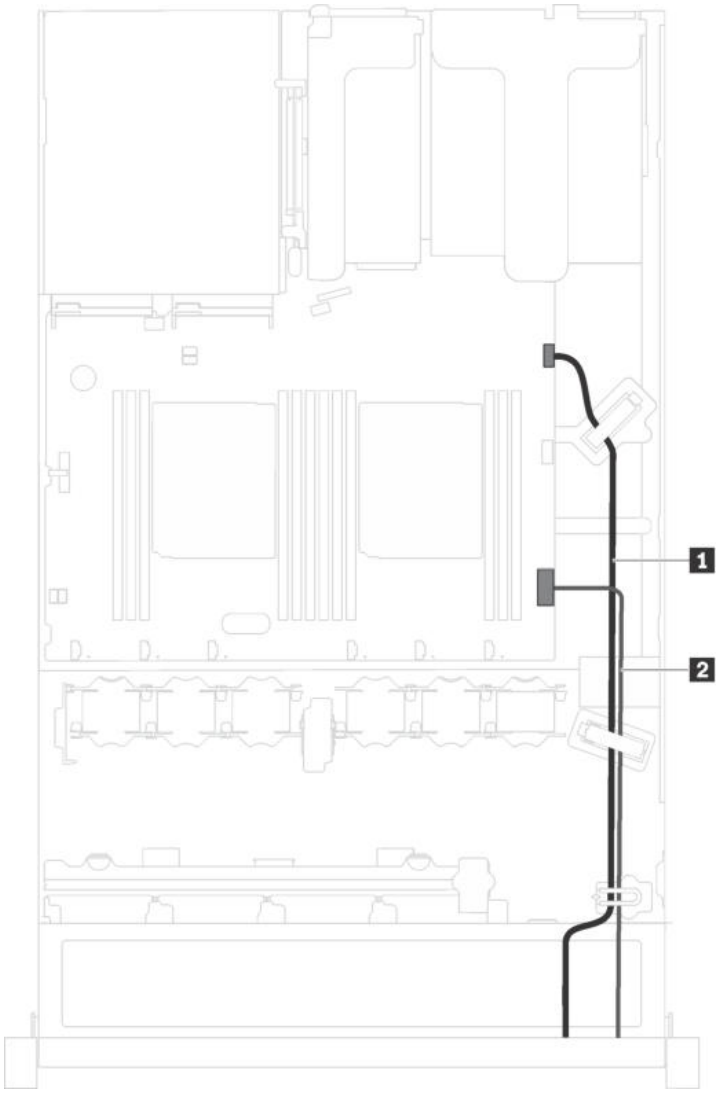


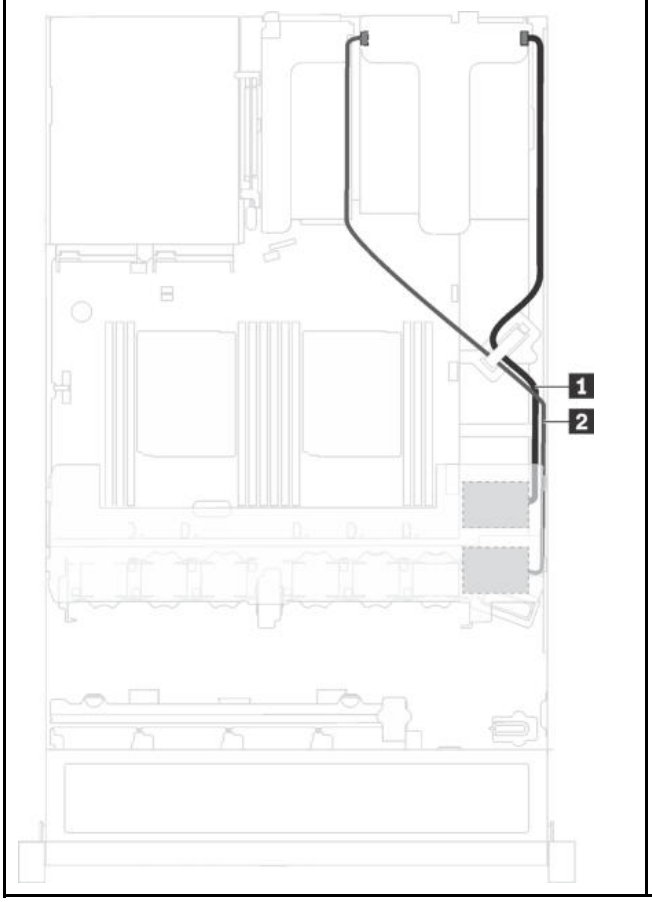
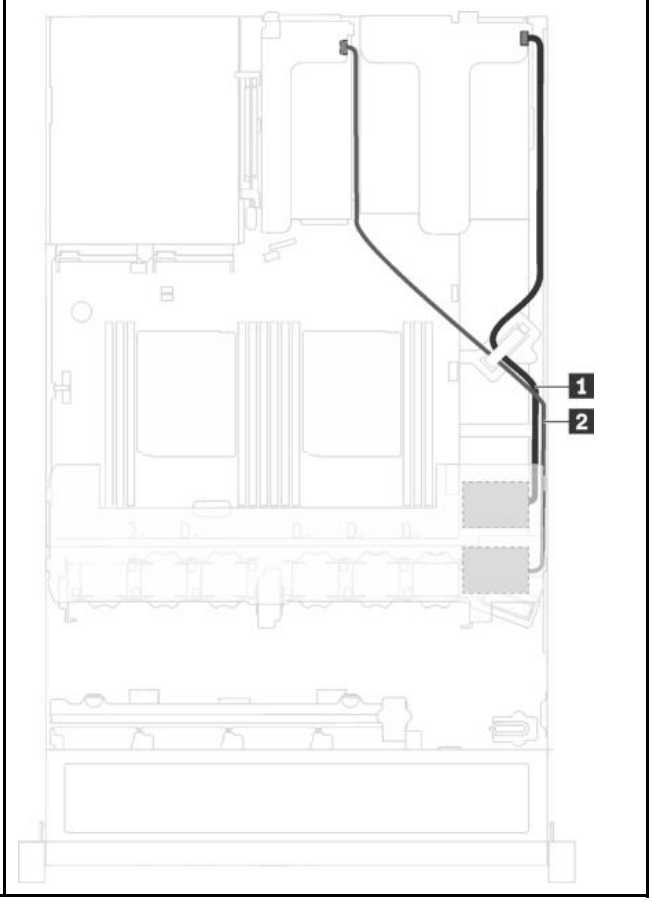
Figure 15. Cable routing for the front I/O assembly

From	To
1 Front USB cable	Front USB connector on the system board
2 Operator-information-panel cable	Operator-information-panel connector on the system board

RAID super capacitor module

Use this section to understand the cable routing for RAID super capacitor modules.

Your server supports up to two RAID super capacitor modules.

Scenario 1: the second RAID adapter in PCIe slot 2	Scenario 2: the second RAID adapter in PCIe slot 3
	

1 Cable routing for RAID super capacitor module 1

2 Cable routing for RAID super capacitor module 2

An extension cable is provided for each RAID super capacitor module for connection.

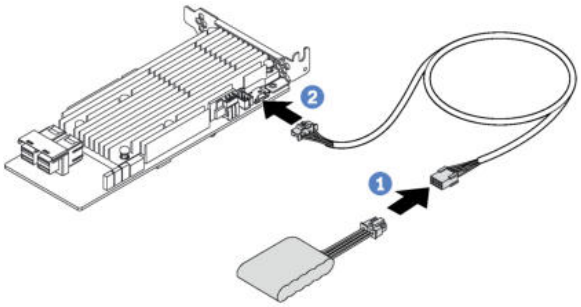


Figure 16. Connecting the RAID super capacitor module to the RAID adapter

Backplanes

Use this section to understand the cable routing for the backplanes.

Server model with eight 2.5-inch hot-swap drives

Use this section to understand the internal cable routing for the server model with eight 2.5-inch hot-swap drives.

The following illustration shows the cable routing for the server model with eight 2.5-inch hot-swap drives.

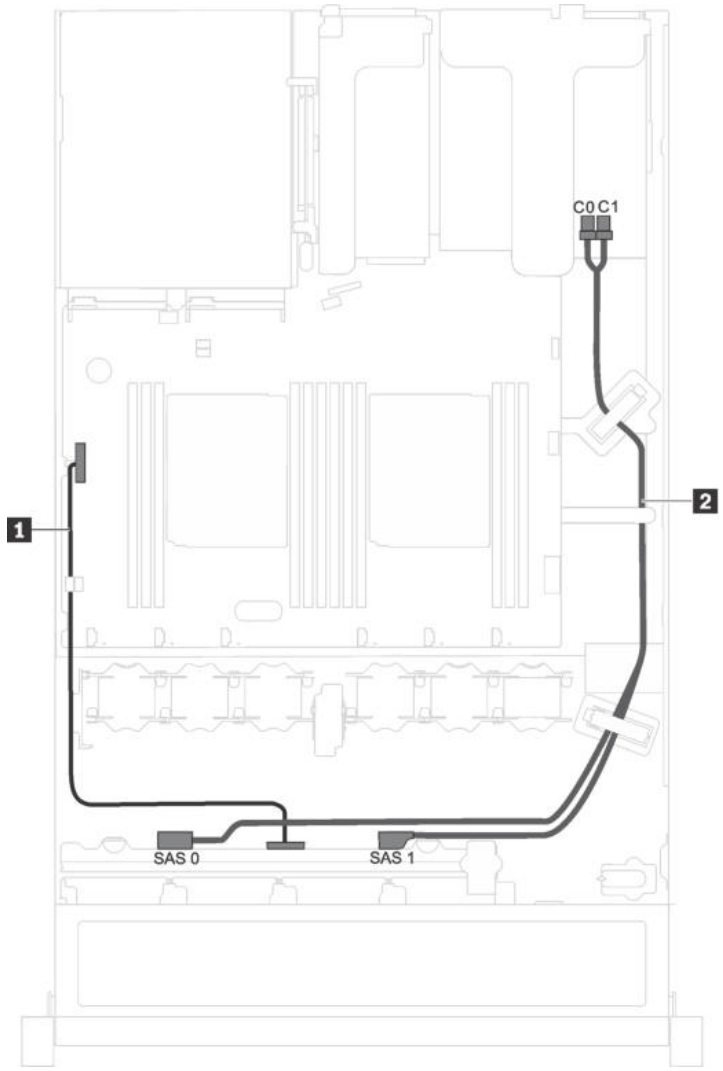


Figure 17. Cable routing for the server model with eight 2.5-inch hot-swap drives

Cable	From	To
1 Power cable	Power connector on the backplane	Backplane power connector on the system board
2 SAS signal cable	SAS 0 and SAS 1 connectors on the backplane	C0 and C1 connectors on the HBA/RAID adapter

Server model with four 3.5-inch hot-swap drives

Use this section to understand the internal cable routing for the server model with four 3.5-inch hot-swap drives.

The following illustration shows the cable routing for the server model with four 3.5-inch hot-swap drives.

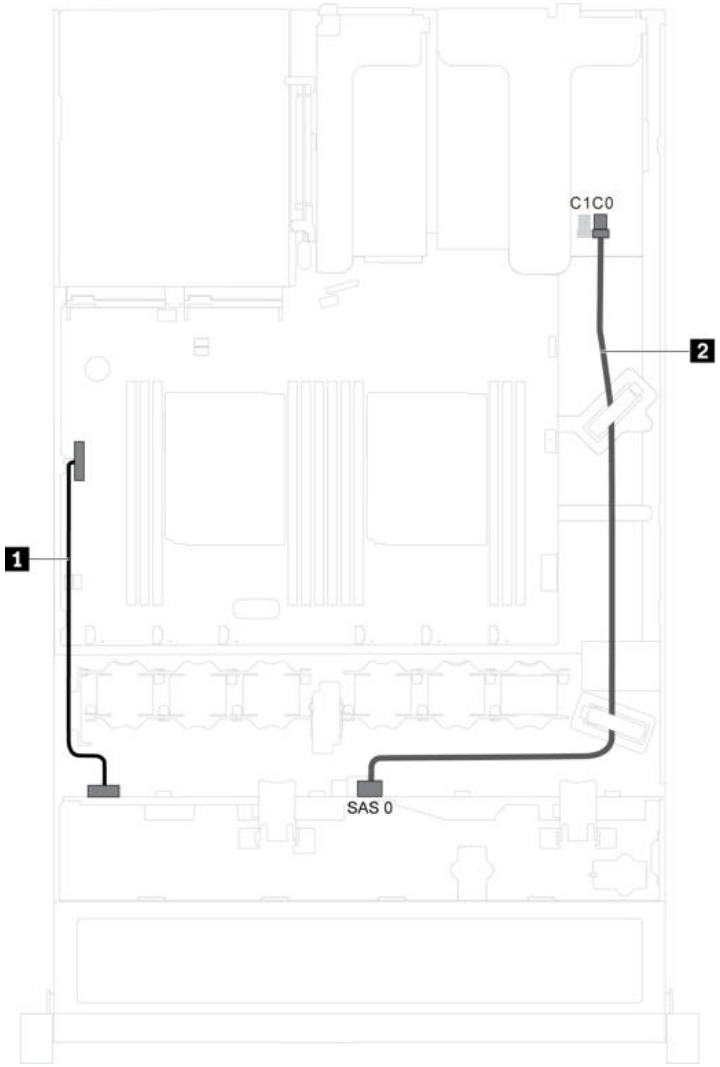


Figure 18. Cable routing for the server model with four 3.5-inch hot-swap drives

Cable	From	To
1 Power cable	Power connector on the backplane	Backplane power connector on the system board
2 SAS signal cable	SAS 0 connector on the backplane	C0 connector on the HBA/RAID adapter

Server model with four 3.5-inch simple-swap drives

Use this section to understand the internal cable routing for the server model with four 3.5-inch simple-swap drives.

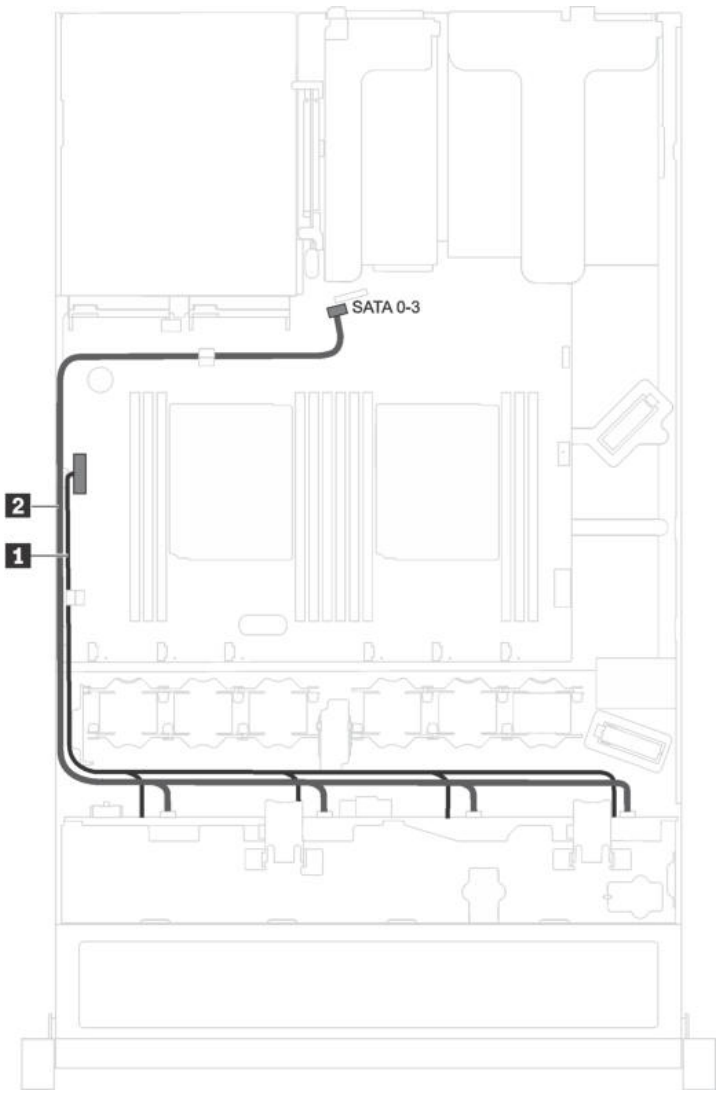


Figure 19. Cable routing for the server model with four 3.5-inch simple-swap drives

The simple-swap drive backplate assembly comes with a power cable and a SATA signal cable.

From	To
1 Power cable of the backplate assembly	Backplane power connector on the system board
2 SATA signal cable of the backplate assembly	SATA 0-3 connector on the system board

Parts list

Use the parts list to identify each of the components that are available for your server.

For more information about ordering the parts shown in Figure 20 “Server components” on page 36, go to:

http://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr530/7x07/parts

Note: Depending on the model, your server might look slightly different from the following illustration. Some of the components might not be available on your server.

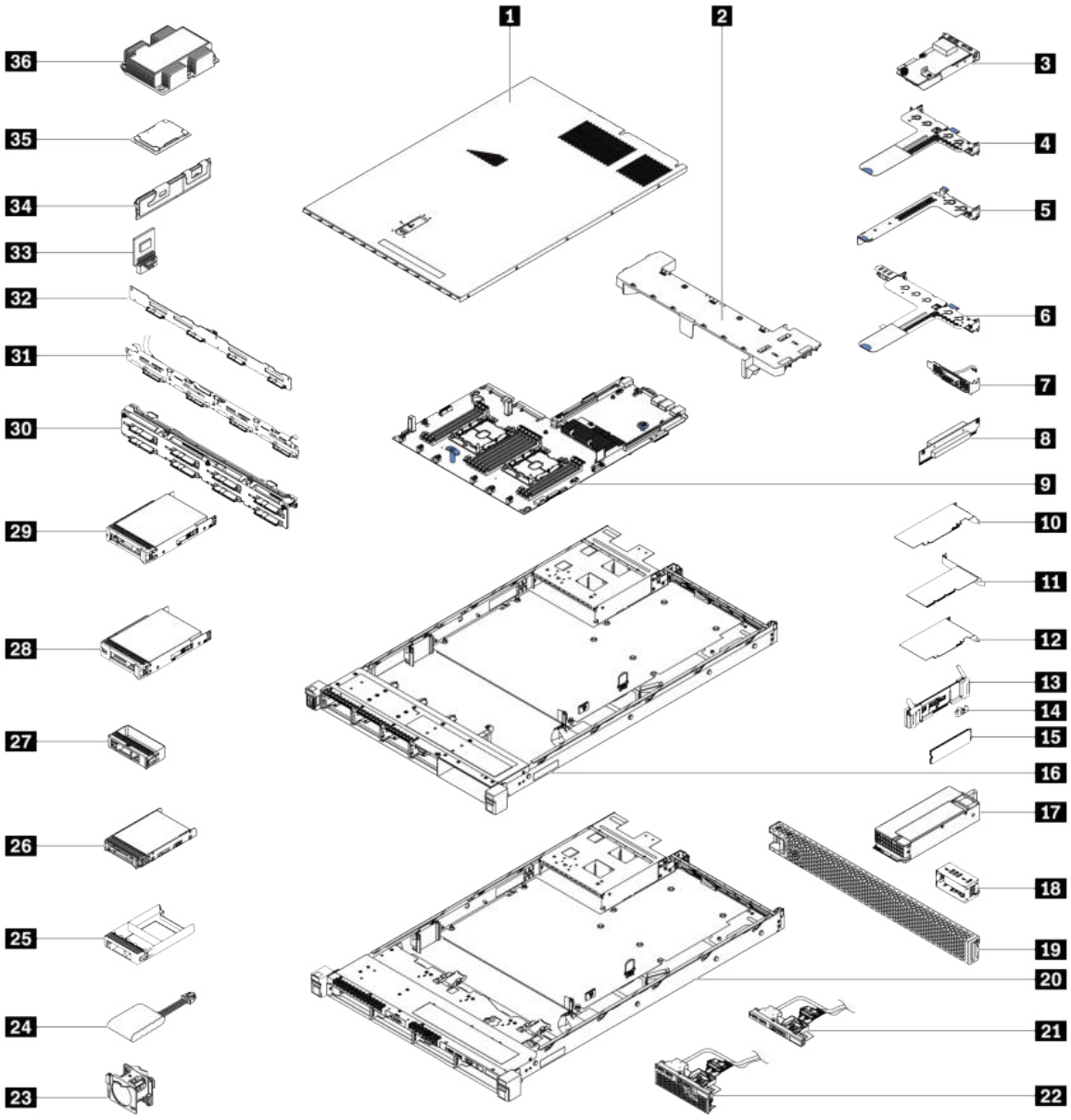


Figure 20. Server components

The parts listed in the following table are identified as one of the following:

- **Tier 1 customer replaceable unit (CRU):** Replacement of Tier 1 CRUs is your responsibility. If Lenovo installs a Tier 1 CRU at your request with no service agreement, you will be charged for the installation.
- **Tier 2 customer replaceable unit:** You may install a Tier 2 CRU yourself or request Lenovo to install it, at no additional charge, under the type of warranty service that is designated for your server.
- **Field replaceable unit (FRU):** FRUs must be installed only by trained service technicians.
- **Consumable and Structural parts:** Purchase and replacement of consumable and structural parts (components, such as a cover or bezel) is your responsibility. If Lenovo acquires or installs a structural component at your request, you will be charged for the service.

Table 9. Parts listing

Index	Description	Tier 1 CRU	Tier 2 CRU	FRU	Consumable and Structural parts
For more information about ordering the parts shown in Figure 20 “Server components” on page 36, go to: http://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr530/7x07/parts					
1	Top cover	√			
2	Air baffle				√
3	LOM adapter	√			
4	Riser 1 bracket (two low profile)	√			
5	Riser 2 bracket (one low profile)	√			
6	Riser 1 bracket (one low-profile and one full-height half-length)	√			
7	Serial port module	√			
8	Riser card	√			
9	System board			√	
10	Low-profile PCIe adapter	√			
11	ML2 adapter	√			
12	Full-height half-length PCIe adapter	√			
13	M.2 backplane	√			
14	M.2 retainer	√			
15	M.2 drive	√			
16	Chassis with eight 2.5-inch drive bays			√	
17	Power supply	√			
18	Power supply filler				√
19	Security bezel	√			
20	Chassis with four 3.5-inch drive bays			√	
21	Front I/O assembly for server models with 3.5-inch drive bays	√			
22	Front I/O assembly for server models with 2.5-inch drive bays	√			

Table 9. Parts listing (continued)

Index	Description	Tier 1 CRU	Tier 2 CRU	FRU	Consumable and Structural parts
23	System fan	√			
24	RAID super capacitor module	√			
25	2.5-inch drive filler				√
26	2.5-inch hot-swap drive	√			
27	3.5-inch drive filler				√
28	3.5-inch simple-swap drive	√			
29	3.5-inch hot-swap drive	√			
30	Backplane for eight hot-swap 2.5-inch drives	√			
31	Simple-swap drive backplate assembly	√			
32	Backplane for four hot-swap 3.5-inch drives	√			
33	TCM/TPM adapter (for Chinese Mainland only)			√	
34	DIMM	√			
35	Processor			√	
36	Processor heat sink			√	

Power cords

Several power cords are available, depending on the country and region where the server is installed.

To view the power cords that are available for the server:

1. Go to:

   http://dcsc.lenovo.com/#/
2. Click **Preconfigured Model** or **Configure to order**.
3. Enter the machine type and model for your server to display the configurator page.
4. Click **Power → Power Cables** to see all line cords.

Notes:

- For your safety, a power cord with a grounded attachment plug is provided to use with this product. To avoid electrical shock, always use the power cord and plug with a properly grounded outlet.
- Power cords for this product that are used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).
- For units intended to be operated at 115 volts: Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a parallel blade, grounding-type attachment plug rated 15 amperes, 125 volts.
- For units intended to be operated at 230 volts (U.S. use): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes, 250 volts.
- For units intended to be operated at 230 volts (outside the U.S.): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.
- Power cords for a specific country or region are usually available only in that country or region.

Chapter 3. Hardware replacement procedures

This section provides installation and removal procedures for all serviceable system components. Each component replacement procedure references any tasks that need to be performed to gain access to the component being replaced.

For more information about ordering parts, go to:

http://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr530/7x07/parts

Note: If you replace a part, such as an adapter, that contains firmware, you might also need to update the firmware for that part. For more information about updating firmware, see “Firmware updates” on page 7.

Installation Guidelines

Before installing components in your server, read the installation guidelines.

Before installing optional devices, read the following notices carefully:

Attention: Prevent exposure to static electricity, which might lead to system halt and loss of data, by keeping static-sensitive components in their static-protective packages until installation, and handling these devices with an electrostatic-discharge wrist strap or other grounding system.

- Read the safety information and guidelines to ensure that you work safely.
  - http://thinksystem.lenovofiles.com/help/topic/safety_documentation/pdf_files.html
  - “Handling static-sensitive devices” on page 43
  - “Working inside the server with the power on” on page 43
- Make sure the components you are installing are supported by the server. For a list of supported optional components for the server, see http://www.lenovo.com/us/en/serverproven/.
- When you install a new server, download and apply the latest firmware. This will help ensure that any known issues are addressed, and that your server is ready to work with optimal performance. Go to ThinkSystem SR530 Drivers and Software to download firmware updates for your server.

  Important: Some cluster solutions require specific code levels or coordinated code updates. If the component is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.
- It is good practice to make sure that the server is working correctly before you install an optional component.
- Keep the working area clean, and place removed components on a flat and smooth surface that does not shake or tilt.
- Do not attempt to lift an object that might be too heavy for you. If you have to lift a heavy object, read the following precautions carefully:
  - Make sure that you can stand steadily without slipping.
  - Distribute the weight of the object equally between your feet.
  - Use a slow lifting force. Never move suddenly or twist when you lift a heavy object.
  - To avoid straining the muscles in your back, lift by standing or by pushing up with your leg muscles.
- Make sure that you have an adequate number of properly grounded electrical outlets for the server, monitor, and other devices.

© Copyright Lenovo 2017, 2020

- Back up all important data before you make changes related to the disk drives.
- Have a small flat-blade screwdriver, a small Phillips screwdriver, and a T8 torx screwdriver available.
- To view the error LEDs on the system board and internal components, leave the power on.
- You do not have to turn off the server to remove or install hot-swap power supplies, hot-swap fans, or hot-plug USB devices. However, you must turn off the server before you perform any steps that involve removing or installing adapter cables, and you must disconnect the power source from the server before you perform any steps that involve removing or installing a riser card.
- Blue on a component indicates touch points, where you can grip to remove a component from or install it in the server, open or close a latch, and so on.
- Orange on a component or an orange label on or near a component indicates that the component can be hot-swapped if the server and operating system support hot-swap capability, which means that you can remove or install the component while the server is still running. (Orange can also indicate touch points on hot-swap components.) See the instructions for removing or installing a specific hot-swap component for any additional procedures that you might have to perform before you remove or install the component.
- The Red strip on the drives, adjacent to the release latch, indicates that the drive can be hot-swapped if the server and operating system support hot-swap capability. This means that you can remove or install the drive while the server is still running.

  Note: See the system specific instructions for removing or installing a hot-swap drive for any additional procedures that you might need to perform before you remove or install the drive.
- After finishing working on the server, make sure you reinstall all safety shields, guards, labels, and ground wires.

System reliability guidelines

Review the system reliability guidelines to ensure proper system cooling and reliability.

Make sure the following requirements are met:

- When the server comes with redundant power, a power supply must be installed in each power-supply bay.
- Adequate space around the server must be spared to allow server cooling system to work properly. Leave approximately 50 mm (2.0 in.) of open space around the front and rear of the server. Do not place any object in front of the fans.
- For proper cooling and airflow, refit the server cover before you turn the power on. Do not operate the server for more than 30 minutes with the server cover removed, for it might damage server components.
- Cabling instructions that come with optional components must be followed.
- A failed fan must be replaced within 48 hours since malfunction.
- A removed hot-swap fan must be replaced within 30 seconds after removal.
- A removed hot-swap drive must be replaced within two minutes after removal.
- A removed hot-swap power supply must be replaced within two minutes after removal.
- Every air baffle that comes with the server must be installed when the server starts (some servers might come with more than one air baffle). Operating the server with a missing air baffle might damage the processor.
- All processor sockets must contain either a socket cover or a processor with heat sink.
- When more than one processor is installed, fan population rules for each server must be strictly followed.

Working inside the server with the power on

You might need to keep the power on with the server cover removed to look at system information on the display panel or to replace hot-swap components. Review these guidelines before doing so.

Attention: The server might stop and loss of data might occur when internal server components are exposed to static electricity. To avoid this potential problem, always use an electrostatic-discharge wrist strap or other grounding systems when working inside the server with the power on.

- Avoid loose-fitting clothing, particularly around your forearms. Button or roll up long sleeves before working inside the server.
- Prevent your necktie, scarf, badge rope, or long hair from dangling into the server.
- Remove jewelry, such as bracelets, necklaces, rings, cuff links, and wrist watches.
- Remove items from your shirt pocket, such as pens and pencils, in case they fall into the server as you lean over it.
- Avoid dropping any metallic objects, such as paper clips, hairpins, and screws, into the server.

Handling static-sensitive devices

Review these guidelines before you handle static-sensitive devices to reduce the possibility of damage from electrostatic discharge.

Attention: Prevent exposure to static electricity, which might lead to system halt and loss of data, by keeping static-sensitive components in their static-protective packages until installation, and handling these devices with an electrostatic-discharge wrist strap or other grounding system.

- Limit your movement to prevent building up static electricity around you.
- Take additional care when handling devices during cold weather, for heating would reduce indoor humidity and increase static electricity.
- Always use an electrostatic-discharge wrist strap or other grounding system, particularly when working inside the server with the power on.
- While the device is still in its static-protective package, touch it to an unpainted metal surface on the outside of the server for at least two seconds. This drains static electricity from the package and from your body.
- Remove the device from the package and install it directly into the server without putting it down. If it is necessary to put the device down, put it back into the static-protective package. Never place the device on the server or on any metal surface.
- When handling a device, carefully hold it by the edges or the frame.
- Do not touch solder joints, pins, or exposed circuitry.
- Keep the device from others' reach to prevent possible damages.

Rack latches replacement

Use this information to remove and install the rack latches.

Remove the rack latches

Use this information to remove the rack latches.



"**Read** the installation Guidelines" on page 41

Before removing the rack latches:

1. If you have installed the security bezel, remove it. See "Remove the security bezel" on page 48.
2. Use a flat-blade screwdriver to remove the ID label plate on the right rack latch and place it in a safe place.

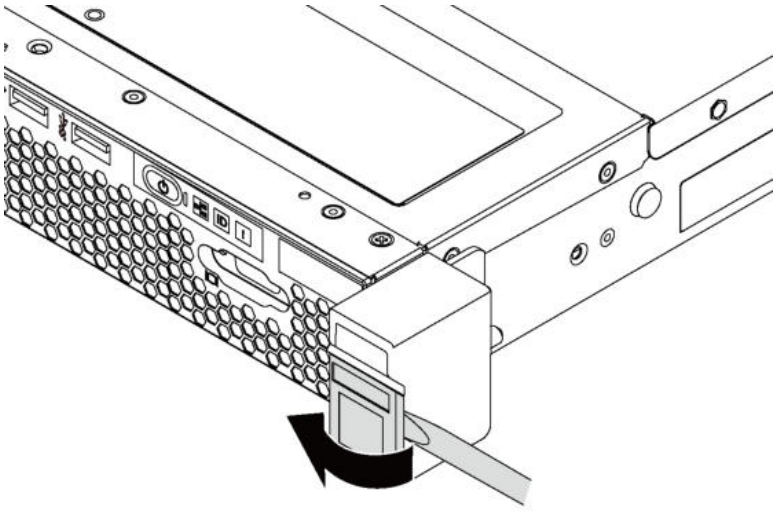


Figure 21. ID label plate removal

To remove the rack latches, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. On each side of the server, remove the two screws that secure the rack latch.

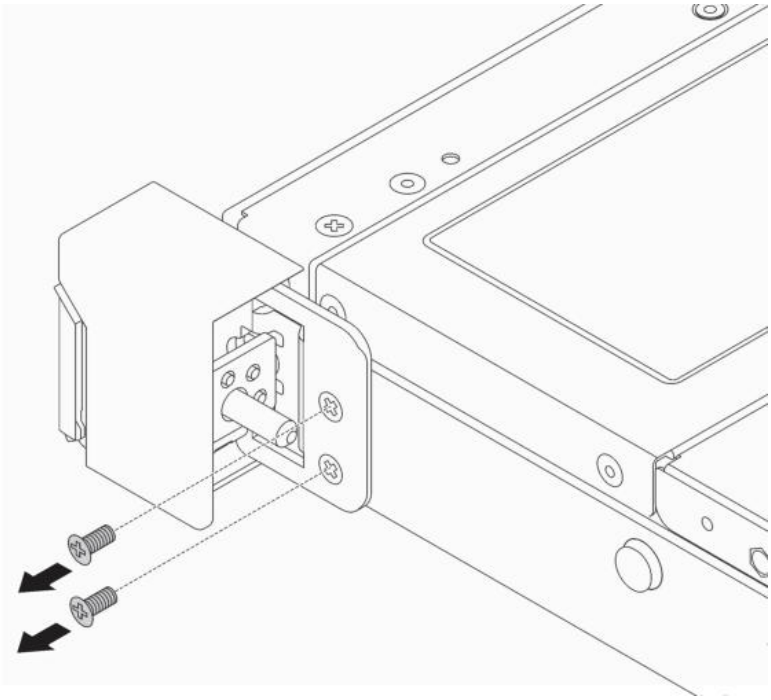


Figure 22. Rack latch screws removal

Step 2. On each side of the server, remove the rack latch from the chassis as shown.

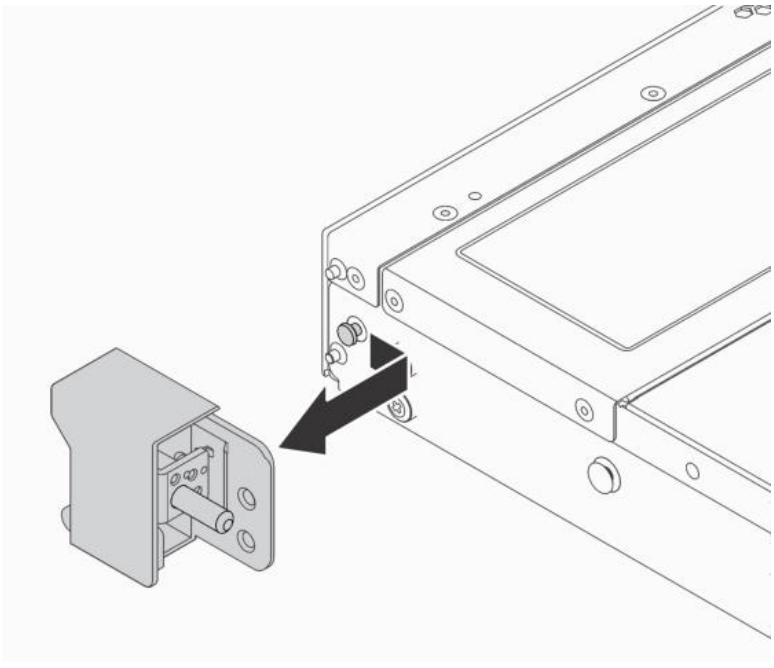


Figure 23. Rack latch removal

If you are instructed to return the old rack latches, follow all packaging instructions and use any packaging materials that are provided.

Install the rack latches

Use this information to install the rack latches.

"**Read** the installation Guidelines" on page 41

To install the rack latches, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. On each side of the server, align the rack latch with the pin on the chassis; then, press the rack latch onto the chassis and slightly slide it forward as shown.

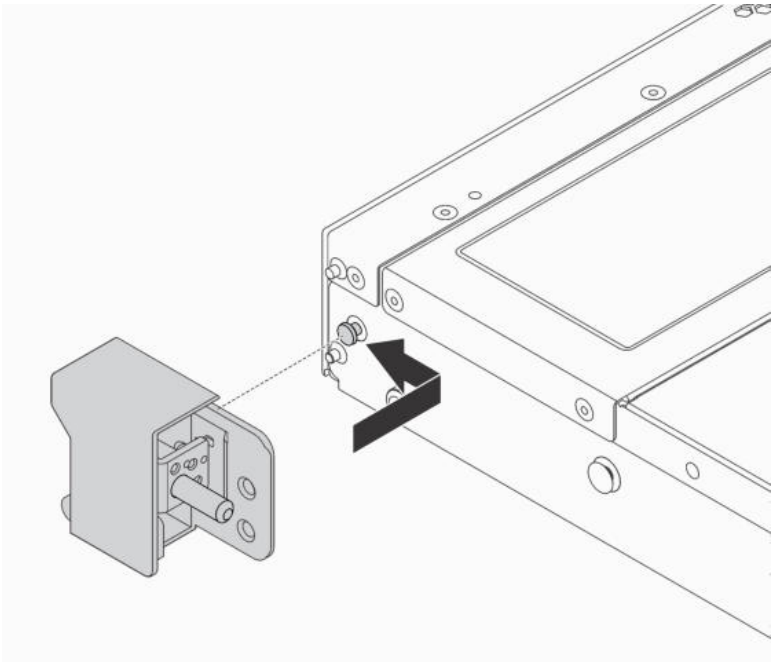


Figure 24. Rack latch installation

Step 2. Install the two screws to secure the rack latch on each side of the server.

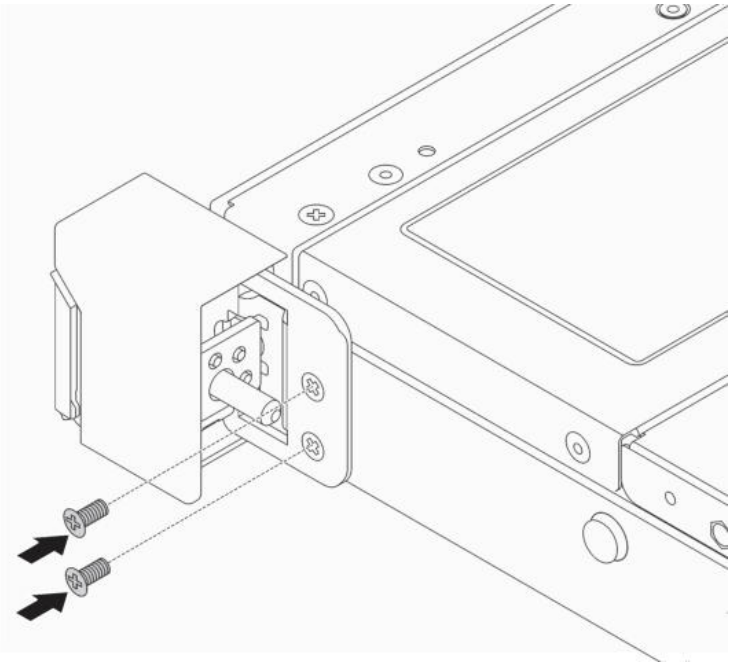


Figure 25. Rack latch screws installation

After installing the rack latches:

1. Install the ID label plate to the right rack latch as shown.

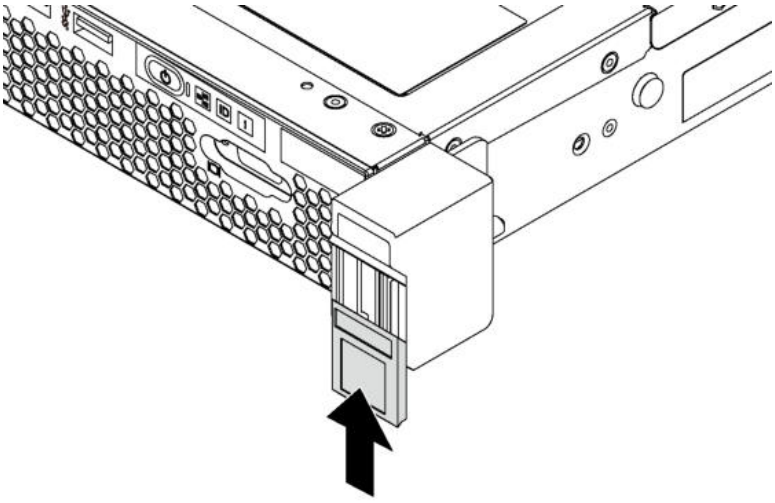


Figure 26. ID label plate installation

2. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Security bezel replacement

Use this information to remove and install the security bezel.

Remove the security bezel

Use this information to remove the security bezel.



"**Read** the installation Guidelines" on page 41

To remove the security bezel, complete the following steps:

Step 1. Use the key to unlock the security bezel.

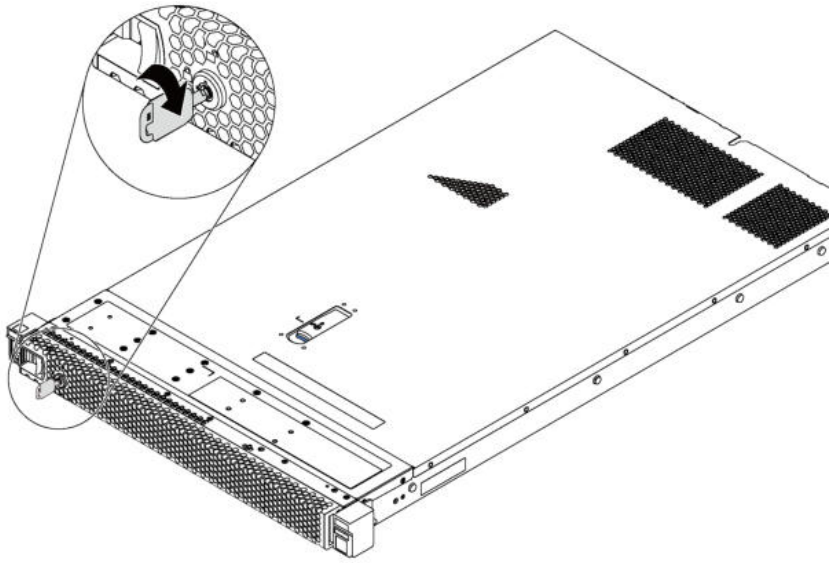


Figure 27. Security bezel unlock

Step 2. Press the blue release latch 1 and pivot the security bezel outward to remove it from the chassis.

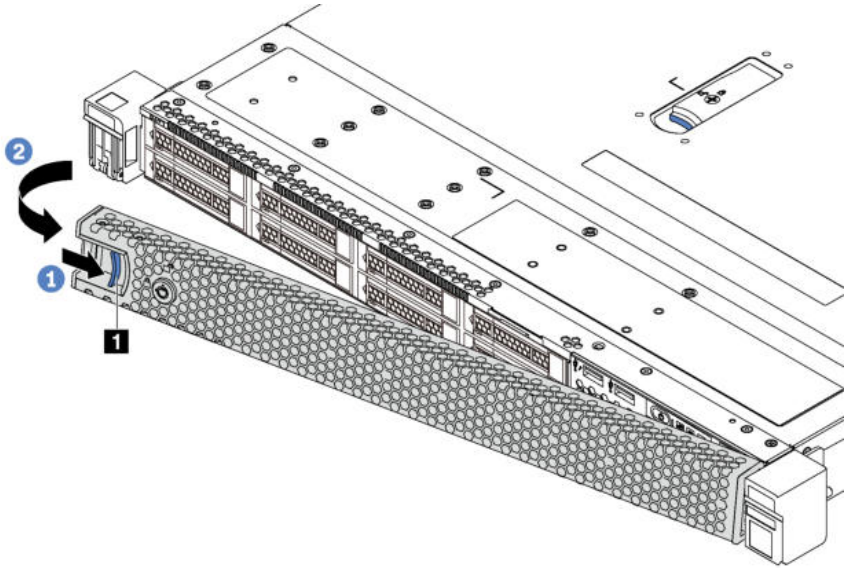


Figure 28. Security bezel removal

Attention: Before you ship the rack with the server installed, reinstall and lock the security bezel into place.

Install the security bezel

Use this information to install the security bezel.



"**Read** the installation Guidelines" on page 41

Attention: Before you ship the rack with the server installed, install and lock the security bezel into place.

Before installing the security bezel, if you have removed the rack latches, reinstall them. See "Install the rack latches" on page 46.

To install the security bezel, complete the following steps:

Step 1. If the key is held inside the security bezel, remove it out of the security bezel.

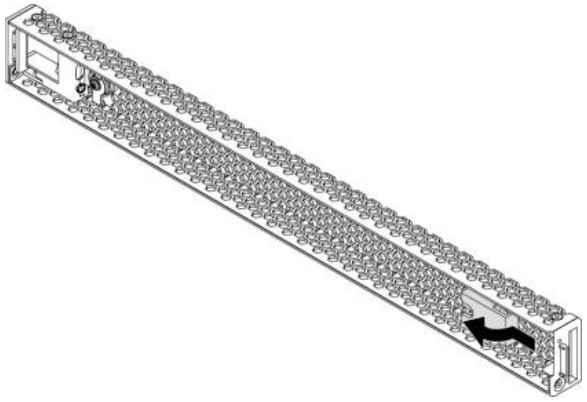


Figure 29. Key removal

Step 2. Insert the tab on the security bezel into the slot on the right side of the chassis. Then, press the blue release latch 1 and pivot the security bezel inward until it clicks into place.

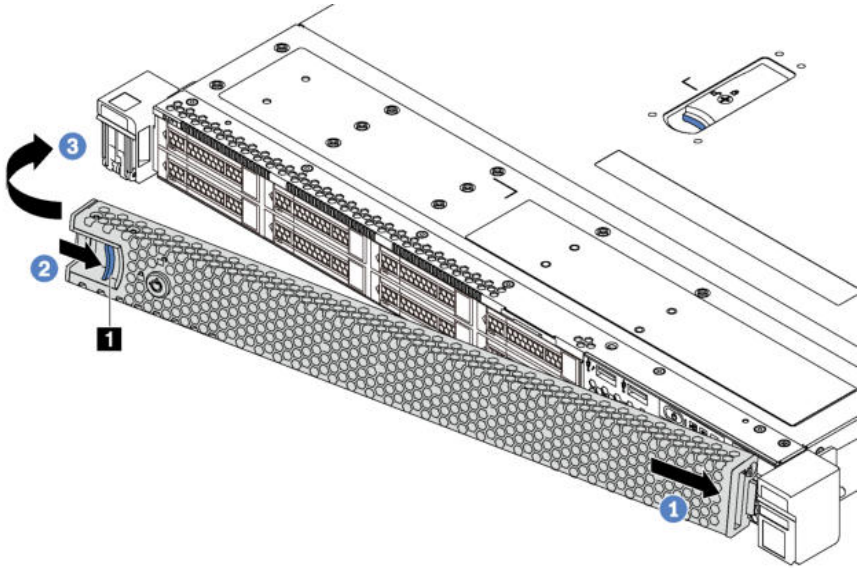


Figure 30. Security bezel installation

Step 3. Use the key to lock the security bezel.

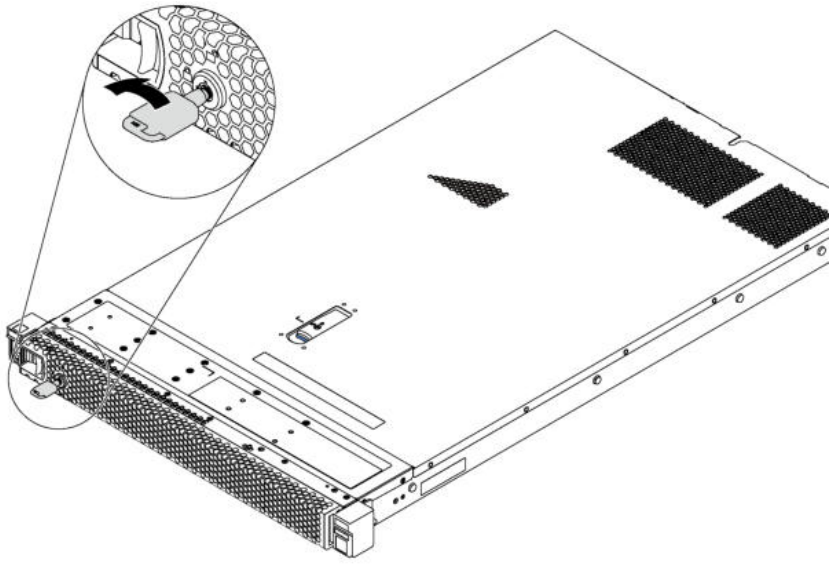


Figure 31. Security bezel lockup

Top cover replacement

Use this information to remove and install the top cover.

S033



CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

S014



CAUTION:
Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the label is attached.

Remove the top cover

Use this information to remove the top cover.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

To remove the top cover, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

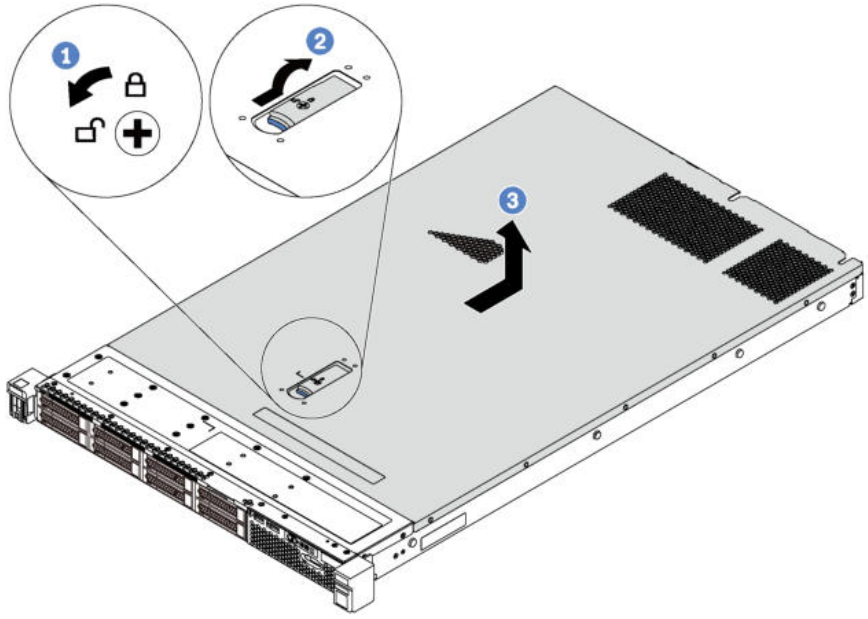


Figure 32. Top cover removal

Step 1. Use a screwdriver to turn the cover lock to the open position.

Step 2. Press the blue button on the cover latch and open the cover latch.

Step 3. Slide the cover to the rear until it is disengaged from the chassis. Then, lift the cover off the chassis and place it on a flat clean surface.

Attention:

- Handle the top cover carefully. Dropping the top cover with the cover latch open might damage the cover latch.
- For proper cooling and airflow, install the top cover before you power on the server.

Install the top cover

Use this information to install the top cover.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the top cover:

1. Ensure that all cables, adapters, and other components are installed and seated correctly and that you have not left loose tools or parts inside the server.
2. Ensure that all internal cables are correctly routed. See “Internal cable routing” on page 28.
3. If you are installing a new top cover, attach the service label to the new top cover first if necessary.

   Note: A new top cover comes without a service label attached. If you need a service label, order it together with the new top cover. The service label is free of charge.

To install the top cover, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

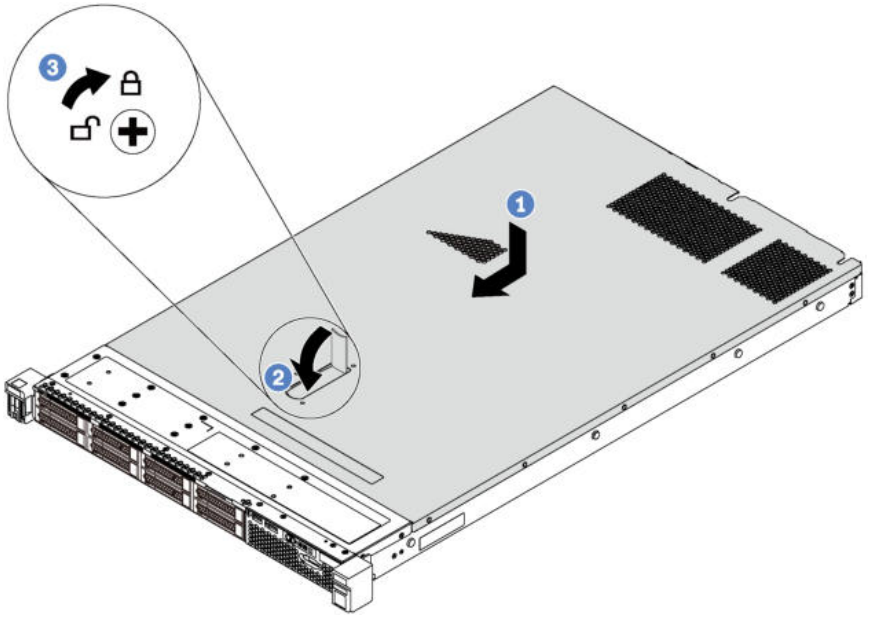


Figure 33. Top cover installation

Note: Before you slide the top cover forward, ensure that all the tabs on the top cover engage the chassis correctly. If the tabs do not engage the chassis correctly, it will be very difficult to remove the top cover later.

Step 1. Ensure that the cover latch is in the open position. Lower the cover onto the chassis until all tabs on both sides of the cover engage with the guides on both sides of the chassis.

Step 2. Pivot the cover latch and slide the cover forward until the cover snaps into position. Ensure that the cover latch is completely closed.

Step 3. Use a screwdriver to turn the cover lock to the closed position.

After installing the top cover, complete the parts replacement. See “Complete the parts replacement” on page 143.

Air baffle replacement

Use this information to remove and install the air baffle

S033



CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

S017



CAUTION:
Hazardous moving fan blades nearby. Keep fingers and other body parts away.

Remove the air baffle

Use this information to remove the air baffle.



“**Read** the installation Guidelines” on page 41



“**Power off** the server for this task” on page 11

To remove the air baffle, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

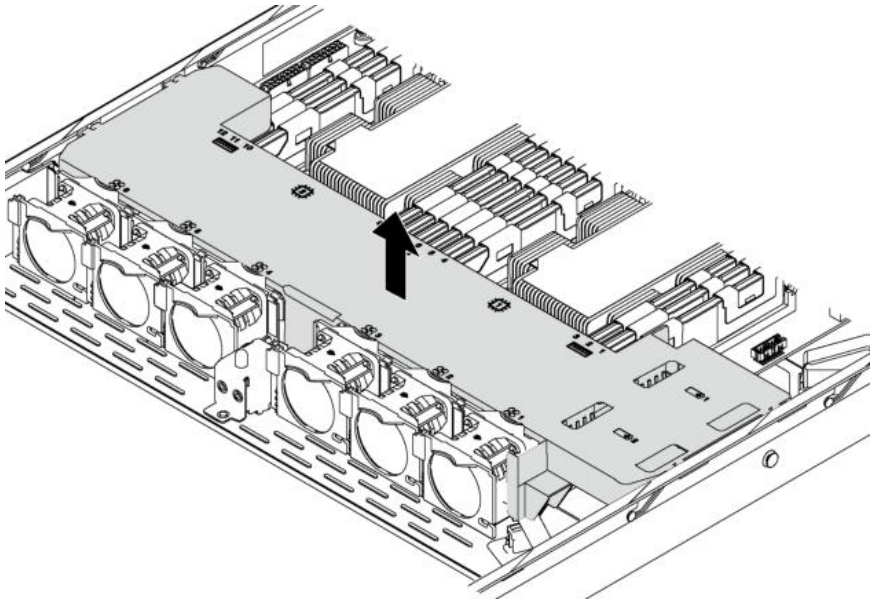


Figure 34. Air baffle removal

Step 1. Remove the top cover. See “Remove the top cover” on page 52.

Step 2. If the server has a RAID super capacitor module installed underneath the air baffle, disconnect its cable from the extension cable.

Step 3. Grasp the air baffle and carefully lift it out of the server.

Attention: For proper cooling and airflow, install the air baffle before you power on the server. Operating the server without an air baffle might damage server components.

Install the air baffle

Use this information to install the air baffle.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11

Before installing the air baffle:

1. Ensure that the retaining clips on each end of the DIMM connectors are closed.
2. If you want to install a RAID super capacitor module, install it onto the air baffle first. See "Install a RAID super capacitor module" on page 60.

To install the air baffle, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

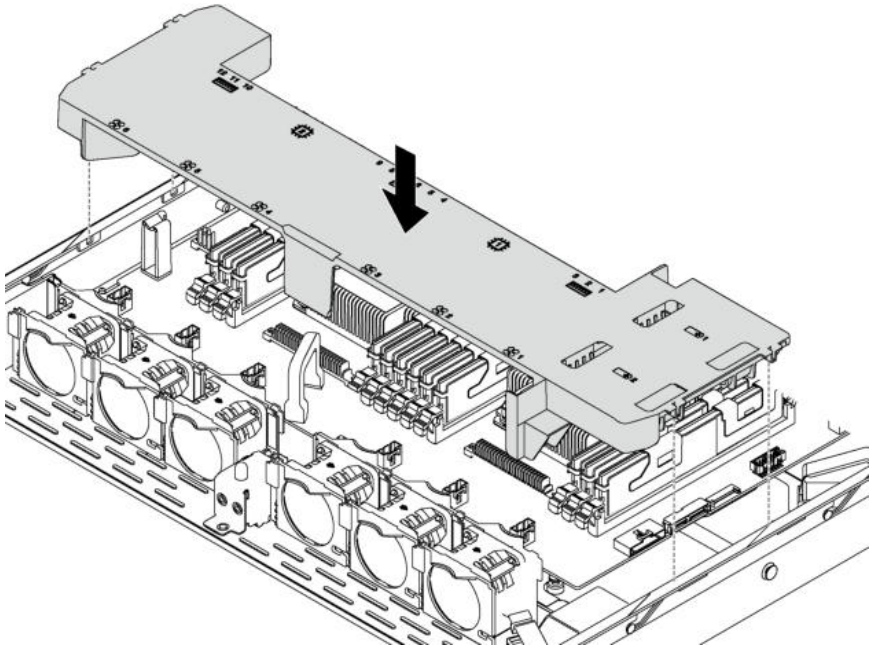


Figure 35. Air baffle installation

Step 1. Align the tabs on both sides of the air baffle with the corresponding slots on both sides of the chassis.

Step 2. Lower the air baffle into the server and press the air baffle down until it is securely seated.

After installing the air baffle:

1. If you have installed a RAID super capacitor module, connect it to the RAID adapter using the extension cable that comes with the RAID super capacitor module. See "Internal cable routing" on page 28.
2. Complete the parts replacement. See "Complete the parts replacement" on page 143.

RAID super capacitor module replacement

Use this information to remove and install a RAID super capacitor module.

Your server supports up to two RAID super capacitor modules. The RAID super capacitor holders are located underneath the air baffle.

Remove a RAID super capacitor module

Use this information to remove a RAID super capacitor module.

		
“**Read** the installation Guidelines” on page 41	“**Power off** the server for this task” on page 11	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing the RAID super capacitor module:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Locate the RAID super capacitor module, and disconnect its cable. The RAID super capacitor holders are located underneath the air baffle.
3. Remove the air baffle and turn it over. See “Remove the air baffle” on page 55.

To remove the RAID super capacitor module, complete the following steps:

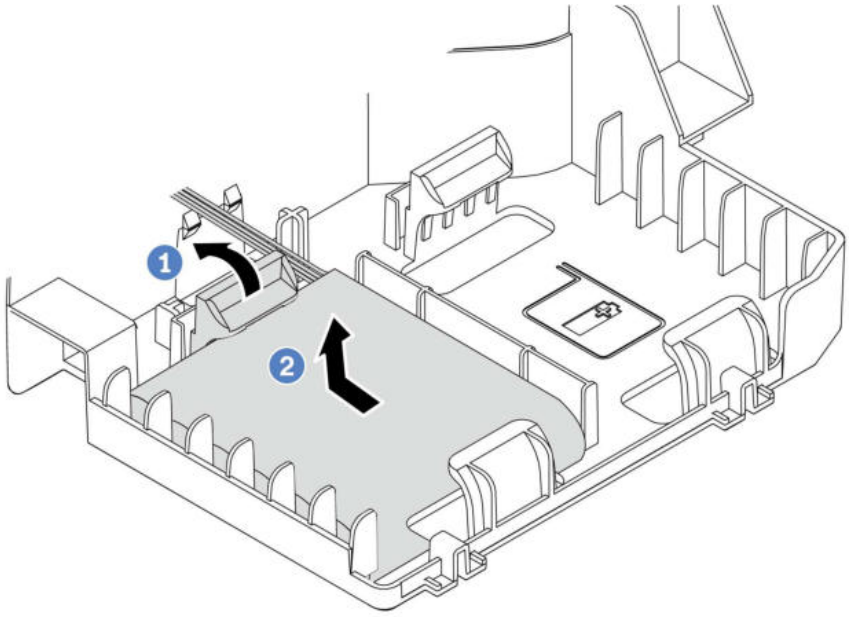


Figure 36. RAID super capacitor module removal

Step 1. Gently pivot the retaining clip as shown.

Step 2. Lift the RAID super capacitor up and remove it from the holder.

If you are instructed to return the old RAID super capacitor module, follow all packaging instructions and use any packaging materials that are provided.

Install a RAID super capacitor module

If your server has a RAID adapter with a super capacitor connector, you can install a RAID super capacitor module in your server.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11
	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43	

Before installing the RAID super capacitor module:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Remove the air baffle and turn it over. See “Remove the air baffle” on page 55.
3. Locate the RAID super capacitor holder.
4. Touch the static-protective package that contains the new RAID super capacitor module to any unpainted surface on the outside of the server. Then, take the new RAID super capacitor module out of the package and place it on a static-protective surface.

To install the RAID super capacitor module, complete the following steps:

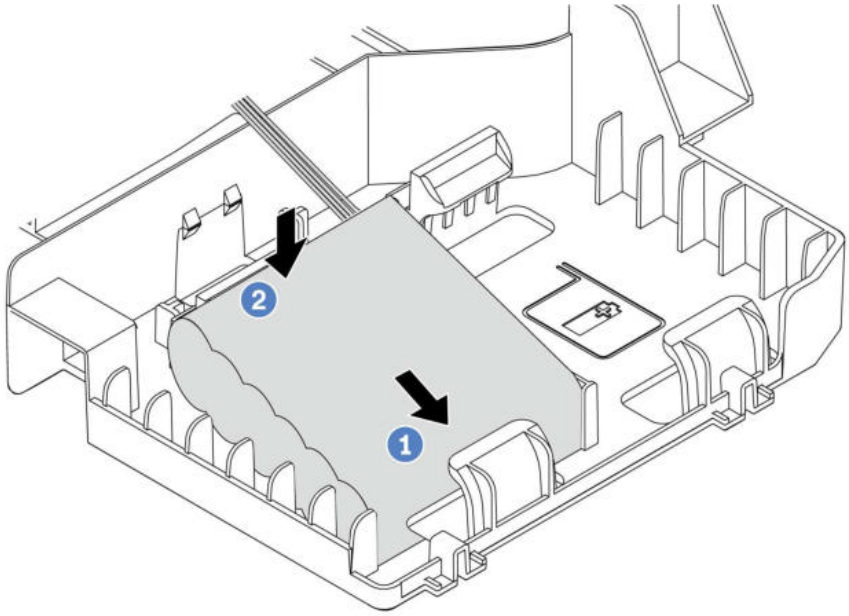


Figure 37. RAID super capacitor module installation

Step 1. Insert the RAID super capacitor module into the retaining clip at one side as shown.

Step 2. Press the RAID super capacitor module down on the other side until it snaps into place.

Step 3. Connect the RAID super capacitor module to the RAID adapter using an extension cable. See “Internal cable routing” on page 28.

Step 4. If your server has two RAID adapters each with a super capacitor connector, you can continue to install the second RAID super capacitor module.

After installing the RAID super capacitor module, complete the parts installation. See “Complete the parts replacement” on page 143.

System fan replacement

Use this information to remove and install a system fan.

S033



CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

S009



CAUTION:
To avoid personal injury, disconnect the fan cables before removing the fan from the device.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

Remove a system fan

Use this information to remove a system fan.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing a system fan:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Remove the air baffle. See “Remove the air baffle” on page 55.

To remove a system fan, complete the following steps:

Watch the procedure. A video of the removal process is available:

- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

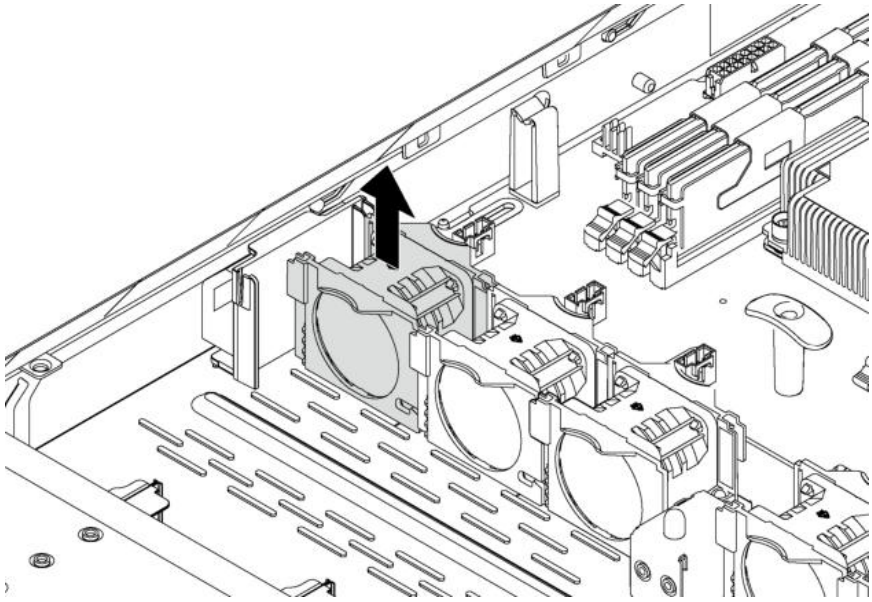


Figure 38. System fan removal

Step 1. Disconnect the system fan cable from the system board.

Step 2. Grasp the system fan with your index finger and thumb and carefully lift it straight up.

After removing the system fan:

1. Install a new fan to cover the fan bay.
2. If you are instructed to return the old system fan, follow all packaging instructions and use any packaging materials that are provided.

Install a system fan

Use this information to install a system fan.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before installing a system fan, touch the static-protective package that contains the new system fan to any unpainted surface on the outside of the server. Then, take the new system fan out of the package and place it on a static-protective surface.

To install a system fan, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

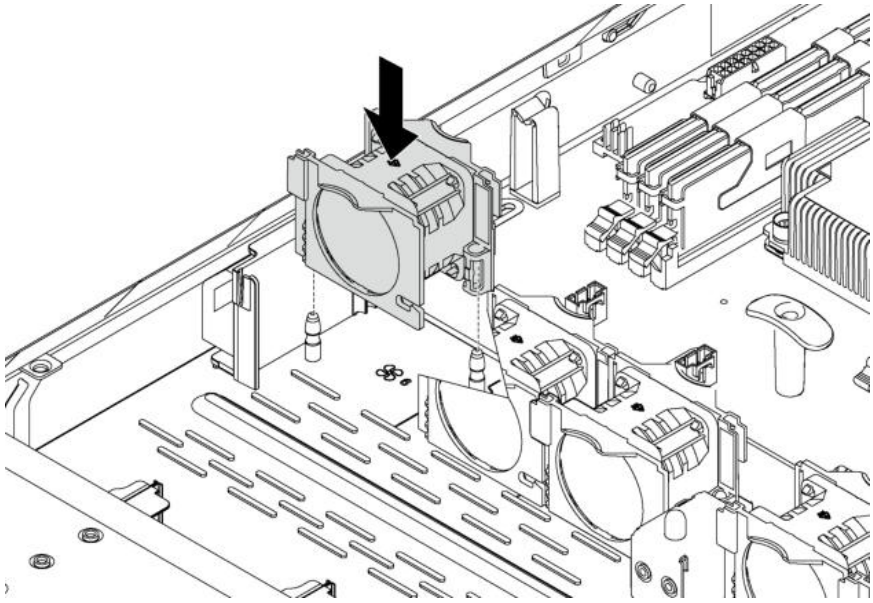


Figure 39. System fan installation

Step 1. Align the support holes of the system fan with the two pins in the chassis, and press it straight down until it is seated into place.

Note: Ensure that the system fan cable is at the side next to the system board.

Step 2. Connect the system fan cable to the system fan connector on the system board.

After installing the system fan, complete the parts replacement. See "Complete the parts replacement" on page 143.

Front I/O assembly replacement

Use this information to remove and install the front I/O assembly.

Remove the front I/O assembly

Use this information to remove the front I/O assembly.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11
	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43	

Before removing the front I/O assembly:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. If the security bezel is installed, remove it. See “Remove the security bezel” on page 48.
3. Disconnect cables of the front I/O assembly from the system board.

To remove the front I/O assembly, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Table 10. Front I/O assembly removal

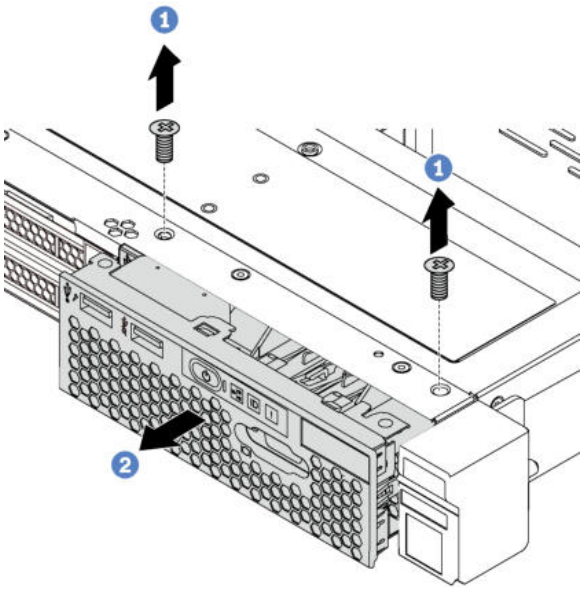


Figure 40. Server models with 2.5-inch drive bays

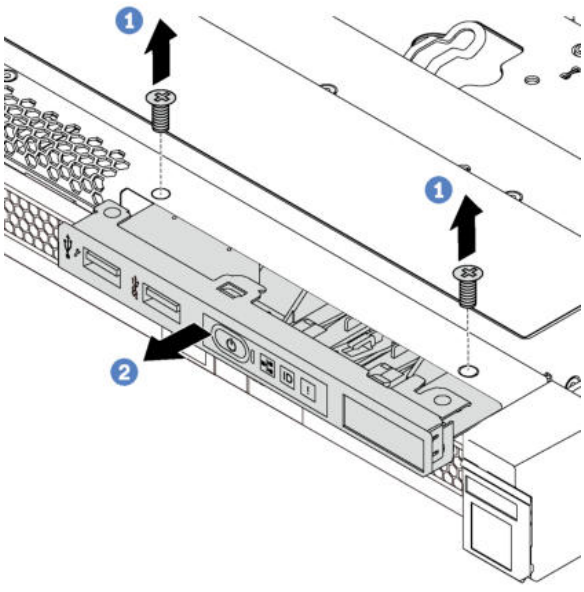


Figure 41. Server models with 3.5-inch drive bays

Step 1. Remove the screws that secure the front I/O assembly.

Step 2. Slide the front I/O assembly out of the assembly bay.

If you are instructed to return the old front I/O assembly, follow all packaging instructions and use any packaging materials that are provided.

Install the front I/O assembly

Use this information to install the front I/O assembly.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the front I/O assembly, touch the static-protective package that contains the new front I/O assembly to any unpainted surface on the outside of the server. Then, take new the front I/O assembly out of the package and place it on a static-protective surface.

To install the front I/O assembly, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Table 11. Front I/O assembly installation

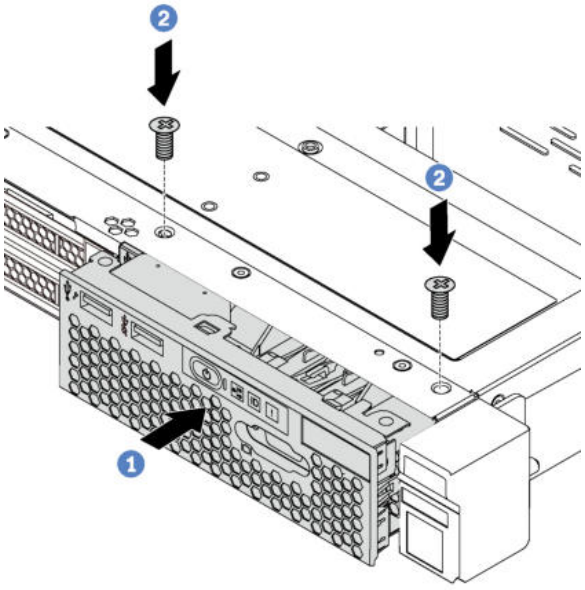


Figure 42. Server models with 2.5-inch drive bays

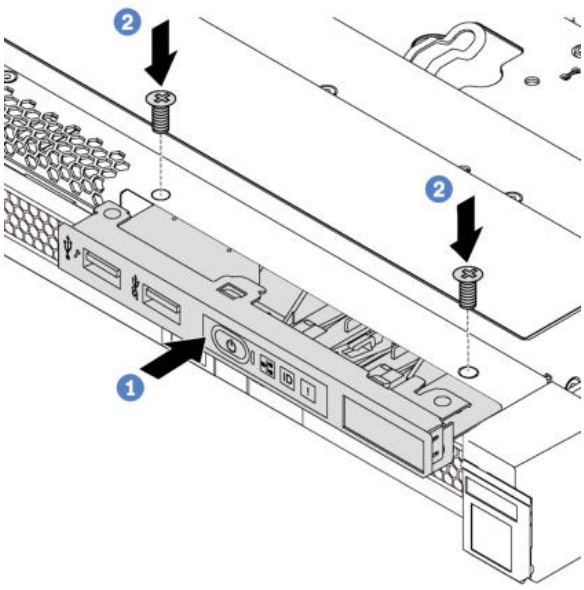


Figure 43. Server models with 3.5-inch drive bays

Step 1. Insert the front I/O assembly into the assembly bay.

Step 2. Install the screws to secure the front I/O assembly in place.

Step 3. Connect the cables of the front I/O assembly to the system board. See “Internal cable routing” on page 28.

After installing the front I/O assembly, complete the parts replacement. See “Complete the parts replacement” on page 143.

Hot-swap drive backplane replacement

Use this information to remove and install the hot-swap drive backplane.

Remove the backplane for four 3.5-inch hot-swap drives

Use this information to remove the backplane for four 3.5-inch hot-swap drives.

	"**Read** the installation Guidelines" on page 41	 "**Power off** the server for this task" on page 11	 "**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the backplane:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. Record the cable connections on the backplane and then disconnect cables from the backplane.
3. Remove all the installed drives and drive fillers (if any) from the drive bays. See "Remove a hot-swap drive" on page 73.

To remove the backplane, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

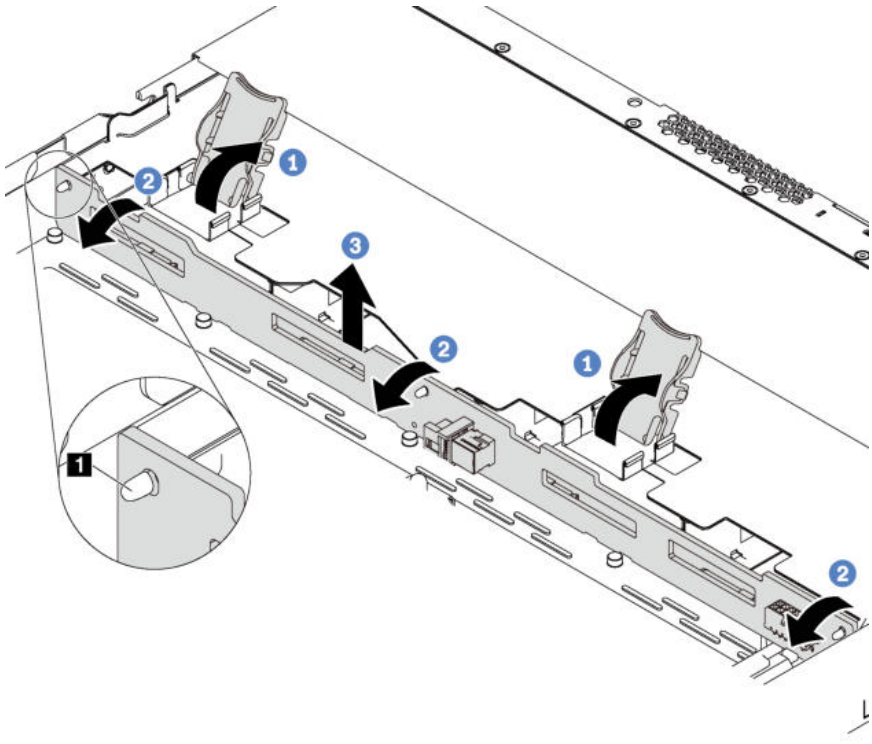


Figure 44. Backplane removal

Step 1. Open the release latches that secure the backplane.

Step 2. Pivot the backplane backward slightly to release it from the three pins 1 on the chassis.

Step 3. Carefully remove the backplane out of the chassis from under the front I/O assembly cables.

If you are instructed to return the old backplane, follow all packaging instructions and use any packaging materials that are provided.

Install the backplane for four 3.5-inch hot-swap drives

Use this information to install the backplane for four 3.5-inch hot-swap drives.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before installing the backplane, touch the static-protective package that contains the new backplane to any unpainted surface on the outside of the server. Then, take the new backplane out of the package and place it on a static-protective surface.

To install the backplane, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

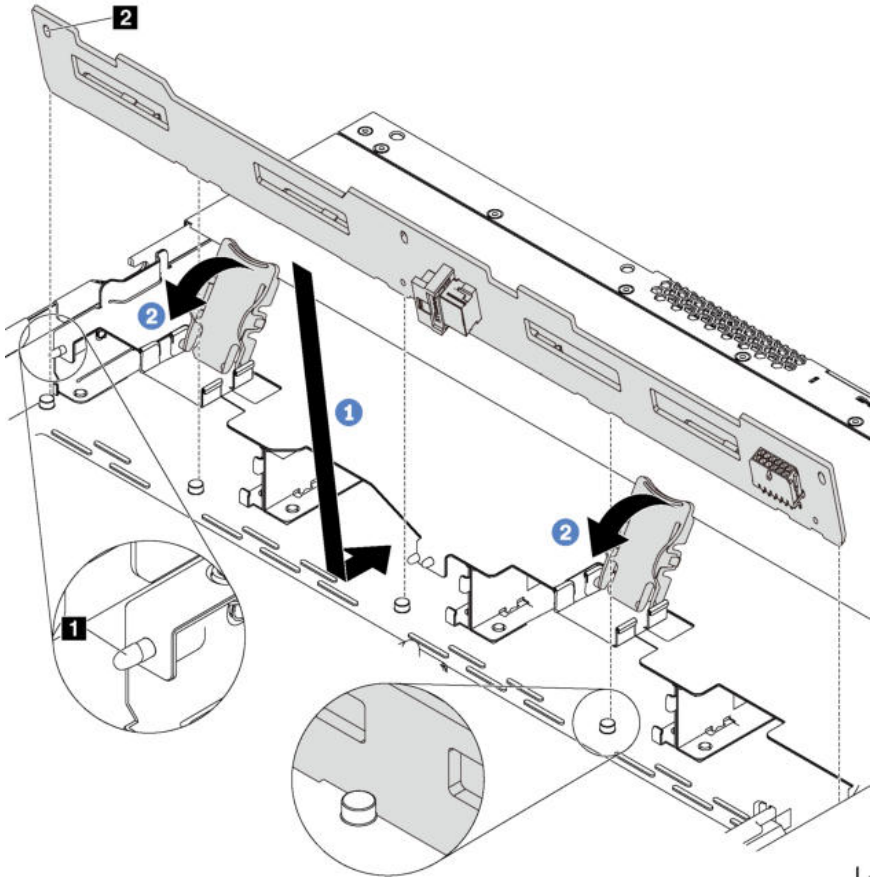


Figure 45. Backplane installation

Step 1. Put the backplane under the front I/O assembly cables, align it with the chassis, and lower it into the chassis. Put the backplane into place with it leaning backward slightly so that the three pins 1 on the chassis pass through the three holes 2 in the backplane.

Step 2. Close the release latches to secure the backplane in place.

After installing the backplane:

1. Connect cables to the backplane. See “Internal cable routing” on page 28.
2. Reinstall all the drives and drive fillers that you removed. See “Install a hot-swap drive” on page 74.
3. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Remove the backplane for eight 2.5-inch hot-swap drives

Use this information to remove the backplane for eight 2.5-inch hot-swap drives.



“**Read** the installation Guidelines” on page 41



“**Power off** the server for this task” on page 11



“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing the backplane:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Record the cable connections on the backplane and then disconnect cables from the backplane.
3. Remove all the installed drives and drive fillers (if any) from the drive bays. See “Remove a hot-swap drive” on page 73.

To remove the backplane, complete the following step:

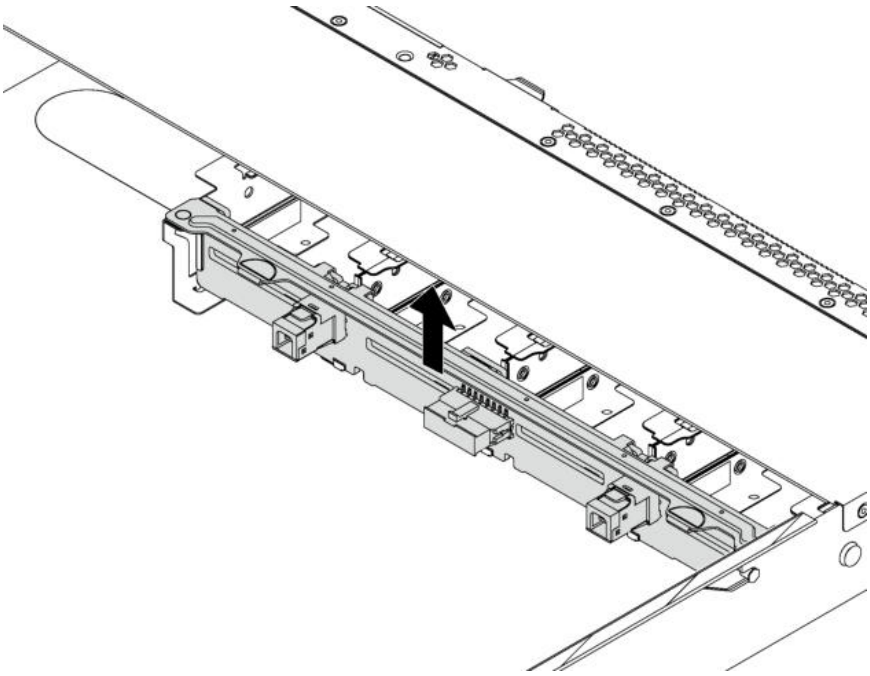


Figure 46. Backplane removal

Step 1. Grasp the backplane and carefully lift it out of the chassis.

If you are instructed to return the old backplane, follow all packaging instructions and use any packaging materials that are provided.

Install the backplane for eight 2.5-inch hot-swap drives

Use this information to install the backplane for eight 2.5-inch hot-swap drives.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the backplane, touch the static-protective package that contains the new backplane to any unpainted surface on the outside of the server. Then, take the new backplane out of the package and place it on a static-protective surface.

To install the backplane, complete the following steps:

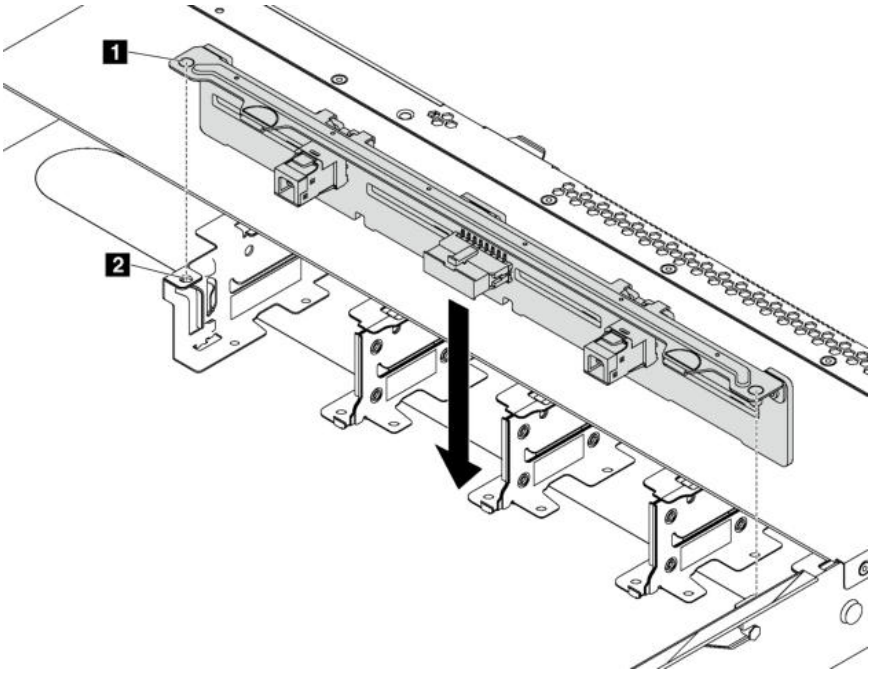


Figure 47. Backplane installation

Step 1. Align pins 1 on the backplane with the holes 2 in the chassis.

Step 2. Lower the backplane into the chassis. Ensure that the pins pass through the holes and the backplane is fully seated in place.

After installing the backplane:

1. Connect cables to the backplane. See “Internal cable routing” on page 28.
2. Reinstall all the drives and drive fillers that you removed. See “Install a hot-swap drive” on page 74.
3. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Simple-swap drive backplate assembly replacement

Use this information to remove and install the simple-swap drive backplate assembly.

Remove the simple-swap drive backplate assembly

Use this information to remove the simple-swap drive backplate assembly.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the simple-swap drive backplate assembly:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. Record the cable connections and disconnect cables of the simple-swap drive backplate assembly.
3. Remove all the installed drives and drive fillers (if any) from the drive bays. See "Remove a simple-swap drive" on page 76.

To remove the simple-swap drive backplate assembly, complete the following steps:

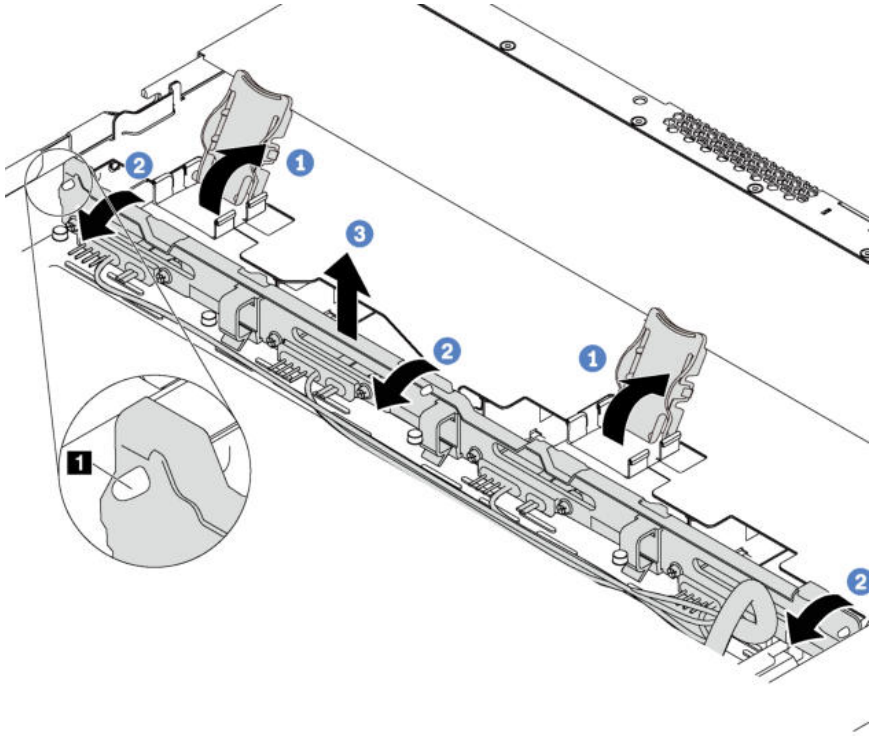


Figure 48. Simple-swap drive backplate assembly removal

Step 1. Open the release latches that secure the simple-swap drive backplate assembly.

Step 2. Pivot the simple-swap drive backplate assembly backward slightly to release it from the three pins 1 on the chassis.

Step 3. Carefully remove the backplate assembly out of the chassis from under the front I/O assembly cables.

If you are instructed to return the old simple-swap drive backplate assembly, follow all packaging instructions and use any packaging materials that are provided.

Install the simple-swap drive backplate assembly

Use this information to install the simple-swap drive backplate assembly.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the simple-swap drive backplate assembly, touch the static-protective package that contains the new backplate assembly to any unpainted surface on the outside of the server. Then, take the new backplate assembly out of the package and place it on a static-protective surface.

To install the simple-swap drive backplate assembly, complete the following steps:

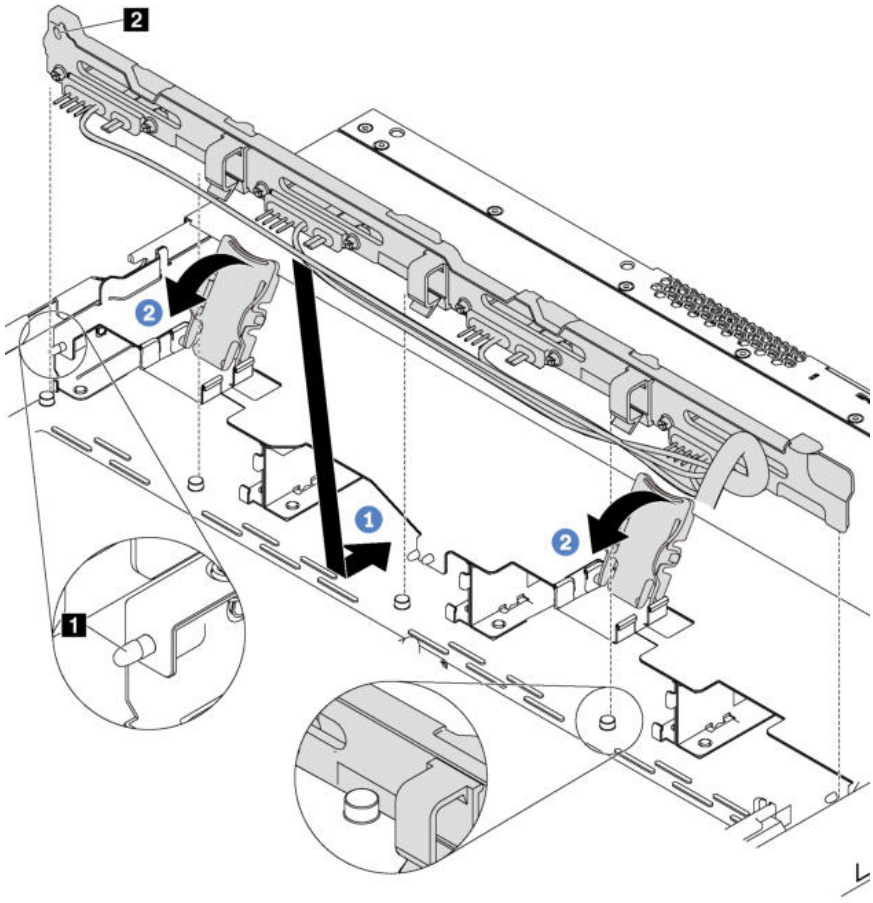


Figure 49. Simple-swap drive backplate assembly installation

Step 1. Put the backplate assembly under the front I/O assembly cables, align it with the chassis, and lower it into the chassis. Put the backplate assembly into place with it leaning backward slightly so that the three pins 1 on the chassis pass through the three holes 2 in the assembly.

Step 2. Close the release latches to secure the backplate assembly in place.

After installing the simple-swap drive backplate assembly:

1. Connect cables of the simple-swap drive backplate assembly to the system board. See “Internal cable routing” on page 28.
2. Reinstall all the drives and drive fillers that you removed. See “Install a simple-swap drive” on page 78.
3. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Hot-swap drive replacement

Use this information to remove and install a hot-swap drive. You can remove or install a hot-swap drive without powering off the server, which helps you avoid significant interruption to the operation of the system.

Notes:

- The term “hot-swap drive” refers to all the supported types of hot-swap hard disk drives (HDDs) and hot-swap solid-state drives (SSDs).
- Use any documentation that comes with the drive and follow those instructions in addition to the instructions in this topic. Ensure that you have all the cables and other equipment that are specified in the documentation that comes with the drive.
- The electromagnetic interference (EMI) integrity and cooling of the server are protected by having all drive bays covered or occupied. The vacant bays are either covered by an EMI-protective panel or occupied by drive fillers. When installing a drive, save the removed drive filler in case that you later remove the drive and need the drive filler to cover the place.
- To avoid damage to the drive connectors, ensure that the top cover is in place and fully closed whenever you install or remove a drive.

Remove a hot-swap drive

Use this information to remove a hot-swap drive.



“**Read** the installation Guidelines” on page 41



“**ATTENTION:**
Static Sensitive Device
Ground package before opening” on page 43

Before removing a hot-swap drive:

1. Ensure that you have back up data on your drive, especially if it is part of a RAID array.
   - Before you make changes to drives, drive controllers, drive backplanes, or drive cables, back up all important data that is stored on the drives.
   - Before you remove any component of a RAID array, back up all RAID configuration information.
2. Remove the security bezel. See “Remove the security bezel” on page 48.

Attention: To ensure that there is adequate system cooling, do not operate the server for more than two minutes without either a drive or a drive filler installed in each bay.

To remove a hot-swap drive, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Slide the release latch to the left to open the drive tray handle.

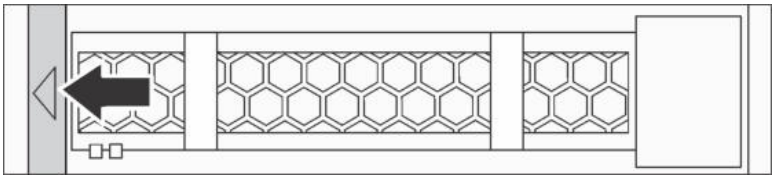


Figure 50. Opening the drive tray handle

Step 2. Grasp the handle and slide the drive out of the drive bay.

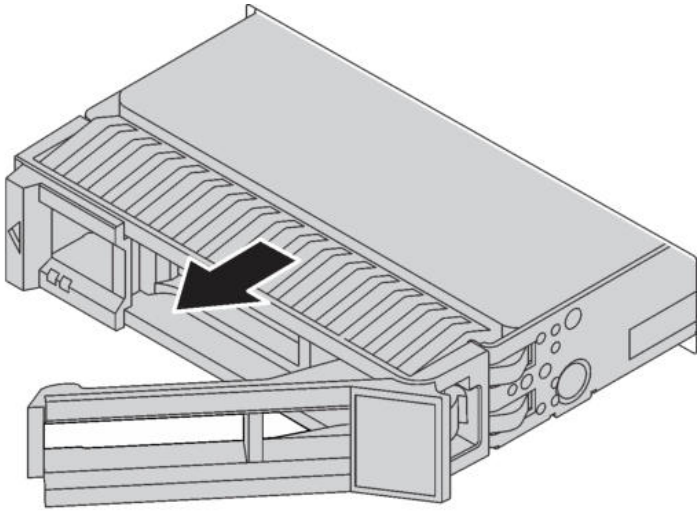


Figure 51. Sliding the drive out of the drive bay

Step 3. Install a drive filler or a new drive to cover the drive bay.

If you are instructed to return the old drive, follow all packaging instructions and use any packaging materials that are provided.

Install a hot-swap drive

Use this information to install a hot-swap drive.



"**Read** the installation Guidelines" on page 41



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Notes:

- For a list of supported drives, see http://www.lenovo.com/us/en/serverproven/.
- The drive bays are numbered to indicate the installation order (starting from number "0"). Follow the installation order when you install a drive. See "Front view" on page 13.
- You can mix drives of different types and different capacities in one system, but not in one RAID array. The following order is recommended when installing the drives:

  - Drive type priority: SAS SSD, SATA SSD, SAS HDD, SATA HDD
  - Drive capacity priority: the lowest capacity first
- The drives in a single RAID array must be the same type, same size, and same capacity.

Before installing a hot-swap drive:

1. If there is a drive filler installed, remove it and keep it in a safe place.
2. Touch the static-protective package that contains the new drive to any unpainted surface on the outside of the server. Then, take the new drive out of the package and place it on a static-protective surface.

To install a hot-swap drive, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

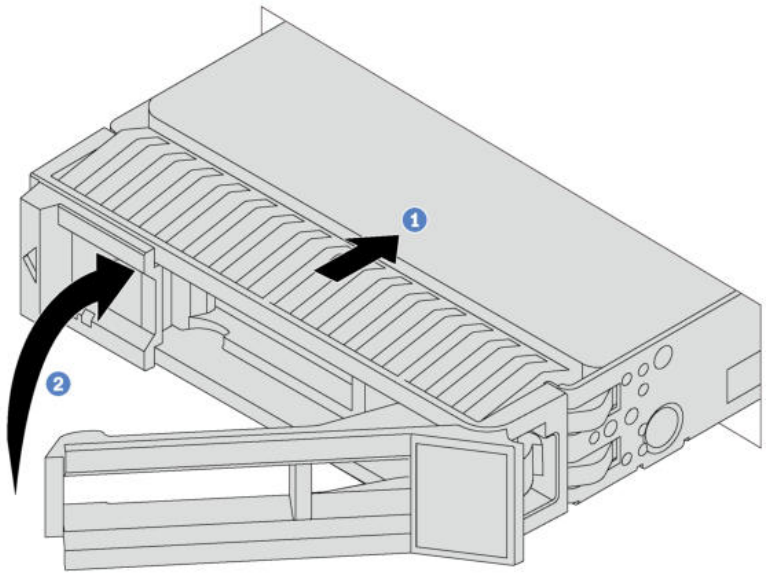


Figure 52. Hot-swap drive installation

Step 1. Ensure that the drive tray handle is in the open position. Slide the drive into the drive bay until it snaps into position.

Step 2. Close the drive tray handle to lock the drive in place.

Step 3. Check the drive status LED to verify that the drive is operating correctly.
- If the yellow drive status LED is lit continuously, that drive is faulty and must be replaced.
- If the green drive activity LED is flashing, the drive is being accessed.

Step 4. Continue to install additional hot-swap drives if necessary.

After installing all drives:

1. Reinstall the security bezel. See “Install the security bezel” on page 50.
2. Use the Lenovo XClarity Provisioning Manager to configure the RAID if necessary. For more information, see:

http://sysmgt.lenovofiles.com/help/topic/LXPM/RAID_setup.html

Simple-swap drive replacement

Use this information to remove and install a simple-swap drive.

Notes:

- The term “simple-swap drive” refers to all the supported types of simple-swap hard disk drives (HDDs) and simple-swap solid-state drives (SSDs).
- You must power off the server before installing or replacing a simple-swap drive.
- Use any documentation that comes with the drive and follow those instructions in addition to the instructions in this topic. Ensure that you have all the cables and other equipment that are specified in the documentation that comes with the drive.
- The electromagnetic interference (EMI) integrity and cooling of the server are protected by having all drive bays covered or occupied. The vacant bays are either covered by an EMI-protective panel or occupied by drive fillers. When installing a drive, save the removed drive filler in case that you later remove the drive and need the drive filler to cover the place.
- To avoid damage to the drive connectors, ensure that the top cover is in place and fully closed whenever you install or remove a drive.

Remove a simple-swap drive

Use this information to remove a simple-swap drive.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing a simple-swap drive:

1. Ensure that you have back up data on your drive, especially if it is part of a RAID array.
   - Before you make changes to drives, drive controllers, drive backplanes, or drive cables, back up all important data that is stored on the drives.
   - Before you remove any component of a RAID array, back up all RAID configuration information.
2. Remove the security bezel. See “Remove the security bezel” on page 48.

Attention: To make sure that there is adequate system cooling, do not operate the server for more than two minutes without either a drive or a drive filler installed in each bay.

To remove a simple-swap drive, complete the following steps:

Step 1. Use a screwdriver to unlock the handle lock 1. The handle opens automatically.

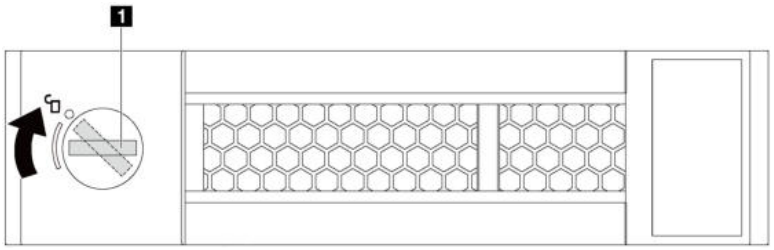


Figure 53. Opening the drive tray handle

Step 2. Grasp the handle and slide the drive out of the drive bay.

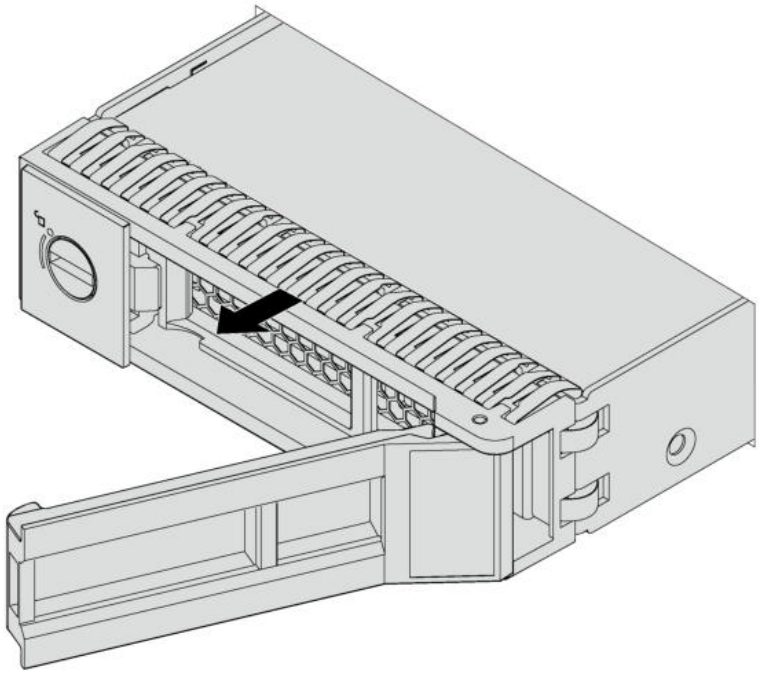


Figure 54. Sliding the drive out of the drive bay

Step 3. Install a drive filler or a new drive to cover the drive bay.

If you are instructed to return the old drive, follow all packaging instructions and use any packaging materials that are provided.

Install a simple-swap drive

Use this information to install a simple-swap drive.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Notes:

- For a list of supported drives, see http://www.lenovo.com/us/en/serverproven/.
- The drive bays are numbered to indicate the installation order (starting from number “0”). Follow the installation order when you install a drive. See “Front view” on page 13.
- You can mix drives of different types and different capacities in one system, but not in one RAID array. The following order is recommended when installing the drives:
  - Drive type priority: SATA SSD, SATA HDD
  - Drive capacity priority: the lowest capacity first
- The drives in a single RAID array must be the same type, same size, and same capacity.

Before installing a simple-swap drive:

1. If there is a drive filler installed, remove it and keep it in a safe place.
2. Touch the static-protective package that contains the new drive to any unpainted surface on the outside of the server. Then, take the new drive out of the package and place it on a static-protective surface.

To install a simple-swap drive, complete the following steps:

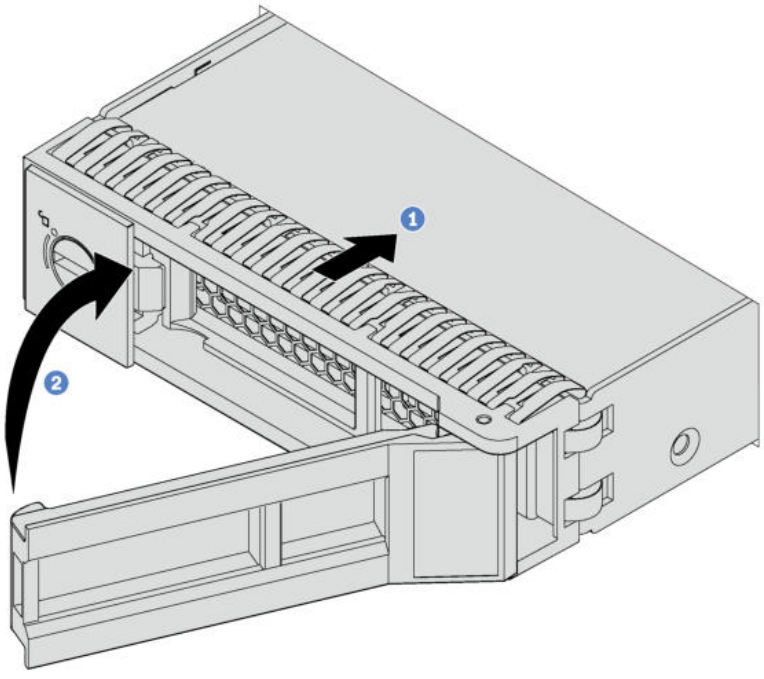


Figure 55. Simple-swap drive installation

Step 1. Ensure that the drive tray handle is in the open position. Slide the drive into the drive bay until it snaps into position.

Step 2. Close the drive tray handle to lock the drive in place.

Step 3. Continue to install additional simple-swap drives if necessary.

After you have installed all drives:

1. Reinstall the security bezel. See “Install the security bezel” on page 50.
2. Power on the server.
3. Use the Lenovo XClarity Provisioning Manager to configure the RAID if necessary. For more information, see:
   http://sysmgt.lenovofiles.com/help/topic/LXPM/RAID_setup.html

Memory module replacement

Use this information to remove and install a memory module.

Remove a memory module

Use this information to remove a memory module.



“**Read** the installation Guidelines” on page 41



“**Power off** the server for this task” on page 11



“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Attention:

- Disconnect all power cords for this task.
- Memory modules are sensitive to static discharge and require special handling. In addition to the standard guidelines for “Handling static-sensitive devices” on page 43:
  - Always wear an electrostatic-discharge strap when removing or installing memory modules. Electrostatic-discharge gloves can also be used.
  - Never hold two or more memory modules together so that they touch. Do not stack memory modules directly on top of each other during storage.
  - Never touch the gold memory module connector contacts or allow these contacts to touch the outside of the memory module connector housing.
  - Handle memory modules with care: never bend, twist, or drop a memory module.

Before removing a memory module:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Remove the air baffle. See “Remove the air baffle” on page 55.

To remove a memory module, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

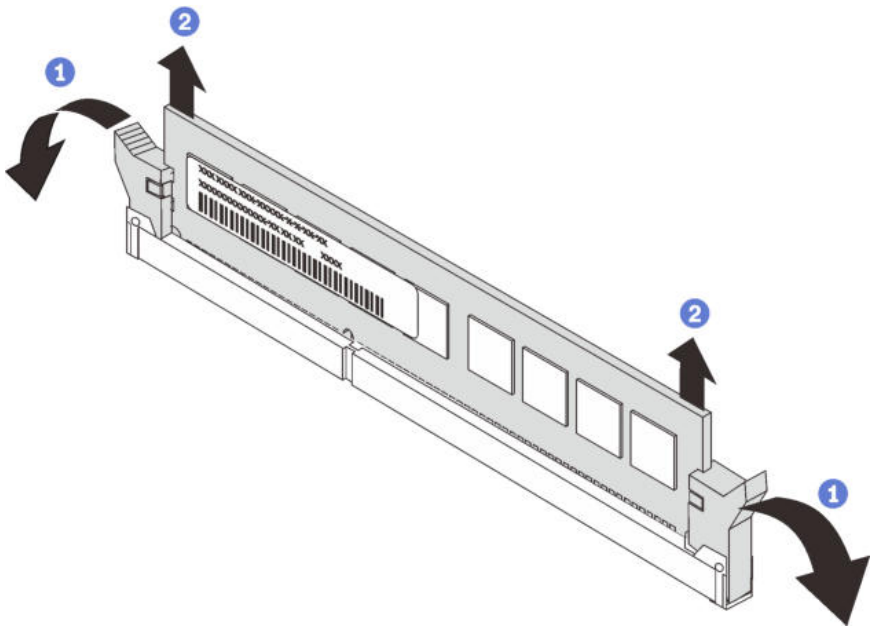


Figure 56. Memory module removal

Step 1. Open the retaining clips on each end of the memory module slot.

Attention: To avoid breaking the retaining clips or damaging the memory module slots, handle the clips gently.

Step 2. Grasp the memory module at both ends and carefully lift it out of the slot.

Step 3. Install a memory module filler or a new memory module to cover the slot.

If you are instructed to return the old memory module, follow all packaging instructions and use any packaging materials that are provided.

Memory module installation rules

Memory modules must be installed in a specific order based on the memory configuration that you implement on your server.

Your server supports up to 6 memory modules when one processor is installed, and up to 12 memory modules when two processors are installed. It supports the following types of memory modules depending on the processors installed:

For Intel Xeon SP Gen 1 processors

- Minimum: 8 GB
- Maximum:
  - 384 GB using registered DIMMs (RDIMMs)
  - 768 GB using load-reduced DIMMs (LRDIMMs)
- Type (depending on the model):
  - TruDDR4 2666, single-rank or dual-rank, 8 GB/16 GB/32 GB RDIMMs
  - TruDDR4 2666, quad-rank, 64 GB LRDIMMs
- Slots: 12 slots

For Intel Xeon SP Gen 2 processors

- Minimum: 8 GB
- Maximum: 768 GB
- Type (depending on the model):
  - TruDDR4 2666, single-rank or dual-rank, 16 GB/32 GB RDIMMs
  - TruDDR4 2933, single-rank or dual-rank, 8 GB/16 GB/32 GB/64 GB RDIMMs
- Slots: 12 slots

For a list of supported memory, see:
http://www.lenovo.com/us/en/serverproven/

Notes: Before installing a memory module, ensure that all memory modules to be installed must be the same type. Your server supports the following types of memory modules:

- DDR4 RDIMM with ECC technology
- DDR4 LRDIMM with ECC technology

The following illustration helps you to locate the memory module slots on the system board.

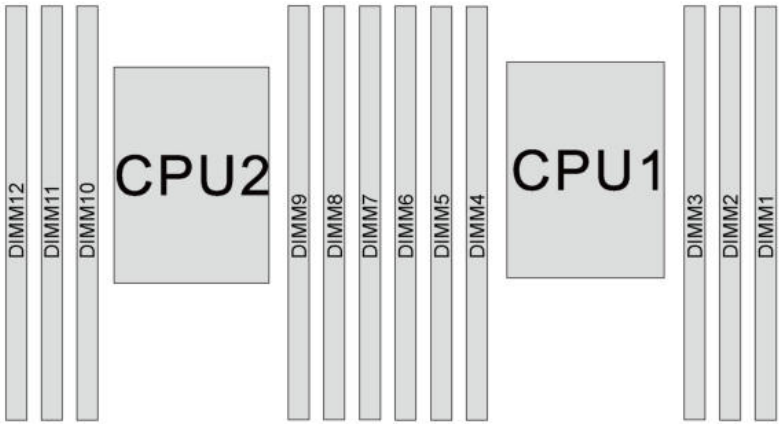


Figure 57. Memory module slots on the system board

The following memory configurations are available:
- “Independent mode” on page 81
- “Mirroring mode” on page 82
- “Rank sparing mode” on page 83

Independent mode

Independent mode provides high performance memory capability. You can populate all channels with no matching requirements. Individual channels can run at different memory module timings, but all channels must run at the same interface frequency.

The following table shows the memory module population sequence for independent mode when only one processor (CPU1) is installed.

Note: If there are three identical memory modules to be installed for CPU1, and the three memory modules have the same Lenovo part number, install the three memory modules in slots 1, 2, and 3.

Table 12. Independent mode with one processor

Total memory modules	Processor 1						Total memory modules
	6	5	4	3	2	1	
1				3			**1**
2			4	3			**2**
3			4	3	2		**3**
4		5	4	3	2		**4**
5		5	4	3	2	1	**5**
6	6	5	4	3	2	1	**6**

The following table shows the memory module population sequence for independent mode when two processors (CPU1 and CPU2) are installed.

Notes:

- If there are three identical memory modules to be installed for CPU1, and the three memory modules have the same Lenovo part number, install the three memory modules in slots 1, 2, and 3.
- If there are three identical memory modules to be installed for CPU2, and the three memory modules have the same Lenovo part numbers, install the three memory modules in slots 7, 8, and 9.

Table 13. Independent mode with two processors

Total memory modules	Processor 2						Processor 1						Total memory modules
	12	11	10	9	8	7	6	5	4	3	2	1	
2				9						3			**2**
3				9					4	3			**3**
4			10	9					4	3			**4**
5			10	9					4	3	2		**5**
6			10	9	8				4	3	2		**6**
7			10	9	8			5	4	3	2		**7**
8		11	10	9	8			5	4	3	2		**8**
9		11	10	9	8			5	4	3	2	1	**9**
10		11	10	9	8	7		5	4	3	2	1	**10**
11		11	10	9	8	7	6	5	4	3	2	1	**11**
12	12	11	10	9	8	7	6	5	4	3	2	1	**12**

Mirroring mode

In mirroring mode, each memory module in a pair must be identical in size and architecture. The channels are grouped in pairs with each channel receiving the same data. One channel is used as a backup of the other, which provides redundancy.

Note: All memory modules to be installed must be the same type with the same capacity, frequency, voltage, and rank.

The following table shows the memory module population sequence for mirroring mode when one processor (CPU1) is installed.

Table 14. Mirroring mode with one processor

Total memory modules	Processor 1						Total memory modules
	6	5	4	3	2	1	
2				3	2		**2**
3				3	2	1	**3**
4		5	4	3	2		**4**
6	6	5	4	3	2	1	**6**

The following table shows the memory module population sequence for mirroring mode when two processors (CPU1 and CPU2) are installed.

Table 15. Mirroring mode with two processors

Total memory modules	Processor 2						Processor 2						Total memory modules
	12	11	10	9	8	7	6	5	4	3	2	1	
4				9	8					3	2		**4**
5				9	8					3	2	1	**5**
6				9	8	7				3	2	1	**6**
8		11	10	9	8			5	4	3	2		**8**
9				9	8	7	6	5	4	3	2	1	**9**
10		11	10	9	8		6	5	4	3	2	1	**10**
12	12	11	10	9	8	7	6	5	4	3	2	1	**12**

Rank sparing mode

In rank sparing mode, one rank of a memory module works as the spare rank for the other ranks on the same channel. The spare rank is not available as system memory.

Notes:

- All memory modules to be installed must be the same type with the same capacity, frequency, voltage, and number of ranks.
- Single-rank memory modules do not support rank sparing mode.

Table 16. Rank sparing mode with one processor

Total memory modules	Processor 1						Total memory modules
	6	5	4	3	2	1	
1				3			**1**
2			4	3			**2**
3			4	3	2		**3**
4		5	4	3	2		**4**

Table 16. Rank sparing mode with one processor (continued)

Total memory modules	Processor 1						Total memory modules
	6	5	4	3	2	1	
5		5	4	3	2	1	**5**
6	6	5	4	3	2	1	**6**

The following table shows the memory module population sequence for rank sparing mode when two processors (CPU1 and CPU2) are installed.

Table 17. Rank sparing mode with two processors

Total memory modules	Processor 2						Processor 1						Total memory modules
	12	11	10	9	8	7	6	5	4	3	2	1	
2				9						3			**2**
3				9					4	3			**3**
4			10	9					4	3			**4**
5			10	9					4	3	2		**5**
6			10	9	8				4	3	2		**6**
7			10	9	8			5	4	3	2		**7**
8		11	10	9	8			5	4	3	2		**8**
9		11	10	9	8			5	4	3	2	1	**9**
10		11	10	9	8	7		5	4	3	2	1	**10**
11		11	10	9	8	7	6	5	4	3	2	1	**11**
12	12	11	10	9	8	7	6	5	4	3	2	1	**12**

Install a memory module

Use this information to install a memory module.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Attention:

- Disconnect all power cords for this task.
- Memory modules are sensitive to static discharge and require special handling. Refer to the standard guidelines for "Handling static-sensitive devices" on page 43:
  - Always wear an electrostatic-discharge strap when removing or installing memory modules. Electrostatic-discharge gloves can also be used.
  - Never hold two or more memory modules together so that they do not touch each other. Do not stack memory modules directly on top of each other during storage.
  - Never touch the gold memory module connector contacts or allow these contacts to touch the outside of the memory module connector housing.
  - Handle memory modules with care: never bend, twist, or drop a memory module.
  - Do not use any metal tools (such as jigs or clamps) to handle the memory modules, because the rigid metals may damage the memory modules.
  - Do not insert memory modules while holding packages or passive components, which can cause package cracks or detachment of passive components by the high insertion force.

Before installing a memory module:

1. Touch the static-protective package that contains the new memory module to any unpainted surface on the outside of the server. Then, take the new memory module out of the package and place it on a static-protective surface.
2. Locate the memory module slot on the system board by referring to "Memory module installation rules" on page 80. Ensure that you observe the installation rules and sequence.

To install a memory module, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

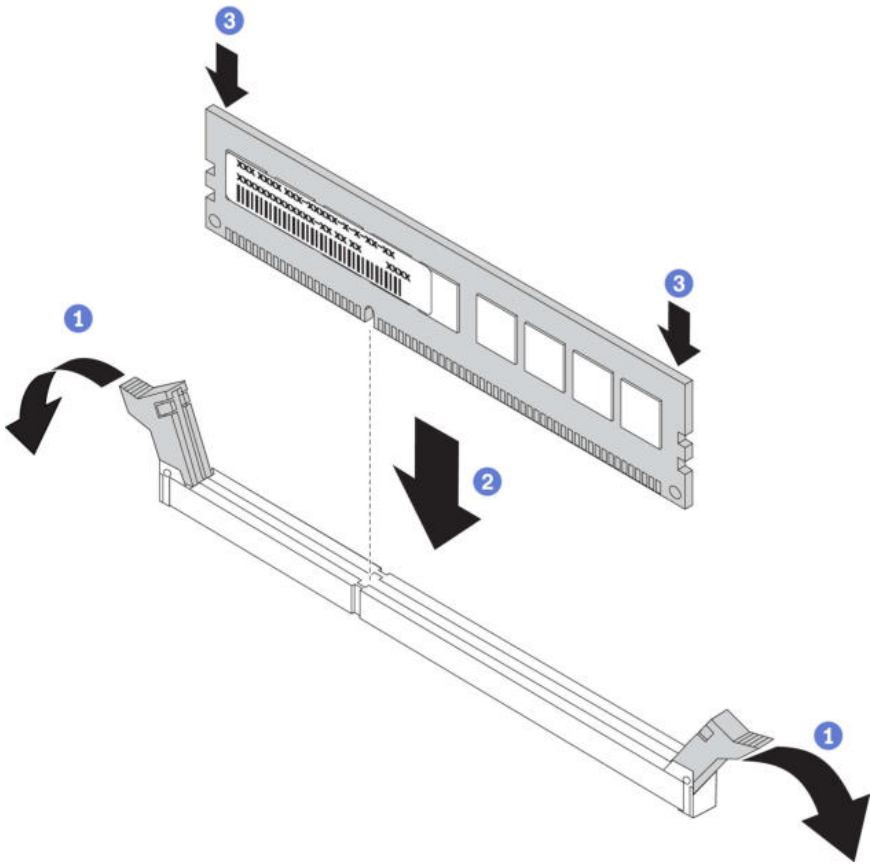


Figure 58. Memory module installation

Step 1. Open the retaining clips on each end of the memory module slot.

Attention: To avoid breaking the retaining clips or damaging the memory module slots, open and close the clips gently.

Step 2. Align the memory module with the slot, and gently place the memory module on the slot with both hands.

Step 3. Firmly press both ends of the memory module straight down into the slot until the retaining clips snap into the locked position.

Note: If there is a gap between the memory module and the retaining clips, the memory module has not been correctly inserted. In this case, open the retaining clips, remove the memory module, and then reinsert it.

After installing a memory module, complete the parts installation. See “Complete the parts replacement” on page 143.

CMOS battery replacement

Use this information to remove and install the CMOS battery.

Remove the CMOS battery

Use this information to remove the CMOS battery.

	"**Read** the installation Guidelines" on page 41	 "**Power off** the server for this task" on page 11	 "**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

The following tips describe information that you must consider when removing the CMOS battery.

- Lenovo has designed this product with your safety in mind. The lithium CMOS battery must be handled correctly to avoid possible danger. If you replace the CMOS battery, you must adhere to the following instructions.

  Note: In the U.S., call 1-800-IBM-4333 for information about battery disposal.
- If you replace the original lithium battery with a heavy-metal battery or a battery with heavy-metal components, be aware of the following environmental consideration. Batteries and accumulators that contain heavy metals must not be disposed of with normal domestic waste. They will be taken back free of charge by the manufacturer, distributor, or representative, to be recycled or disposed of in a proper manner.
- To order replacement batteries, call 1-800-IBM-SERV within the U.S., and 1-800-465-7999 or 1-800-465-6666 within Canada. Outside the U.S. and Canada, call your support center or business partner.

  Note: After you replace the CMOS battery, you must reconfigure the server and reset the system date and time.

S004



CAUTION:
When replacing the lithium battery, use only Lenovo specified part number or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of. *Do not:*

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

To remove the CMOS battery, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Remove the top cover. See “Remove the top cover” on page 52.

Step 2. Locate the CMOS battery, see “System board components” on page 23.

Step 3. Press the battery clip as shown and carefully lift CMOS battery out of the socket.

Attention: Do not tilt or push the CMOS battery using excessive force. Failing to remove the CMOS battery properly might damage the socket on the system board. Any damage to the socket might require replacing the system board.

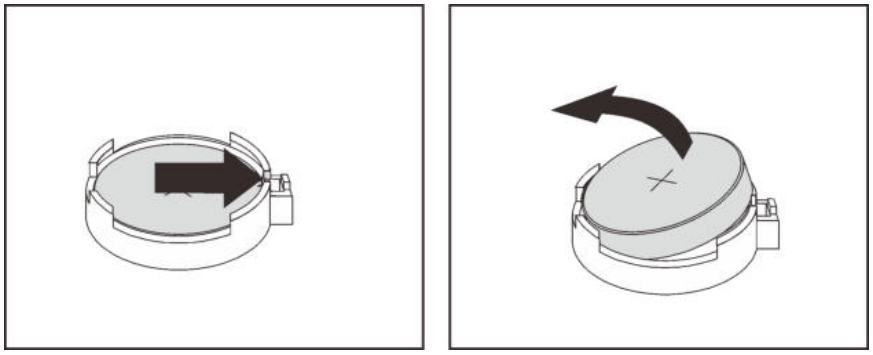


Figure 59. CMOS battery removal

After removing the CMOS battery:

1. Install a new CMOS battery.
2. Dispose of the CMOS battery as required by local ordinances or regulations.

Install the CMOS battery

Use this information to install the CMOS battery.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

The following tips describe information that you must consider when installing the CMOS battery.

- Lenovo has designed this product with your safety in mind. The lithium battery must be handled correctly to avoid possible danger. If you install the CMOS battery, you must adhere to the following instructions.

  Note: In the U. S., call 1-800-IBM-4333 for information about battery disposal.
- If you replace the original lithium battery with a heavy-metal battery or a battery with heavy-metal components, be aware of the following environmental consideration. Batteries and accumulators that contain heavy metals must not be disposed of with normal domestic waste. They will be taken back free of charge by the manufacturer, distributor, or representative, to be recycled or disposed of in a proper manner.
- To order replacement batteries, call 1-800-IBM-SERV within the U.S., and 1-800-465-7999 or 1-800-465-6666 within Canada. Outside the U.S. and Canada, call your support center or business partner.

  Note: After you install the CMOS battery, you must reconfigure the server and reset the system date and time.

S004



CAUTION:
When replacing the lithium battery, use only Lenovo specified part number or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of. *Do not:*

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To

remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

To install the CMOS battery, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Touch the static-protective package that contains the new CMOS battery to any unpainted surface on the outside of the server. Then, take the new CMOS battery out of the package and place it on a static-protective surface.

Step 2. Install the new CMOS battery. Ensure that the battery is seated in place.

Attention: Do not tilt or push the CMOS battery using excessive force. Any damage to the socket might require replacing the system board.

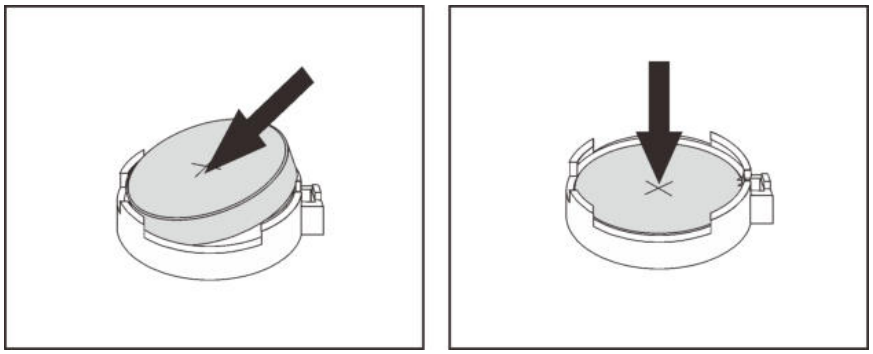


Figure 60. CMOS battery installation

After installing the CMOS battery:

1. Complete the parts installation. See “Complete the parts replacement” on page 143.
2. Use the Setup utility to set the date, time, and any passwords.

TCM/TPM adapter replacement (for Chinese Mainland only)

Use this information to remove and install the TCM/TPM adapter (sometimes called a daughter card).

Remove the TCM/TPM adapter (for Chinese Mainland only)

Use this information to remove the TCM/TPM adapter.

	“**Read** the installation Guidelines” on page 41	
	“**Power off** the server for this task” on page 11	
	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43	

To remove the TCM/TPM adapter, complete the following steps:

Step 1. Remove the top cover. See “Remove the top cover” on page 52.

Step 2. Locate the TCM/TPM connector on the system board, press the release latch on the TCM/TPM adapter, and lift it straight up.

Notes:

- Carefully handle the TCM/TPM adapter by its edges.
- Your TCM/TPM adapter might look slightly different from the illustration.

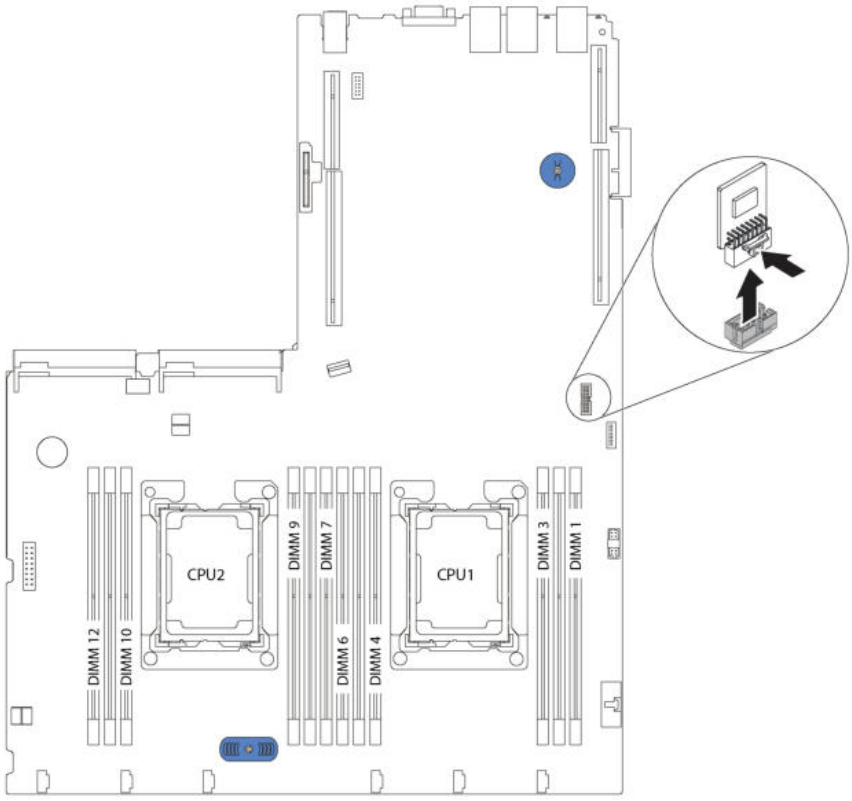


Figure 61. TCM/TPM adapter removal

If you are instructed to return the old TCM/TPM adapter, follow all packaging instructions and use any packaging materials that are provided.

Install the TCM/TPM adapter (for Chinese Mainland only)

Use this information to install the TCM/TPM adapter.

	"**Read** the installation Guidelines" on page 41	
	"**Power off** the server for this task" on page 11	
		"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before installing the TCM/TPM adapter, touch the static-protective package that contains the new TCM/TPM adapter to any unpainted surface on the outside of the server. Then, take the new TCM/TPM adapter out of the package and place it on a static-protective surface.

To install the TCM/TPM adapter, complete the following steps:

Step 1. Locate the TCM/TPM connector on the system board.

Step 2. Insert the TCM/TPM adapter into the TCM/TPM connector on the system board.

Notes:

- Carefully handle the TCM/TPM adapter by its edges.

- Your TCM/TPM adapter might look slightly different from the illustration.

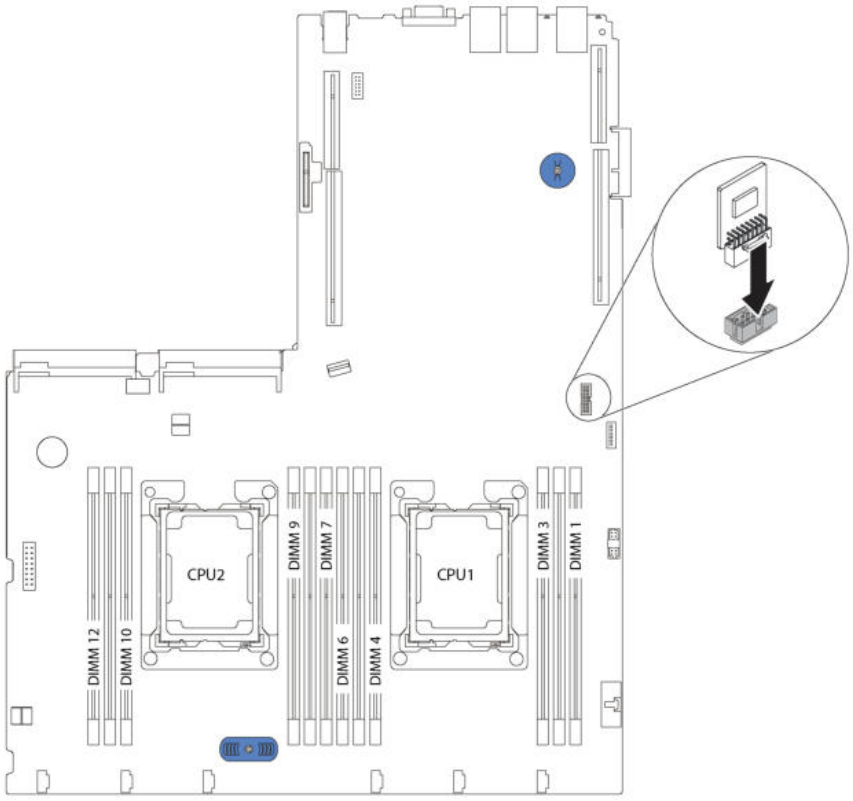


Figure 62. TCM/TPM adapter installation

After installing the TCM/TPM adapter, complete the parts replacement. See “Complete the parts replacement” on page 143.

Hot-swap power supply replacement

Use this information to remove and install the hot-swap power supply.

Remove a hot-swap power supply

Use this information to remove a hot-swap power supply.

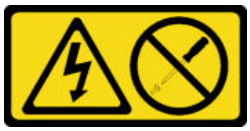


"**Read** the installation Guidelines" on page 41



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

S035



CAUTION:
Never remove the cover on a power supply or any part that has this label attached. Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

S001



DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect any equipment that will be attached to this product to properly wired outlets .**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	**To Disconnect:**
1. Turn everything OFF. 2. Attach all cables to devices. 3. Attach signal cables to connectors. 4. Attach power cords to outlet. 5. Turn device ON.	1. Turn everything OFF. 2. Remove power cords from outlet. 3. Remove signal cables from connectors. 4. Remove all cables from devices.



Figure 63. Hot-swap power supply label on the cover

Attention: This type of power supply is hot-swap only when two power supplies are installed for redundancy. If only one power supply is installed, you must power off the server before removing the power supply.

The following tips describe the information that you must consider when you remove a power supply with dc input.

CAUTION:

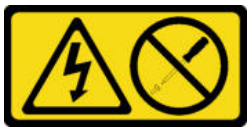
- **240 V dc input (input range: 180-300 V dc) is supported in Chinese Mainland ONLY. Power supply with 240 V dc input cannot support hot plugging power cord function. Before removing the power supply with dc input, please turn off server or disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the power cord.**
- **In order for the ThinkSystem products to operate error free in both a DC or AC electrical environment, a TN-S earthing system which complies to 60364-1 IEC 2005 standard has to be present or installed.**



在直流输入状态下，若电源供应器插座不支持热插拔功能，请务必不要对设备电源线进行热插拔。此操作可能导致设备损坏及数据丢失。因错误执行热插拔导致的设备故障或损坏，不属于保修范围。

NEVER CONNECT AND DISCONNECT THE POWER SUPPLY CABLE AND EQUIPMENT WHILE YOUR EQUIPMENT IS POWERED ON WITH DC SUPPLY (hot-plugging). Otherwise you may damage the equipment and result in data loss, the damages and losses result from incorrect operation of the equipment will not be covered by the manufacturers' warranty.

S035



CAUTION:
Never remove the cover on a power supply or any part that has this label attached. Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

S019



CAUTION:
The power-control button on the device does not turn off the electrical current supplied to the device. The device also might have more than one connection to dc power. To remove all electrical current from the device, ensure that all connections to dc power are disconnected at the dc power input terminals.

S029



DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded power source.**
- **Connect to properly wired power sources any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached ac power cords, dc power sources, network connections, telecommunications systems, and serial cables before you open the device covers, unless you are instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	**To Disconnect:**
1. Turn OFF all power sources and equipment that is to be attached to this product. 2. Attach signal cables to the product. 3. Attach power cords to the product. • For ac systems, use appliance inlets. • For dc systems, ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety. 4. Attach signal cables to other devices. 5. Connect power cords to their sources. 6. Turn ON all the power sources.	1. Turn OFF all power sources and equipment that is to be attached to this product. • For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit. • For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables. 2. Remove the signal cables from the connectors. 3. Remove all cables from the devices.

To remove a hot-swap power supply, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. If the server is in a rack, adjust the cable management arm (CMA) to gain access to the power supply.

If you have installed the 1U CMA Upgrade Kit for Toolless Slide Rail or Toolless Slide Rail Kit with 1U CMA, do the following:

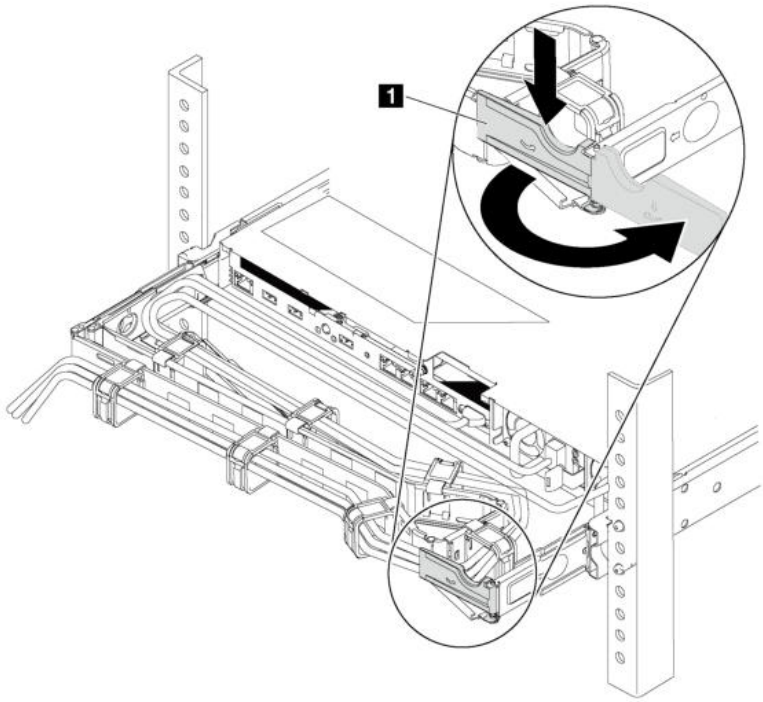


Figure 64. CMA adjustment

a. Press down the stop bracket 1 and rotate it to the open position.
b. Rotate the CMA out of the way to gain access to the power supply.

Step 2. Disconnect the power cord from the hot-swap power supply.

Note: If you are replacing two power supplies, do the power supply replacement one by one to ensure that the power supply to the server is not interrupted. Do not disconnect the power cord from the secondly replaced power supply until the power output LED for the firstly replaced power supply is lit. For the location of the power output LED, refer to “Rear view LEDs” on page 21.

Step 3. Press the release tab toward the handle and carefully pull the handle at the same time to slide the hot-swap power supply out of the chassis.

Notes: Slightly pull the power supply upwards when sliding the power supply out of the chassis, if you have installed one of the following CMA kits:

- 1U CMA Upgrade Kit for Toolless Slide Rail
- Toolless Slide Rail Kit with 1U CMA

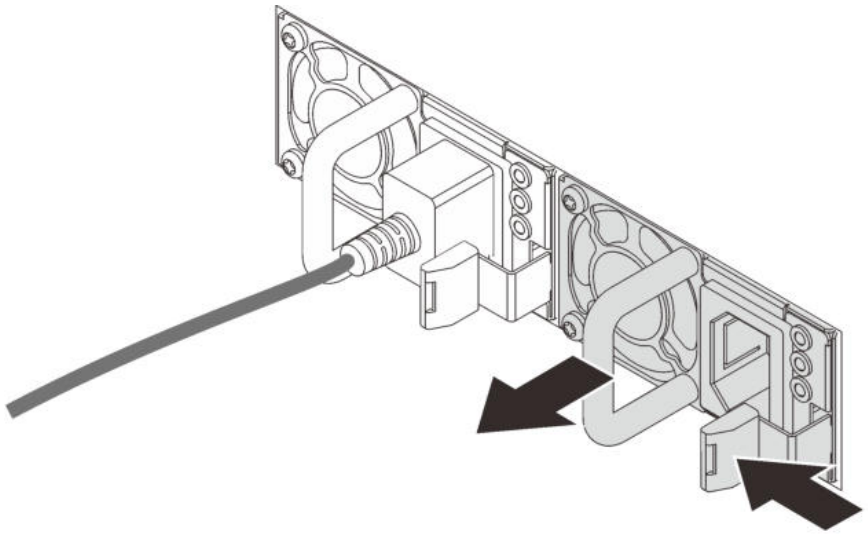


Figure 65. Hot-swap power supply removal

After removing the power supply:

- Install a power supply filler or a new power supply to cover the power supply bay.

  Important: To ensure proper cooling during normal server operation, both of the power supply bays must be occupied. This means that each bay must have a power supply installed; or one has a power supply installed and the other has a power supply filler installed.
- If you are instructed to return the old power supply, follow all packaging instructions and use any packaging materials that are provided.

Install a hot-swap power supply

Use this information to install a hot-swap power supply.

	“**Read** the installation Guidelines” on page 41
	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

The following tips describe the type of power supply that the server supports and other information that you must consider when you install a power supply:

- The standard shipping has only one power supply installed in the server. For redundancy and hot-swap support, you must install an additional hot-swap power supply. Certain customized models might be shipped with two power supplies installed.
- Ensure that the devices that you are installing are supported. For a list of supported optional devices for the server, go to:
  http://www.lenovo.com/us/en/serverproven/

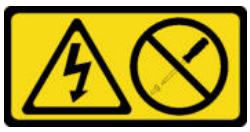
Notes:

- Ensure that the two power supplies installed on the server have the same wattage.
- If you are replacing the existing power supply with a new power supply of different wattage, attach the power rating label that comes with this option onto the existing label on the top cover near the power supply.



Figure 66. Hot-swap power supply label on the cover

S035



CAUTION:
Never remove the cover on a power supply or any part that has this label attached. Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

S002



CAUTION:

The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

S001



DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect any equipment that will be attached to this product to properly wired outlets .**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	**To Disconnect:**
1. Turn everything OFF. 2. Attach all cables to devices. 3. Attach signal cables to connectors. 4. Attach power cords to outlet. 5. Turn device ON.	1. Turn everything OFF. 2. Remove power cords from outlet. 3. Remove signal cables from connectors. 4. Remove all cables from devices.

The following tips describe the information that you must consider when you install a power supply with dc input.

CAUTION:

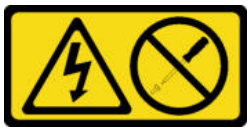
- **240 V dc input (input range: 180-300 V dc) is supported in Chinese Mainland ONLY. Power supply with 240 V dc input cannot support hot plugging power cord function. Before removing the power supply with dc input, please turn off server or disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the power cord.**
- **In order for the ThinkSystem products to operate error free in both a DC or AC electrical environment, a TN-S earthing system which complies to 60364-1 IEC 2005 standard has to be present or installed.**



在直流输入状态下，若电源供应器插座不支持热插拔功能，请务必不要对设备电源线进行热插拔。此操作可能导致设备损坏及数据丢失。因错误执行热插拔导致的设备故障或损坏，不属于保修范围。

NEVER CONNECT AND DISCONNECT THE POWER SUPPLY CABLE AND EQUIPMENT WHILE YOUR EQUIPMENT IS POWERED ON WITH DC SUPPLY (hot-plugging). Otherwise you may damage the equipment and result in data loss, the damages and losses result from incorrect operation of the equipment will not be covered by the manufacturers' warranty.

S035



CAUTION:
Never remove the cover on a power supply or any part that has this label attached. Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

S019



CAUTION:
The power-control button on the device does not turn off the electrical current supplied to the device. The device also might have more than one connection to dc power. To remove all electrical current from the device, ensure that all connections to dc power are disconnected at the dc power input terminals.

S029



DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded power source.**
- **Connect to properly wired power sources any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached ac power cords, dc power sources, network connections, telecommunications systems, and serial cables before you open the device covers, unless you are instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
2. Attach signal cables to the product.
3. Attach power cords to the product.
   - For ac systems, use appliance inlets.
   - For dc systems, ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety.
4. Attach signal cables to other devices.
5. Connect power cords to their sources.
6. Turn ON all the power sources.

To Disconnect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
   - For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.
   - For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.
2. Remove the signal cables from the connectors.
3. Remove all cables from the devices.

To install a hot-swap power supply, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Touch the static-protective package that contains the new power supply to any unpainted surface on the outside of the server. Then, take the new power supply out of the package and place it on a static-protective surface.

Step 2. If the server is in a rack, adjust the CMA to gain access to the power supply bay.

If you have installed the 1U CMA Upgrade Kit for Toolless Slide Rail or Toolless Slide Rail Kit with 1U CMA, do the following:

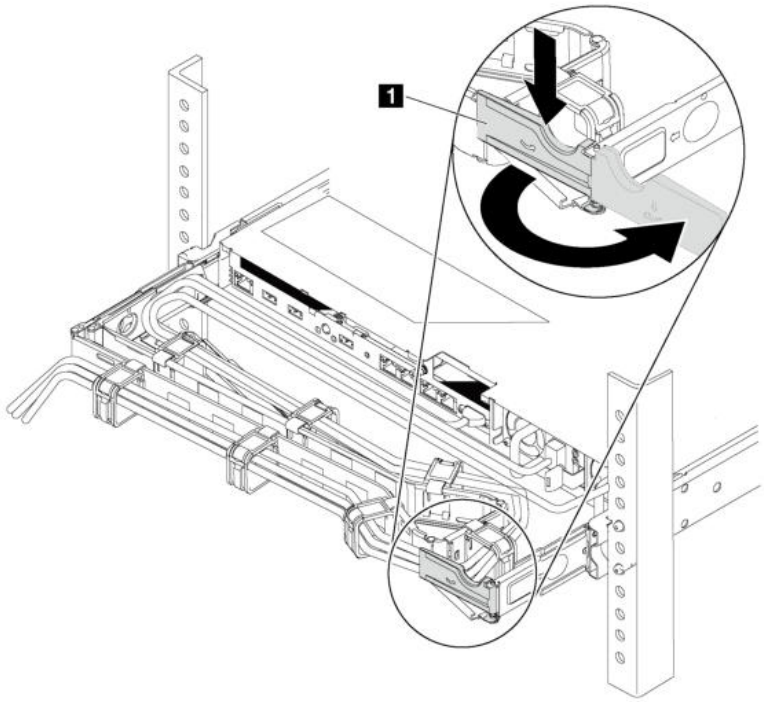


Figure 67. CMA adjustment

a. Press down the stop bracket 1 and rotate it to the open position.
b. Rotate the CMA out of the way to gain access to the power supply bay.

Step 3. If there is a power supply filler installed, remove it.

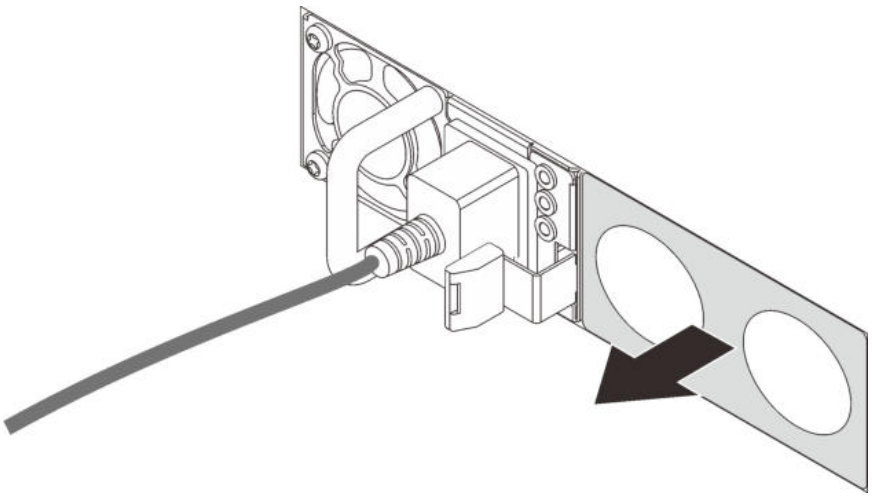


Figure 68. Hot-swap power supply filler removal

Step 4. Slide the new hot-swap power supply into the bay until the release latch clicks into place.

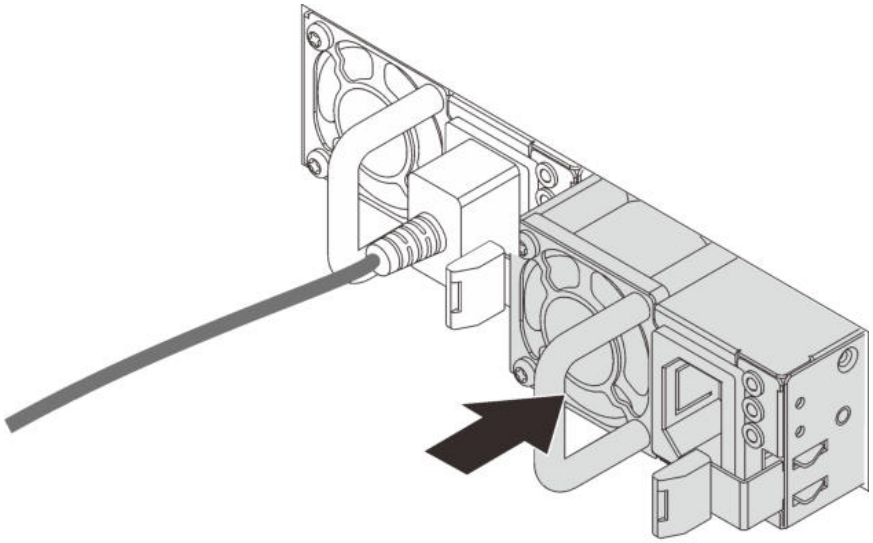


Figure 69. Hot-swap power supply installation

After installing the power supply:

1. Connect the power cord to the new power supply and ensure that it is connected to a properly grounded electrical outlet.
2. If the server is powered off, power on the server. Ensure that both the power input LED and the power output LED on the power supply are lit, indicating that the power supply is operating properly.

PCIe adapter replacement

Use this information to remove and install a PCIe adapter.

The PCIe adapter can be a host bus adapter (HBA), a PCIe RAID adapter, an Ethernet adapter, and any other supported PCIe adapters. For information about the PCIe slots and supported PCIe adapters, see “Rear view” on page 17.

Notes:

- Depending on the specific type, the PCIe adapter might look different from the illustrations in this topic.
- Use any documentation that comes with the PCIe adapter and follow those instructions in addition to the instructions in this topic.

Remove a PCIe adapter

Use this information to remove a PCIe adapter.



“**Read** the installation Guidelines” on page 41



“**Power off** the server for this task” on page 11



“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before removing a PCIe adapter:

1. Remove the top cover. See “Remove the top cover” on page 52.
2. Remove the riser assembly. See “Remove a riser adapter” on page 107.

To remove a PCIe adapter, complete the following steps:

Table 18. PCIe adapter removal

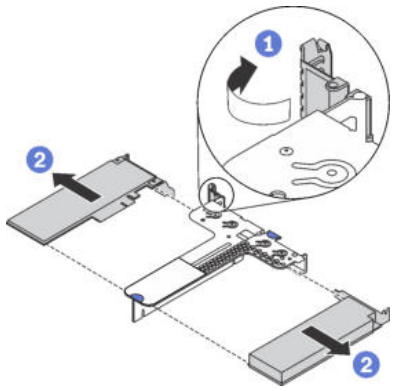


Figure 70. Riser 1 assembly (LP+LP)

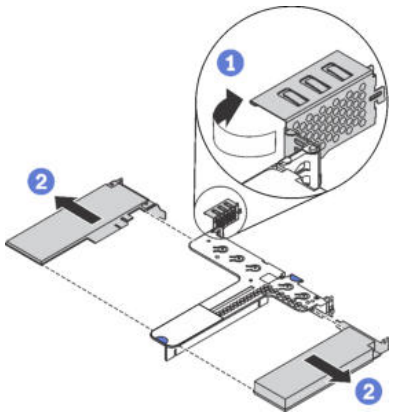


Figure 71. Riser 1 assembly (LP +FHHL)

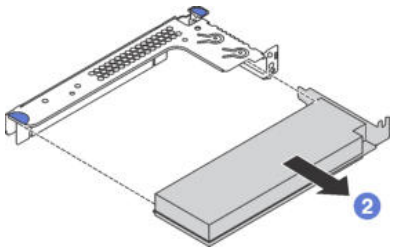


Figure 72. Riser 2 assembly (LP)

Step 1. (Skip this step for riser 2 assembly.) Pivot the latch on the riser bracket to the open position.

Step 2. Grasp the PCIe adapter by its edges and carefully pull it out of the PCIe slot on the riser card.

If you are instructed to return the old PCIe adapter, follow all packaging instructions and use any packaging materials that are provided.

Install a PCIe adapter

Use this information to install a PCIe adapter.

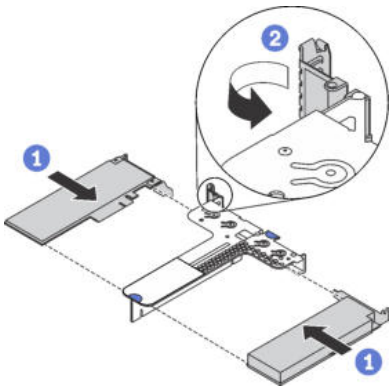
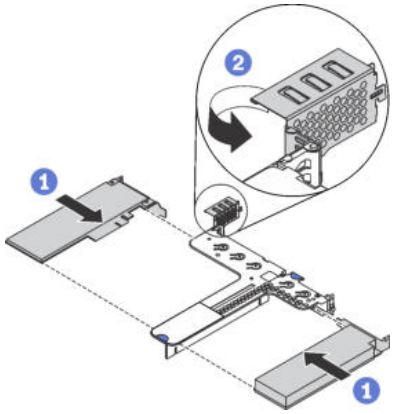
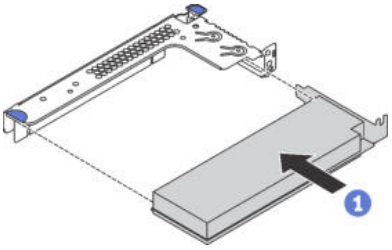
	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing a PCIe adapter,

1. Locate the correct PCIe slot for the PCIe adapter. For information about the PCIe slots and supported PCIe adapters, see “Rear view” on page 17.
2. Touch the static-protective package that contains the new PCIe adapter to any unpainted surface on the outside of the server. Then, take the new PCIe adapter out of the package and place it on a static-protective surface.

To install a PCIe adapter, complete the following steps:

Table 19. PCIe adapter installation

 *Figure 73. Riser 1 assembly (LP+LP)*	 *Figure 74. Riser 1 assembly (LP +FHHL)*	 *Figure 75. Riser 2 assembly (LP)*

Step 1. Align the PCIe adapter with the PCIe slot on the riser card. Then, carefully press the PCIe adapter straight into the slot until it is securely seated and its bracket also is secured.

Step 2. (Skip this step for riser 2 assembly.) Pivot the latch on the riser bracket to the closed position.

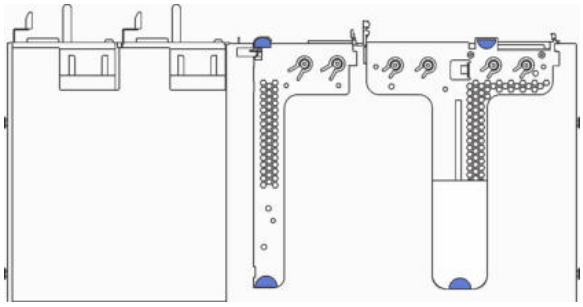
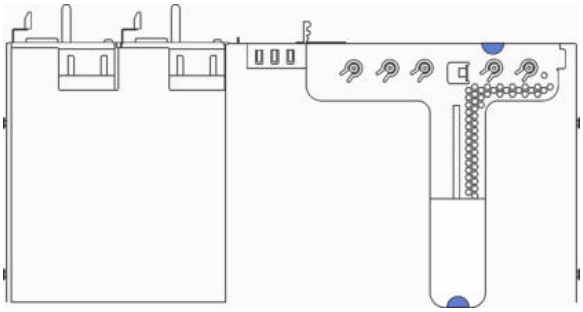
After installing the PCIe adapter:

1. Reinstall the riser assembly. See “Install a riser adapter” on page 109.
2. Complete the parts replacement. See “Complete the parts replacement” on page 143.

Riser card replacement

Use this information to remove and install a riser card.

Your server comes with one of the following riser assembly configurations:

Configuration 1	Configuration 2
 • Riser 1 assembly: LP + LP • Riser 2 assembly: LP (available on some models)	 • Riser 1 assembly: LP + FHHL

For information about the supported riser cards for each configuration, see “Rear view” on page 17.

There are three types of riser assemblies. The removal and installation procedure of the riser card is similar for all types of riser assemblies. The following procedures are based on the riser assembly in configuration 2.

Remove a riser card

Use this information to remove a riser card.

		
“**Read** the installation Guidelines” on page 41	“**Power off** the server for this task” on page 11	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

To remove a riser card, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Note: The riser assembly you want to remove might be different from the illustrations below, but the removal method is the same.

Step 1. Remove the top cover. See “Remove the top cover” on page 52.

Step 2. Grasp the riser assembly by its edges and carefully lift it up.

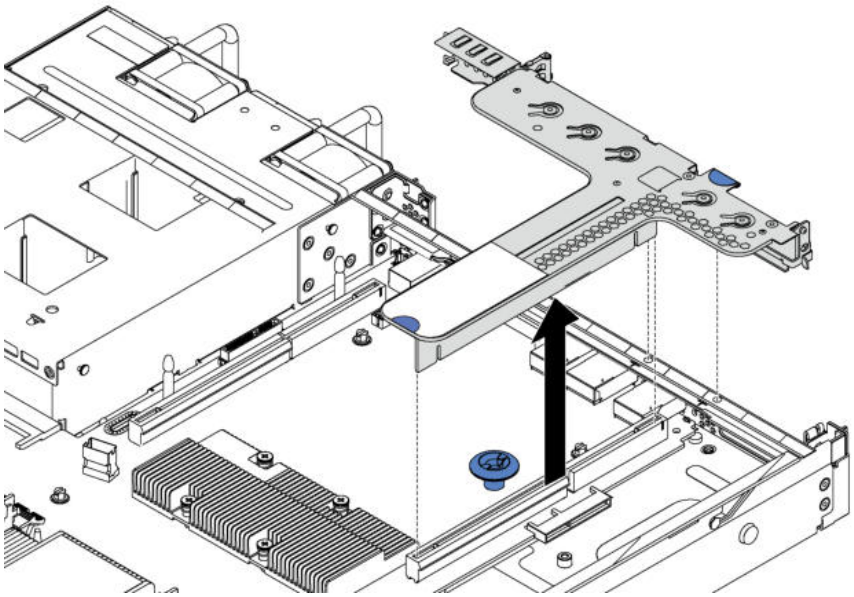


Figure 76. Riser assembly removal

Step 3. If there is any PCIe adapter installed on the riser card, record the cable connections first. Then, disconnect all cables from the PCIe adapter and completely remove the riser assembly out of the chassis.

Step 4. Remove the PCIe adapter that is installed on the riser card. See “Remove a PCIe adapter” on page 105.

Step 5. Remove the two screws that secure the riser card to the bracket. Then, remove the riser card.

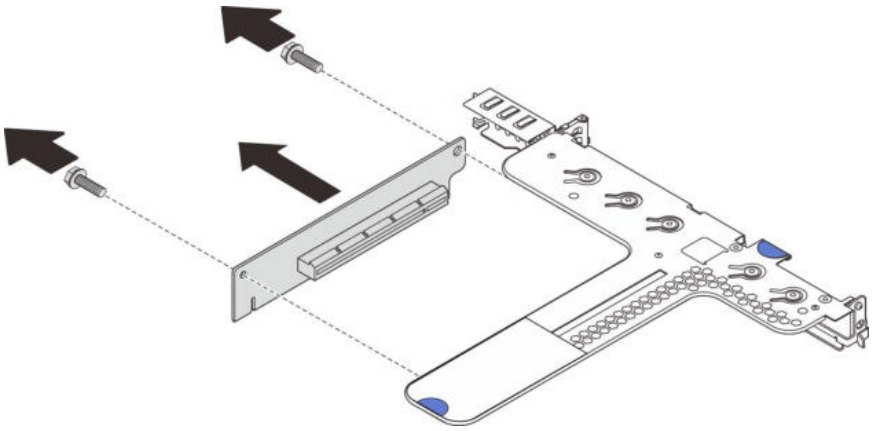


Figure 77. Riser card removal

If you are instructed to return the old riser card, follow all packaging instructions and use any packaging materials that are provided.

Install a riser card

Use this information to install a riser card.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

To install a riser card, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Note: The riser assembly you want to install might be different from the illustrations below, but the installation method is the same.

Step 1. Touch the static-protective package that contains the new riser card to any unpainted surface on the outside of the server. Then, take the new riser card out of the package and place it on a static-protective surface.

Step 2. Note the notch 1 on the riser card and ensure that the orientation of the riser card is correct as shown. Then, align the screw holes in the new riser card with the corresponding ones in the bracket and install the two screws to secure the riser card to the bracket.

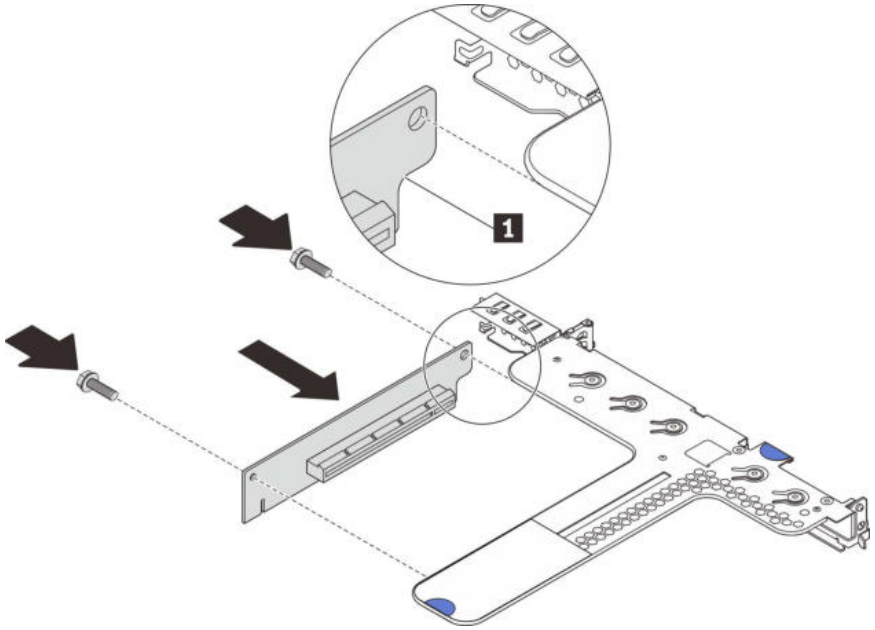


Figure 78. Riser card installation

Step 3. Install a PCIe adapter on the riser card. See “Install a PCIe adapter” on page 106.

Step 4. Connect cables to the PCIe adapter on the riser card. See “Internal cable routing” on page 28.

Step 5. Position the riser assembly on the chassis. Align the two pins on the bracket with the two holes in the chassis and align the riser card with the riser slot on the system board. Then, carefully press the riser assembly straight down into the slot until it is fully seated.

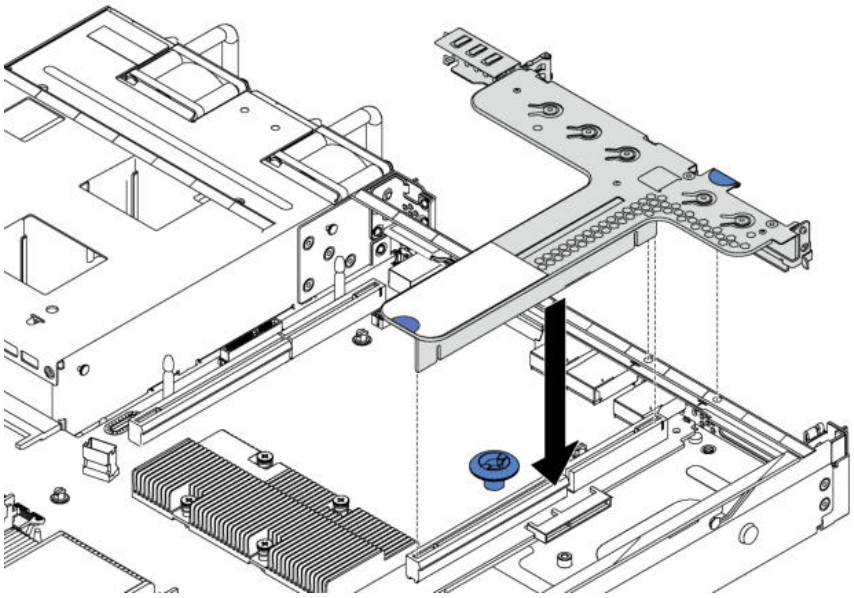


Figure 79. Riser assembly installation

After installing the riser card, complete the parts replacement. See “Complete the parts replacement” on page 143.

M.2 backplane and M.2 drive replacement

Use this information to remove and install the M.2 backplane and M.2 drive (an assembled M.2 backplane and M.2 drive is also known as M.2 module).

Remove the M.2 backplane and M.2 drive

Use this information to remove the M.2 backplane and M.2 drive.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the M.2 backplane and M.2 drive:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. For easier operation, remove the riser assembly next to the M.2 backplane. See "Remove a riser adapter" on page 107.

To remove the M.2 backplane and M.2 drive, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Grasp the M.2 backplane at both ends and pull it straight up to remove it from the system board.

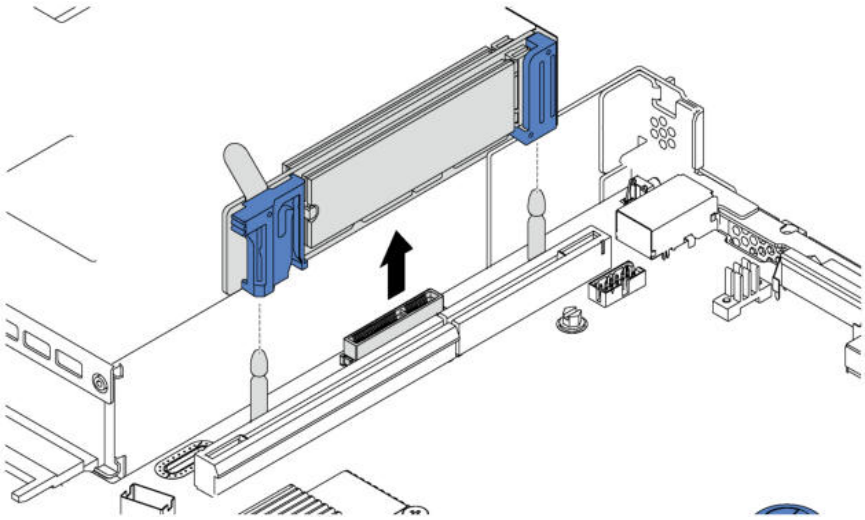


Figure 80. M.2 backplane removal

Step 2. Remove the M.2 drive from the M.2 backplane.

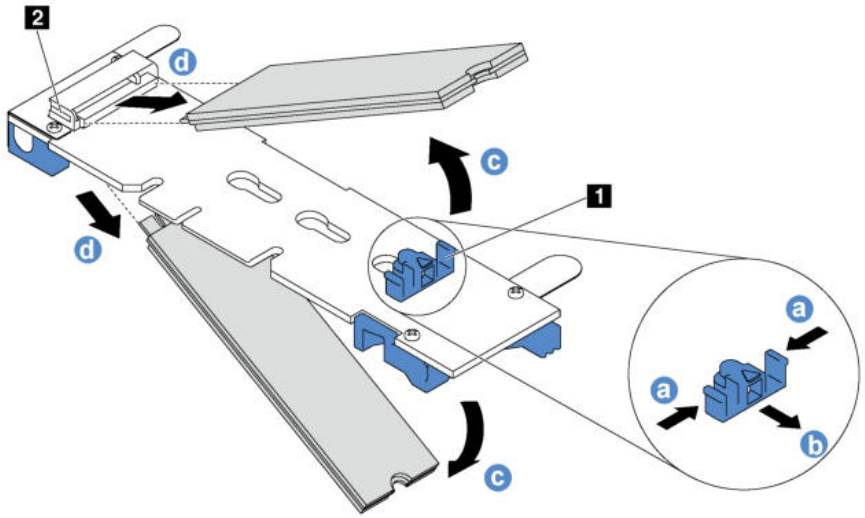


Figure 81. M.2 drive removal

a. Press both sides of the retainer **1**.
b. Slide the retainer backward to loosen the M.2 drive from the M.2 backplane.

   Note: If the M.2 backplane has two M.2 drives, they will both release outward when you slide the retainer backward.
c. Rotate the M.2 drive away from the M.2 backplane.
d. Pull it away from the connector **2** at an angle of approximately 30 degrees.

If you are instructed to return the old M.2 backplane or M.2 drive, follow all packaging instructions and use any packaging materials that are provided.

Adjust the retainer on the M.2 backplane

Use this information to adjust the retainer on the M.2 backplane.

Before adjusting the retainer on the M.2 backplane, locate the correct keyhole that the retainer should be installed into to accommodate the particular size of the M.2 drive you wish to install.

To adjust the retainer on the M.2 backplane, complete the following steps:

Watch the procedure. A video of the adjustment process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

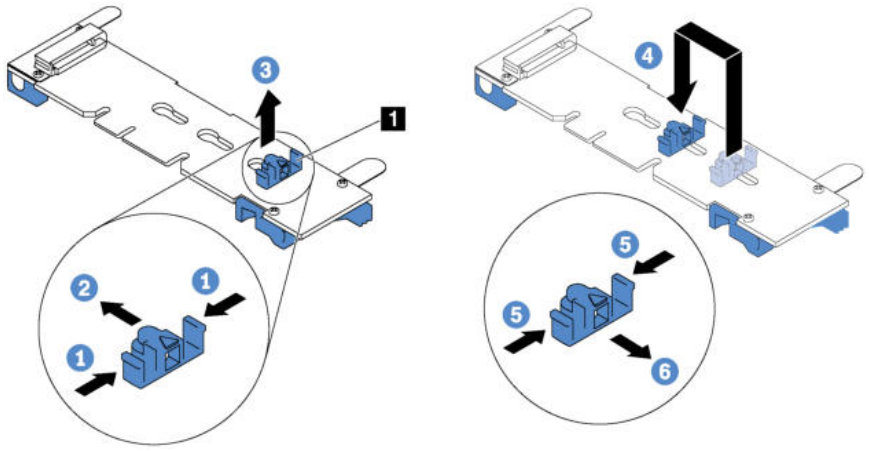


Figure 82. M.2 retainer adjustment

Step 1. Press both sides of the retainer **1**.

Step 2. Move the retainer forward until it is in the large opening of the keyhole.

Step 3. Take the retainer out of the keyhole.

Step 4. Insert the retainer into the correct keyhole.

Step 5. Press both sides of the retainer.

Step 6. Slide the retainer backwards until it is seated in place.

Install the M.2 backplane and M.2 drive

Use this information to install the M.2 backplane and M.2 drive.

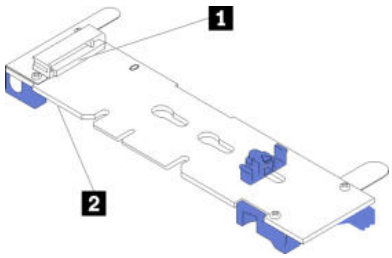
		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before installing the M.2 backplane and M.2 drive:

1. Touch the static-protective package that contains the new M.2 backplane and M.2 drive to any unpainted surface on the outside of the server. Then, take the new M.2 backplane and M.2 drive out of the package and place them on a static-protective surface.
2. Adjust the retainer on the M.2 backplane to accommodate the particular size of the M.2 drive you wish to install. See "Adjust the retainer on the M.2 backplane" on page 113.
3. Locate the connector on each side of the M.2 backplane.

   Notes:

   - Some M.2 backplanes support two identical M.2 drives. When two M.2 drives are installed, align and support both M.2 drives when sliding the retainer forward to secure the M.2 drives.
   - Install the M.2 drive in slot 0 first.



1 Slot 0
2 Slot 1

Figure 83. M.2 drive slot

To install the M.2 backplane and M.2 drive, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

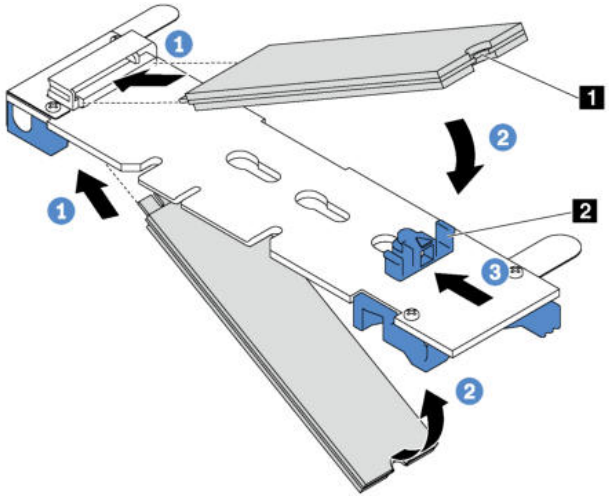


Figure 84. M.2 drive installation

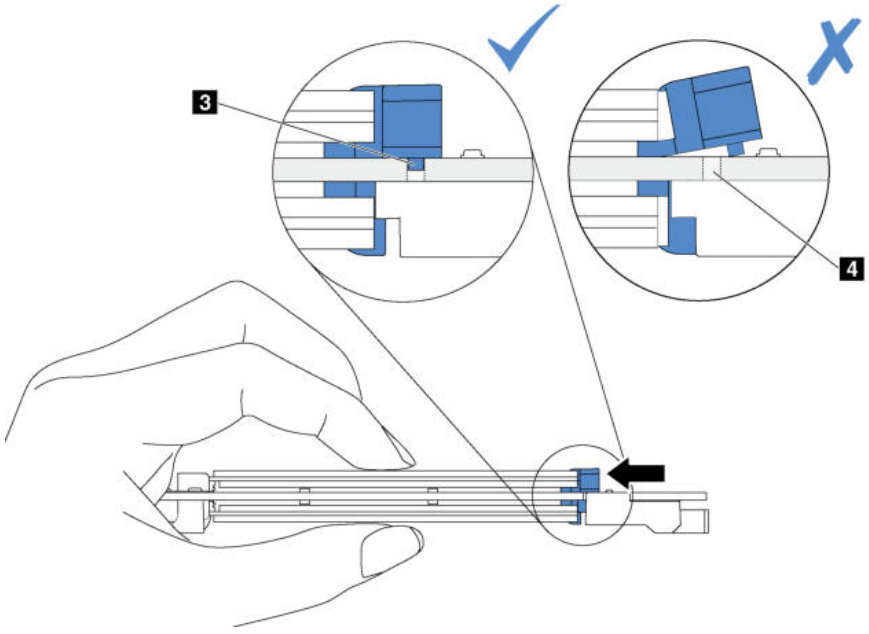
Step 1. Insert the M.2 drive at an angle of approximately 30 degrees into the connector.

Note: If your M.2 backplane supports two M.2 drives, insert the M.2 drives into the connectors at both sides.

Step 2. Rotate the M.2 drive down until the notch 1 catches on the lip of the retainer 2.

Step 3. Slide the retainer forward (toward the connector) to secure the M.2 drive into place.

Attention: When sliding the retainer forward, ensure that the two nubs 3 on the retainer enter the small holes 4 on the M.2 backplane. Once they enter the holes, you will hear a soft “click” sound.



Step 4. Align the blue plastic supports at each end of the M.2 backplane with the guide pins on the system board. Then, insert the M.2 backplane into the M.2 slot on the system board and press it down to fully seat it.

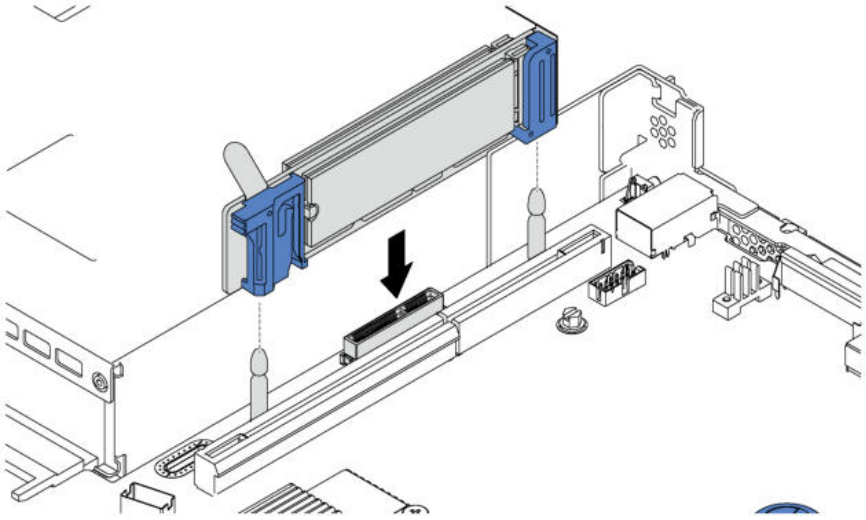


Figure 85. M.2 backplane installation

After installing the M.2 drive and M.2 backplane:

1. Reinstall the riser assembly next to the M.2 backplane. See “Install a riser adapter” on page 109.
2. Complete the parts replacement. See “Complete the parts replacement” on page 143.
3. Use the Lenovo XClarity Provisioning Manager to configure the RAID. For more information, see: http://sysmgt.lenovofiles.com/help/topic/LXPM/RAID_setup.html

Serial port module replacement

Use this information to remove and install the serial port module.

Note: The serial port module is available only on some models.

Remove the serial port module

Use this information to remove the serial port module.

		
"**Read** the installation Guidelines" on page 41	"**Power off** the server for this task" on page 11	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

To remove the serial port module, complete the following steps:

Note: The serial port module might be installed on riser 1 assembly or riser 2 assembly. The following steps are based on the scenario that the serial port module is installed on riser 2 assembly. The removal procedure is the same for the serial port module installed on riser 1 assembly.

Step 1. Remove the top cover. See "Remove the top cover" on page 52.

Step 2. Disconnect the cable of the serial port module from the system board.

Step 3. Grasp the riser 2 assembly with the serial port module and carefully lift the riser assembly out of the server.

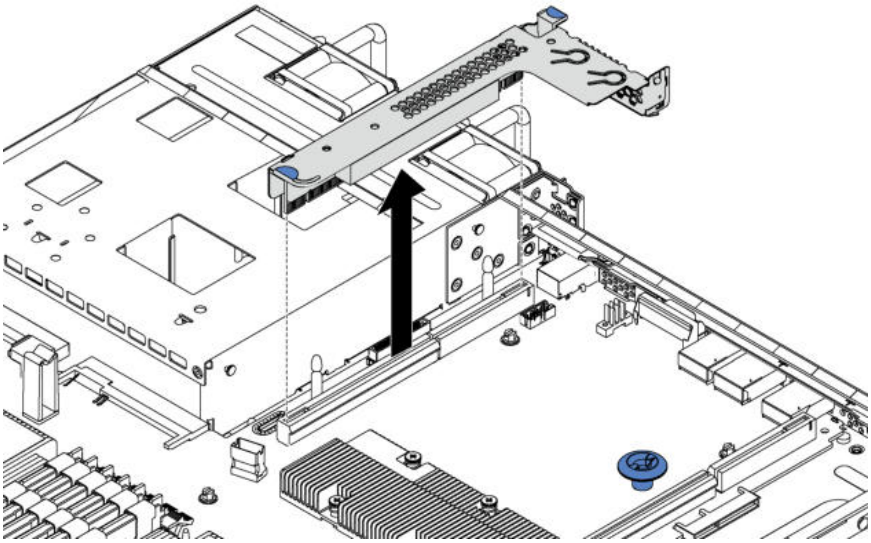


Figure 86. Riser assembly removal

Step 4. Slide the serial port module out of the bracket.

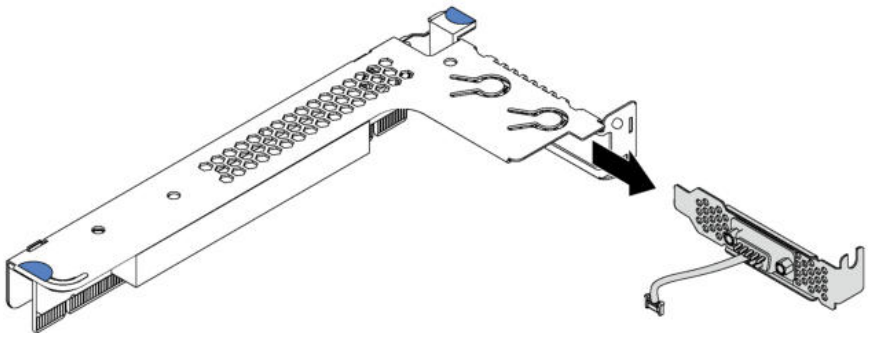


Figure 87. Serial port module removal

After removing the serial port module:

1. Install a new serial port module, a filler, or a PCIe adapter to cover the place.
2. If you are instructed to return the old serial port module, follow all packaging instructions and use any packaging materials that are provided.

Install the serial port module

Use this information to install the serial port module.

		
“**Read** the installation Guidelines” on page 41	“**Power off** the server for this task” on page 11	“**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the serial port module, touch the static-protective package that contains the new serial port module to any unpainted surface out of the server. Then, take the new serial port module out of the package and place it on a static-protective surface.

To install the serial port module, complete the following steps:

Note: The serial port module can be installed on riser 1 assembly or riser 2 assembly. The following steps are based on the scenario that the serial port module is to be installed on riser 2 assembly. The installation procedure is the same for the serial port module to be installed on riser 1 assembly.

Step 1. Locate the riser assembly and remove it from the server.

Step 2. If the riser assembly is covered with a PCIe slot bracket, remove the bracket first. Then, install the serial port module into the riser assembly.

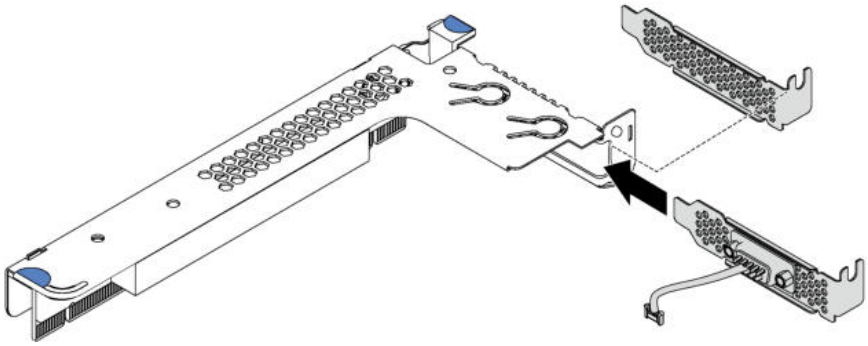


Figure 88. Serial port module installation

Step 3. Insert the riser assembly into the riser slot on the system board. Ensure that the riser assembly is fully seated.

Step 4. Connect the cable of the serial port module to serial-port-module connector on the system board. To locate the connector, see “System board components” on page 23. If the serial port module is installed in PCIe slot 1, route the cable of the serial port module as shown.

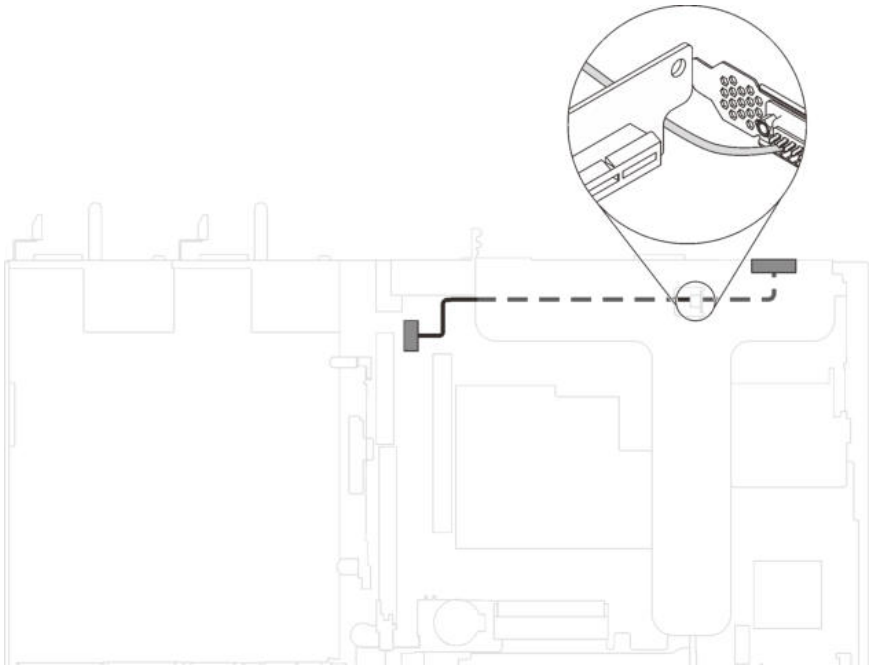


Figure 89. Cable routing for serial port module installed in PCIe slot 1

After installing the serial port module:

1. Complete the parts replacement. See “Complete the parts replacement” on page 143.
2. To enable the serial port module, do one of the following according to the installed operating system:
   - For Linux operating system:

     Open the ipmitool and enter the following command to disable the Serial over LAN (SOL) feature:

     ```
     -I lanplus -H IP -U USERID -P PASSWORD sol deactivate
     ```

   - For Microsoft Windows operating system:
     a. Open the ipmitool and enter the following command to disable the SOL feature:

        ```
        -I lanplus -H IP -U USERID -P PASSWORD sol deactivate
        ```

     b. Open Windows PowerShell and enter the following command to disable the Emergency Management Services (EMS) feature:

        ```
        Bcdedit /ems no
        ```

     c. Restart the server to ensure that the EMS setting takes effect.

LOM adapter replacement

Use this information to remove and install the LOM adapter.

Remove the LOM adapter

Use this information to remove the LOM adapter.

	"**Read** the installation Guidelines" on page 41	 "**Power off** the server for this task" on page 11	 "**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the LOM adapter:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. If riser 1 assembly is installed, remove it to access the LOM adapter slot.

To remove the LOM adapter, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

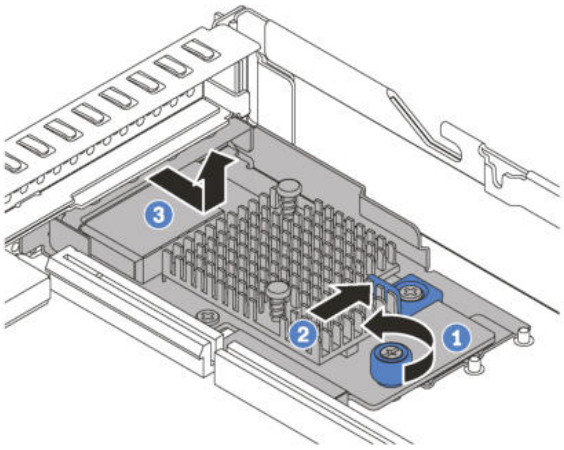


Figure 90. LOM adapter removal

Step 1. Loosen the thumbscrew that secures the LOM adapter.

Step 2. Push the LOM adapter out of the connector on the system board.

Step 3. Slide the LOM adapter as shown and lift the LOM adapter out of the chassis.

If you are instructed to return the old LOM adapter, follow all packaging instructions and use any packaging materials that are provided.

Install the LOM adapter

Use this information to install the LOM adapter.

	“**Read** the installation Guidelines” on page 41	 “**Power off** the server for this task” on page 11	 “**ATTENTION: Static Sensitive Device** Ground package before opening” on page 43

Before installing the LOM adapter:

1. If riser 1 assembly is installed, remove it to access the LOM adapter slot.
2. Touch the static-protective package that contains the new LOM adapter to any unpainted surface on the outside of the server. Then, take the new LOM adapter out of the package and place it on a static-protective surface.

To install the LOM adapter, complete the following steps:

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

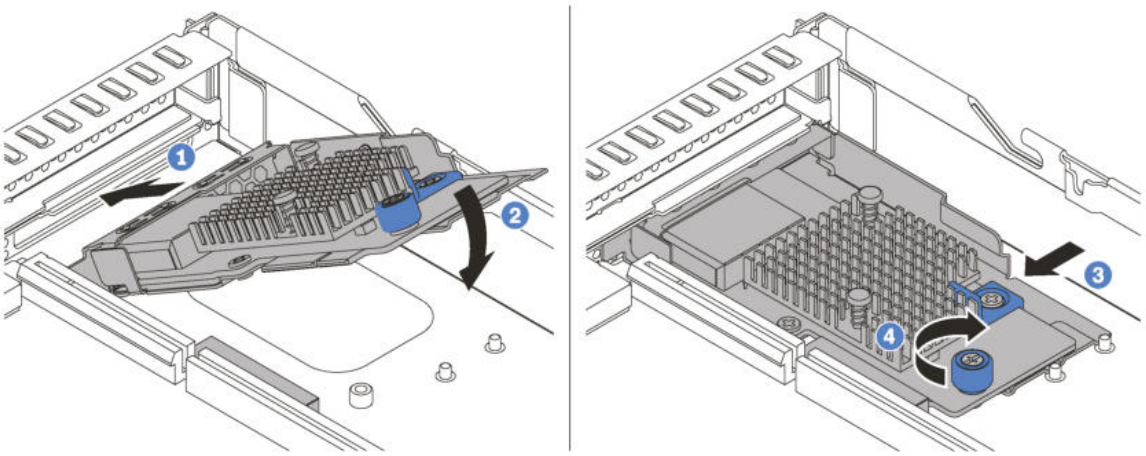


Figure 91. LOM adapter installation

Step 1. Insert the LOM adapter into the rear of the chassis at an angle as shown.

Step 2. Lower the LOM adapter and slide it to the rear of the chassis until the LOM adapter stops.

Step 3. Push the LOM adapter as shown to insert it into the connector on the system board.

Step 4. Tighten the thumbscrew to secure the LOM adapter.

After installing the LOM adapter, complete the parts replacement. See “Complete the parts replacement” on page 143.

Processor and heat sink replacement

Use the following procedures to replace an assembled processor and heat sink, known as a processor-heat-sink module (PHM), a processor, or a heat sink.

Attention:

- Before you begin replacing a processor, make sure that you have an alcohol cleaning pad (part number 00MP352) and gray thermal grease (part number 41Y9292).
- Cascade Lake processors are supported on the system board with part number 01PE840. If you use the system board with part number 00MX681, update your system firmware to the latest level before installing a Cascade Lake processor. Otherwise, the system cannot be powered on.

Important: The processor in your server can throttle, temporarily lowering speed to reduce heat output, in response to thermal conditions. In instances where the throttling period is of extremely short duration (100 ms or less), the only indication will be an entry in the event log. In these instances the event can be ignored and processor replacement is not required.

Remove a processor and heat sink

This task has instructions for removing an assembled processor and heat sink, known as a processor-heat-sink module (PHM), a processor, and a heat sink. All of these tasks require a Torx T30 driver.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Attention:

- Intel Xeon SP Gen 2 processors are supported on the system board with part number 01PE840. If you use the system board with part number 00MX681, update your system firmware to the latest level before installing a Intel Xeon SP Gen 2 processor. Otherwise, the system cannot be powered on.
- Each processor socket must always contain a cover or a PHM. When removing or installing a PHM, protect empty processor sockets with a cover.
- Do not touch the processor socket or processor contacts. Processor-socket contacts are very fragile and easily damaged. Contaminants on the processor contacts, such as oil from your skin, can cause connection failures.
- Remove and install only one PHM at a time. If the system board supports multiple processors, install the PHMs starting with the first processor socket.
- Do not allow the thermal grease on the processor or heat sink to come in contact with anything. Contact with any surface can compromise the thermal grease, rendering it ineffective. Thermal grease can damage components, such as electrical connectors in the processor socket. Do not remove the grease cover from a heat sink until you are instructed to do so.

Before you remove a PHM:

Note: The heat sink, processor, and processor retainer for your system might be different than those shown in the illustrations.

1. Remove the top cover. See "Remove the top cover" on page 52.
2. Remove the air baffle. See "Remove the air baffle" on page 55.
3. Remove any parts and disconnect any cables that might impede your access to the PHM.

Complete the following steps to remove a PHM.

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Remove the PHM from the system board.

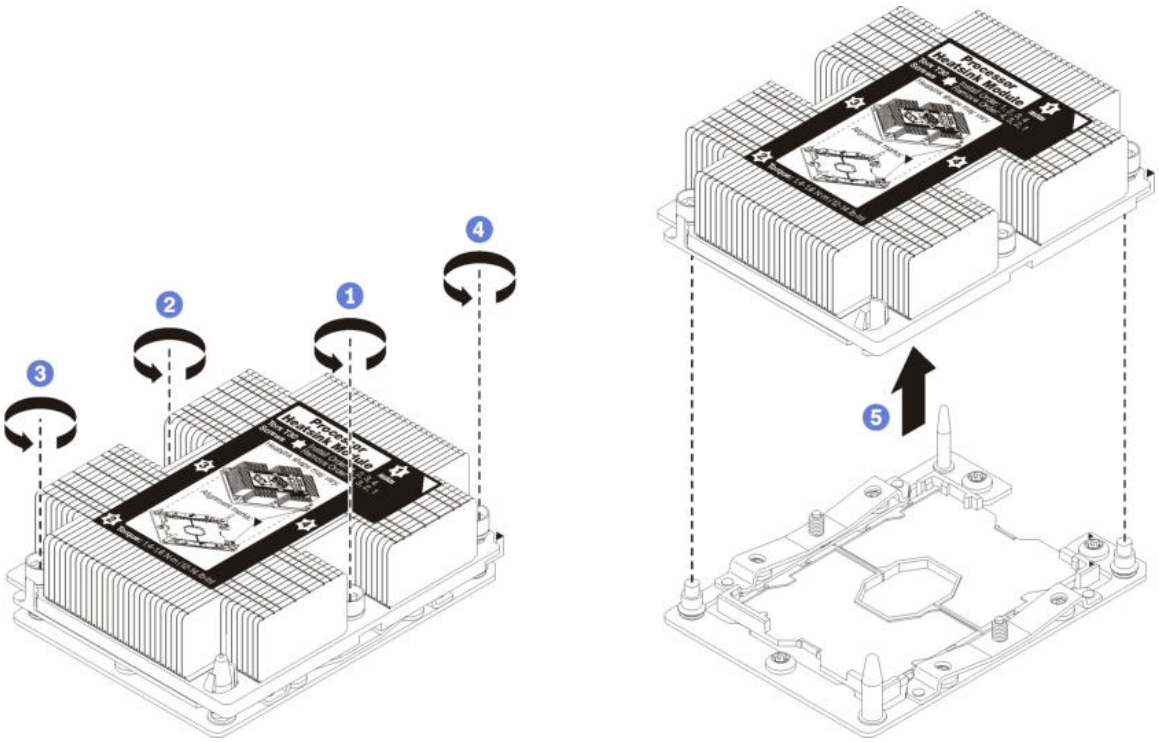


Figure 92. Removing a PHM

Attention: To prevent damage to components, make sure that you follow the indicated loosening sequence.

a. Fully loosen the Torx T30 captive fasteners on the processor-heat-sink module *in the removal sequence shown* on the heat-sink label.

b. Lift the processor-heat-sink module from the processor socket.

After you remove a PHM:

- If you are removing the PHM as part of a system board replacement, set the PHM aside.
- If you are replacing the processor or heat sink, separate the processor and its retainer from the heat sink.

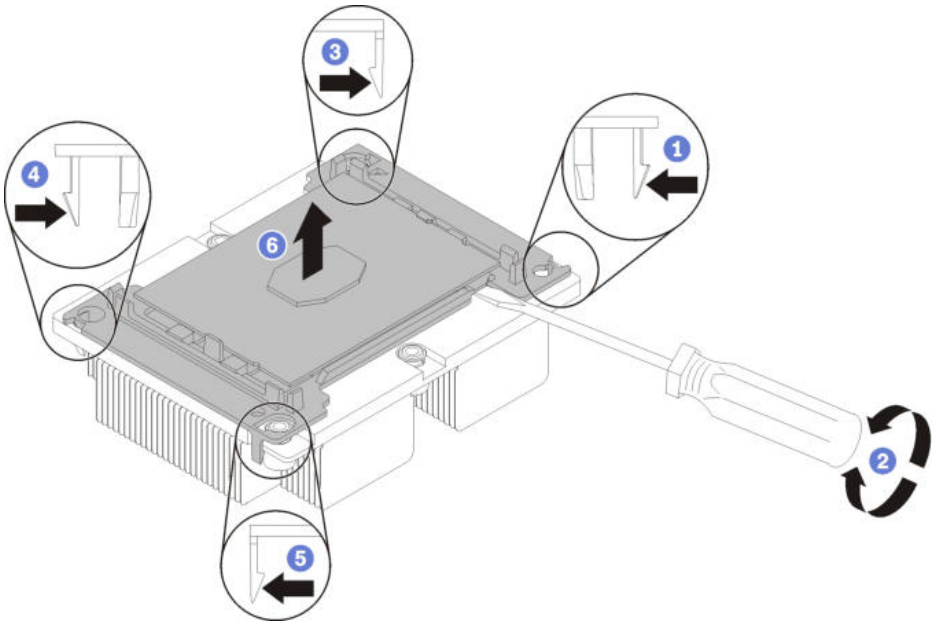


Figure 93. Separating a heat sink from a processor

1. Press the retaining clip at the corner of the processor retainer closest to the pry point; then, gently pry this corner of the retainer away from the heat sink with a flat-bladed screwdriver, using a twisting motion to break the processor-to-heat-sink seal.
2. Release the remaining retaining clips and lift the processor and retainer from the heat sink.
3. After separating the processor and retainer from the heat sink, hold the processor and retainer with the thermal-grease side down and the processor-contact side up to prevent the processor from falling out of the retainer.

   Note: The processor retainer will be removed and discarded in a later step and replaced with a new one.

- If you are replacing the processor, you will be reusing the heat sink. Wipe the thermal grease from the bottom of the heat sink using an alcohol cleaning pad.
- If you are replacing the heat sink, you will be reusing the processor. Wipe the thermal grease from the top of the processor using an alcohol cleaning pad.

If you are instructed to return the processor or heat sink, follow all packaging instructions and use any packaging materials that are provided.

Install a processor and heat sink

This task has instructions for installing an assembled processor and heat sink, known as a processor-heat-sink module (PHM), a processor, and a heat sink. All of these tasks require a Torx T30 driver.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Attention:

- Intel Xeon SP Gen 2 processors are supported on the system board with part number 01PE840. If you use the system board with part number 00MX681, update your system firmware to the latest level before installing a Intel Xeon SP Gen 2 processor. Otherwise, the system cannot be powered on.
- Each processor socket must always contain a cover or a PHM. When removing or installing a PHM, protect empty processor sockets with a cover.
- Do not touch the processor socket or processor contacts. Processor-socket contacts are very fragile and easily damaged. Contaminants on the processor contacts, such as oil from your skin, can cause connection failures.
- Remove and install only one PHM at a time. If the system board supports multiple processors, install the PHMs starting with the first processor socket.
- Do not allow the thermal grease on the processor or heat sink to come in contact with anything. Contact with any surface can compromise the thermal grease, rendering it ineffective. Thermal grease can damage components, such as electrical connectors in the processor socket. Do not remove the grease cover from a heat sink until you are instructed to do so.

Notes:

- PHMs are keyed for the socket where they can be installed and for their orientation in the socket.
- See http://www.lenovo.com/us/en/serverproven/ for a list of processors supported for your server. All processors on the system board must have the same speed, number of cores, and frequency.
- If you are going to install one of the following processors, replace your heat sink with a heat pipe heat sink (part number: 01KP650 or 01KP651):
  - Intel Xeon Platinum 8156 4C 105W 3.6 GHz processor
  - Intel Xeon Platinum 8256 4C 105W 3.8 GHz processor
  - Intel Xeon Gold 5120T 14C 105W 2.2 GHz processor
  - Intel Xeon Gold 5122 4C 105W 3.6 GHz processor
  - Intel Xeon Gold 5217 8C 115W 3.0 GHz processor
  - Intel Xeon Gold 5218T 16C 105W 2.1GHz processor
  - Intel Xeon Gold 5220T 18C 105W 2.2 GHz processor
  - Intel Xeon Gold 5222 4C 105W 3.8 GHz processor
  - Intel Xeon Gold 6126T 12C 125W 2.6 GHz processor
  - Intel Xeon Gold 6128 6C 115W 3.4 GHz processor
  - Intel Xeon Gold 6130T 16C 125W 2.1 GHz processor
  - Intel Xeon Gold 6138T 20C 125W 2.0 GHz processor
  - Intel Xeon Gold 6230N 20C 125W 2.3 GHz processor
  - Intel Xeon Gold 6230T 20C 125W 2.1 GHz processor
  - Intel Xeon Gold 6238T 22C 125W 1.9 GHz processor

- Before you install a new PHM or replacement processor, update your system firmware to the latest level. See “Firmware updates” on page 7.
- Installing an additional PHM can change the memory requirements for your system. See “Memory module installation rules” on page 80 for a list of processor-to-memory relationships.
- Optional devices available for your system might have specific processor requirements. See the documentation that comes with the optional device for information.

Before you install a PHM:

Note: The heat sink, processor, and processor retainer for your system might be different than those shown in the illustrations.

1. Remove the existing PHM, if one is installed. See “Remove a processor and heat sink” on page 123.

   Note: Replacement processors come with both rectangular and square processor retainers. A rectangular retainer comes attached to the processor. The square retainer can be discarded.

2. If you are replacing a heat sink, replace the processor retainer. *Processor retainers should not be reused.*
   a. Remove the old processor retainer.

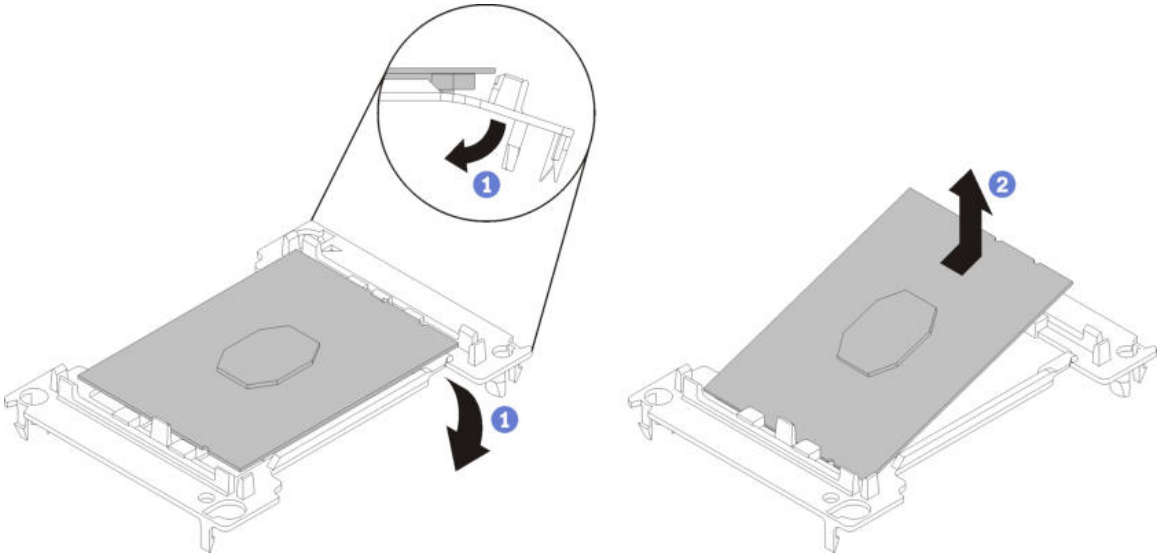


Figure 94. Removing a processor retainer

Note: When the processor is out of its retainer, hold the processor by the long edges to prevent touching the contacts or the thermal grease, if it is applied.

With the processor-contact side up, flex the ends of the retainer down and away from the processor to release the retaining clips; then, remove the processor from the retainer. Discard the old retainer.

   b. Install a new processor retainer.

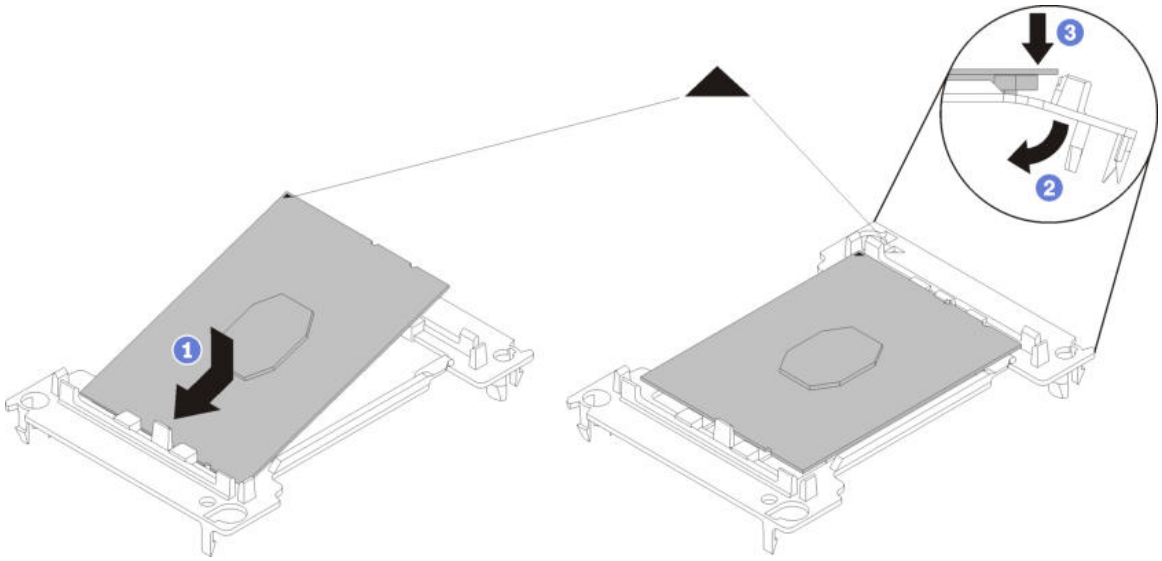


Figure 95. Installing a processor retainer

1) Position the processor on the new retainer so that the triangular marks align; then, insert the unmarked end of the processor into the retainer.
2) Holding the inserted end of the processor in place, flex the opposite end of the retainer down and away from the processor until you can press the processor under the clip on the retainer.

   To prevent the processor from falling out of the retainer after it is inserted, keep the processor-contact side up and hold the processor-retainer assembly by the sides of the retainer.
3) If there is any old thermal grease on the processor, gently clean the top of the processor using an alcohol cleaning pad.

   Note: If you are applying new thermal grease on the top of the processor, make sure to do it after the alcohol has fully evaporated.

3. If you are replacing a processor:
   a. Remove the processor identification label from the heat sink and replace it with the new label that comes with the replacement processor.
   b. Apply the new thermal grease on the top of the new processor with syringe by forming four uniformly spaced dots, while each dot consists of about 0.1 ml of thermal grease.

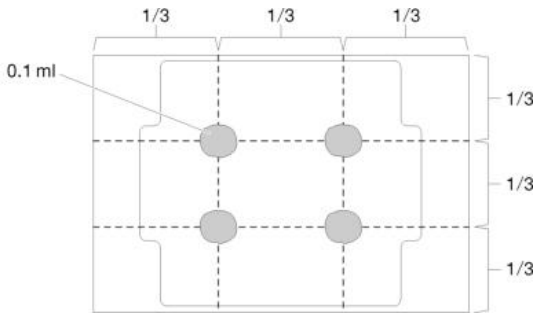


Figure 96. Proper shape of the thermal grease

4. If you are replacing a heat sink, remove the processor identification label from the old heat sink and place it on the new heat sink in the same location. The label is on the side of the heat sink closet to the triangular alignment mark.

If you are unable to remove the label and place it on the new heat sink, or if the label is damaged during transfer, write the processor serial number from the processor identification label on the new heat sink in the same location as the label would be placed using a permanent marker.

5. Assemble the processor and heat sink, if these components are separate.

   Notes:

   - If you are replacing a processor, install the heat sink onto the processor and retainer while the processor and retainer are in the shipping tray.
   - If you are replacing a heat sink, remove the heat sink from its shipping tray and place the processor and retainer in the opposite half of the heat sink shipping tray with the processor-contact side down. To prevent the processor from falling out of the retainer, hold the processor-retainer assembly by its sides with the processor-contact side up until you turn it over to fit in the shipping tray.

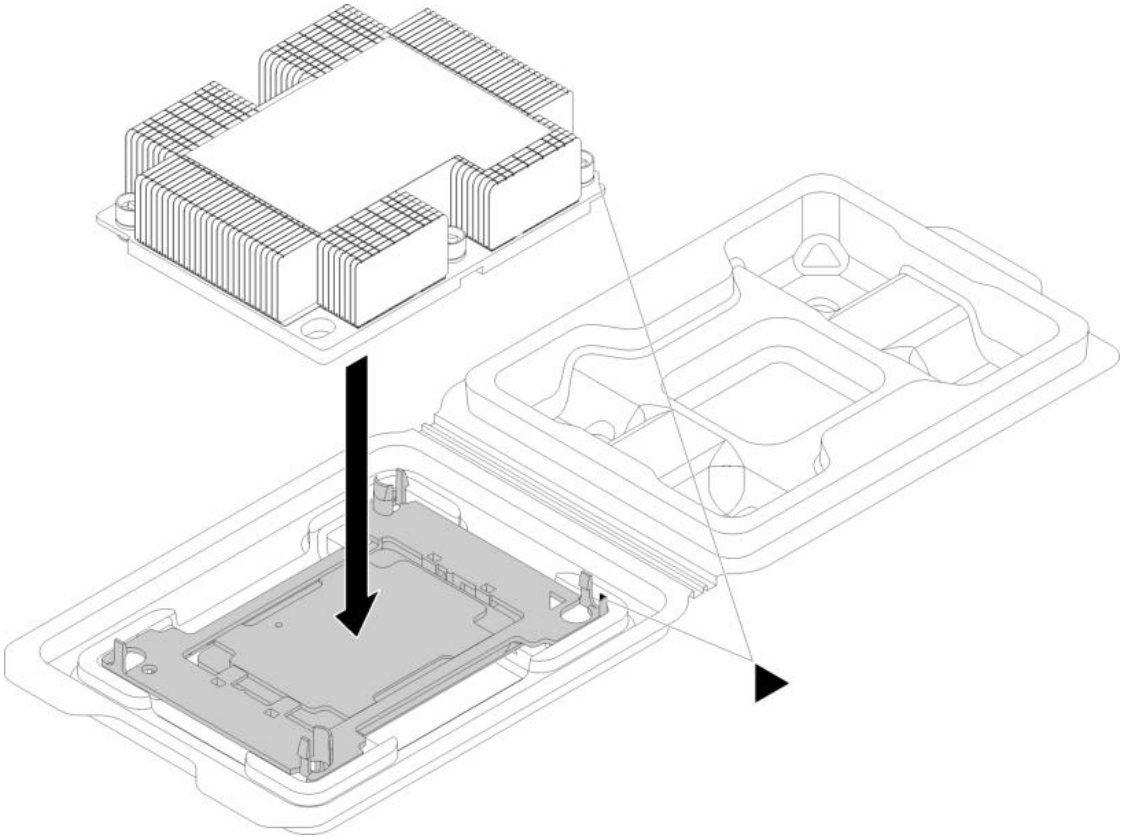


Figure 97. Assembling a PHM in the shipping tray

   a. Align the triangular marks on the processor retainer and the heat sink or align the triangular mark on the processor retainer with the notched corner of the heat sink.
   b. Insert the processor-retainer clips into the holes on the heat sink.
   c. Press the retainer into place until the clips at all four corners engage.

Complete the following steps to install a PHM.

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

Step 1. Remove the processor socket cover, if one is installed on the processor socket, by placing your fingers in the half-circles at each end of the cover and lifting it from the system board.

Step 2. Install the processor-heat-sink module on the system board.

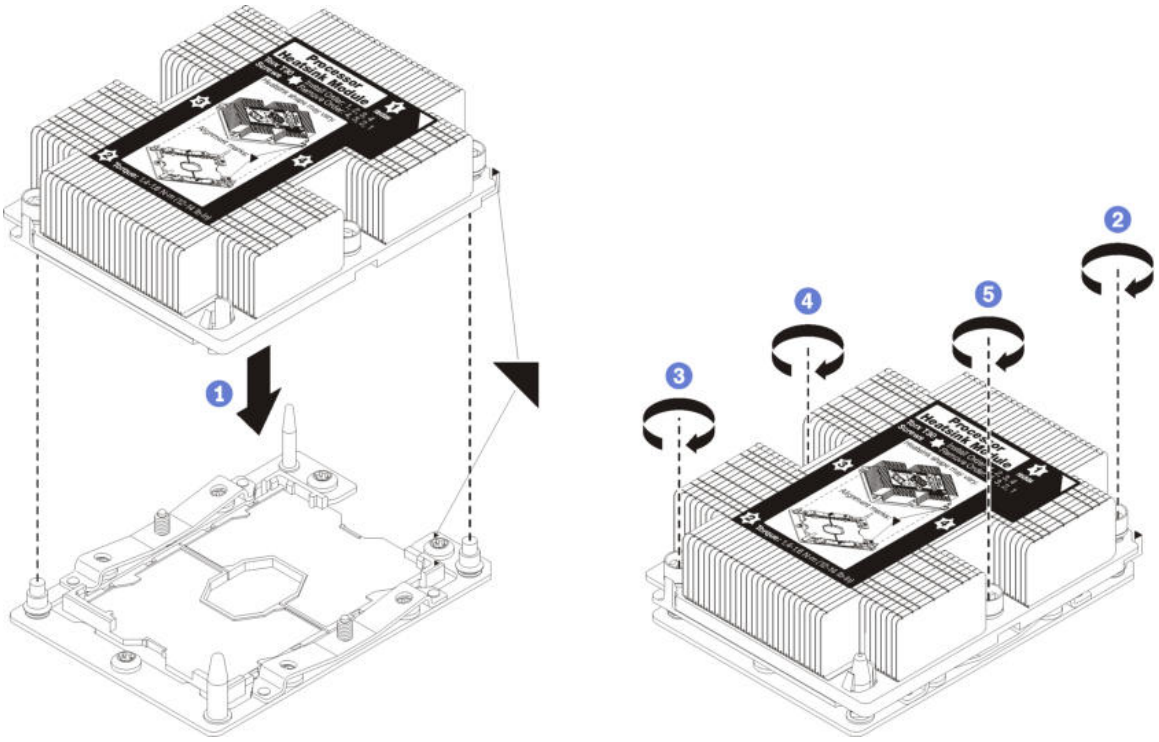


Figure 98. Installing a PHM

a. Align the triangular marks and guide pins on the processor socket with the PHM; then, insert the PHM into the processor socket.

Attention: To prevent damage to components, make sure that you follow the indicated tightening sequence.

b. Fully tighten the Torx T30 captive fasteners *in the installation sequence shown* on the heat-sink label. Tighten the screws until they stop; then, visually inspect to make sure that there is no gap between the screw shoulder beneath the heat sink and the processor socket. (For reference, the torque required for the nuts to fully tighten is 1.4 — 1.6 newton-meters, 12 — 14 inch-pounds).

After you install a PHM:

1. Complete the parts replacement. See “Complete the parts replacement” on page 143.

System board replacement

Use this information to remove and install the system board.

Important: Before you return the system board, make sure that you install the CPU socket dust covers from the new system board. To replace a CPU socket dust cover:

1. Take a dust cover from the CPU socket assembly on the new system board and orient it correctly above the CPU socket assembly on the removed system board.
2. Gently press down the dust cover legs to the CPU socket assembly, pressing on the edges to avoid damage to the socket pins. You might hear a click on the dust cover is securely attached.
3. **Make sure** that the dust cover is securely attached to the CPU socket assembly.

S017



CAUTION:
Hazardous moving fan blades nearby. Keep fingers and other body parts away.

S012



CAUTION:
Hot surface nearby.

Remove the system board

Use this information to remove the system board.



"**Read** the installation Guidelines" on page 41



"**Power off** the server for this task" on page 11



"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43

Before removing the system board:

1. Remove the top cover. See "Remove the top cover" on page 52.
2. Record where the cables are connected to the system board; then, disconnect them.

   Attention: Disengage all latches, cable clips, release tabs, or locks on cable connectors beforehand. Failing to release them before removing the cables will damage the cable connectors on the system board. Any damage to the cable connectors may require replacing the system board.
3. Remove any of the following components that are installed on the system board and put them in a safe, static-protective place. See the related topics in Chapter 3 "Hardware replacement procedures" on page 41.
   - Air baffle

- System fans
- Processor-heat-sink module (PHM)

  Note: Do not disassemble the PHM.
- DIMMs
- CMOS battery
- PCIe adapters
- Riser assembly
- M.2 backplane
- LOM adapter
- TCM/TPM (for Chinese Mainland only)

4. Pull out the power supplies a little bit. Ensure that they are disconnected from the system board.

To remove the system board, complete the following steps:

Watch the procedure. A video of the removal process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

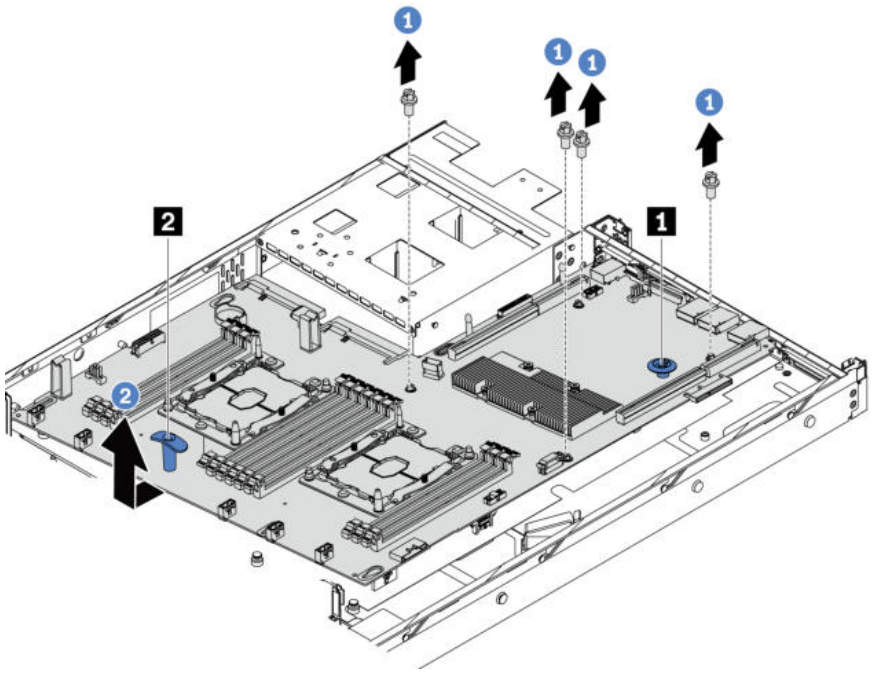


Figure 99. System board removal

Step 1. Remove the screws that secure the system board, and put the screws in a safe place.

Step 2. Grasp the system board by the release pin 1 and the lift handle 2 at the same time and gently slide the system board to the front of the server. Then lift and tilt the system board upwards to remove it from the server.

If you are instructed to return the old system board, follow all packaging instructions and use any packaging materials that are provided.

Important: Before you return the system board, make sure that you install the CPU socket dust covers from the new system board. To replace a CPU socket dust cover:

1. Take a dust cover from the CPU socket assembly on the new system board and orient it correctly above the CPU socket assembly on the removed system board.
2. Gently press down the dust cover legs to the CPU socket assembly, pressing on the edges to avoid damage to the socket pins. You might hear a click on the dust cover is securely attached.
3. **Make sure** that the dust cover is securely attached to the CPU socket assembly.

Install the system board

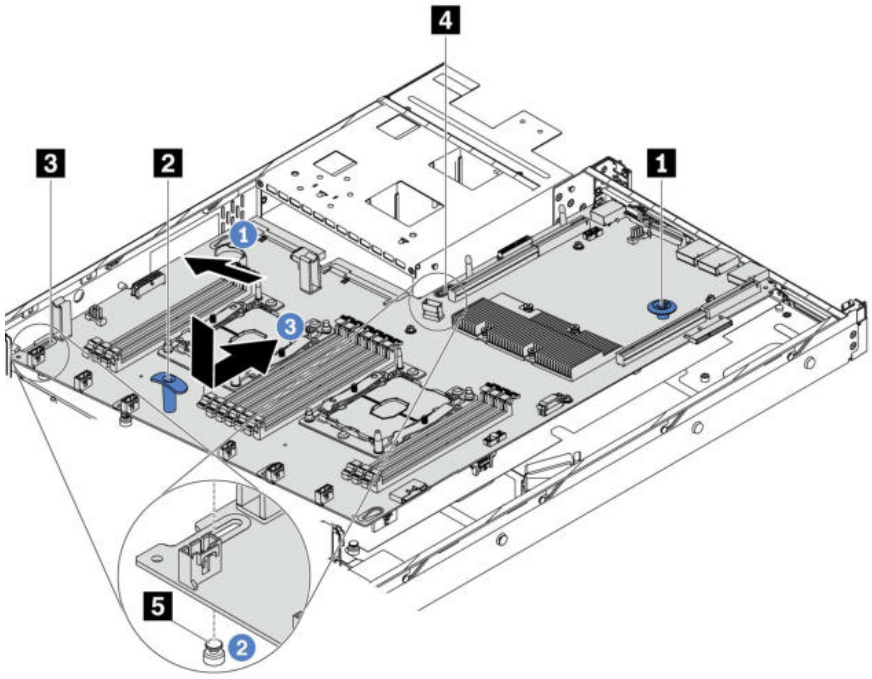
Use this information to install the system board.

	"**Read** the installation Guidelines" on page 41	 "**Power off** the server for this task" on page 11
	"**ATTENTION: Static Sensitive Device** Ground package before opening" on page 43	

Before installing the system board, touch the static-protective package that contains the new system board to any unpainted surface on the outside of the server. Then, take the new system board out of the package and place it on a static-protective surface.

Watch the procedure. A video of the installation process is available:
- Youtube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
- Youku: http://list.youku.com/albumlist/show/id_50437162

To install the system board, complete the following steps:



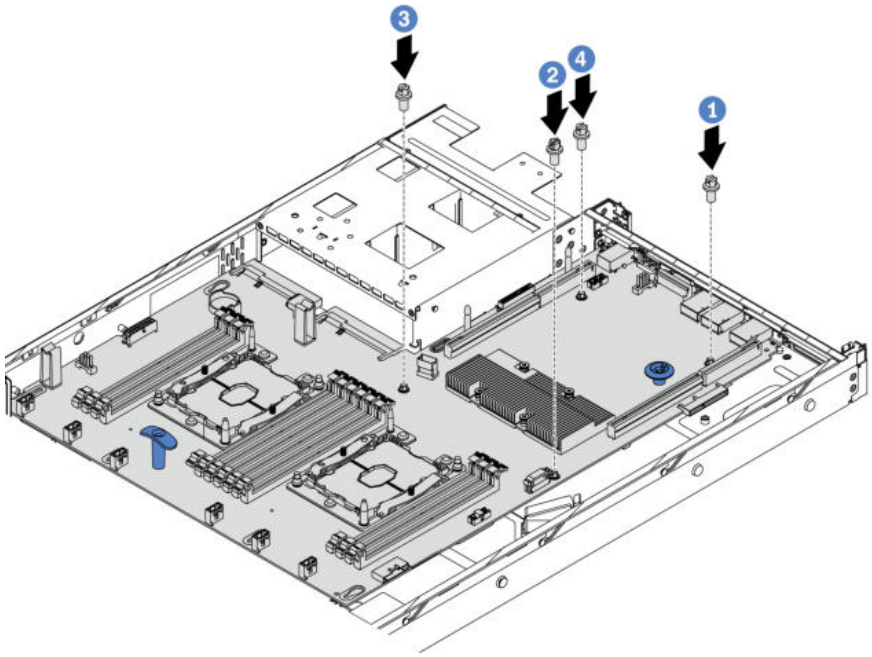
Step 1. Grasp the system board by the release pin 1 and the lift handle 2 at the same time, and tilt the system board at an angle of approximately 20 degrees as shown.

Step 2. Align the hole 3 on the system board with the corresponding mounting stud 5 on the chassis first, and then align the hole 4 by the same way.

Note: Before you align the two holes, prevent the system board from touching the mounting studs on the chassis.

Step 3. Lower the system board into the chassis and slide it to the rear of the chassis until it clicks into position.

Step 4. Install the four screws in the following sequence.



After installing the system board:

1. Push the power supplies into the bays until they click into place.
2. Install any components that you removed from the failing system board. See the related topics in Chapter 3 “Hardware replacement procedures” on page 41.
3. Complete the parts replacement. See “Complete the parts replacement” on page 143.
4. Update the Universally Unique Identifier (UUID) and DMI/SMBIOS data with new vital product data (VPD). Use the Lenovo XClarity Provisioning Manager to update the UUID and DMI/SMBIOS data. See “Update the Universal Unique Identifier (UUID)” on page 135 and “Update the DMI/SMBIOS data” on page 137.
5. Enable TPM/TCM. See “Enable TPM/TCM” on page 139.
6. Optionally, enable Secure Boot.

Update the Universal Unique Identifier (UUID)

The Universal Unique Identifier (UUID) must be updated when the system board is replaced. Use the Lenovo XClarity Provisioning Manager to update the UUID in the UEFI-based server. Lenovo XClarity Essentials OneCLIcan be used to update the UUID in the UEFI-based server as a command line option. Lenovo XClarity Essentials OneCLI is an online tool that supports several operating systems; make sure that you download the version for your operating system.

1. Start the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface.
2. From the System Summary page, click **Update VPD**.
3. Update the UUID.

   Note: You can use Lenovo XClarity Essentials OneCLI to update the UUID for the server.

To download Lenovo XClarity Essentials OneCLI, go to the following site:

https://datacentersupport.lenovo.com/solutions/HT116433

Lenovo XClarity Essentials OneCLI sets the UUID in the Lenovo XClarity Controller. Select one of the following methods to access the Lenovo XClarity Controller and set the UUID:

- Operate from the target system, such as LAN or keyboard console style (KCS) access
- Remote access to the target system (TCP/IP based)

Step 1. Copy and unpack the OneCLI package, which also includes other required files, to the server. Make sure that you unpack the OneCLI and the required files to the same directory.

Step 2. After you have OneCLI in place, use the following command syntax to set the UUID:

```
onecli config set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value> [access_method]
```

Where:

<uuid_value>
Up to 16-byte hexadecimal value assigned by you.

[access_method]
The access method that you selected to use from the following methods:

- Online authenticated LAN access, type the command:

  Example that does not use the user ID and password default values:
  ```
  onecli config set SYSTEM_PROD_DATA.SYsInfoUUID <uuid_value> --user <user_id>
  --password <password>
  ```

  Example that uses the user ID and password default values:
  ```
  onecli config set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>
  ```

- Online KCS access (unauthenticated and user restricted):

  You do not need to specify a value for *access_method* when you use this access method.

  Example:
  ```
  onecli config set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>
  ```

  Note: The KCS access method uses the IPMI/KCS interface, which requires that the IPMI driver be installed.

- Remote LAN access, type the command:

  Note: When using the remote LAN/WAN access method to access Lenovo XClarity Controller from a client, the *host* and the *xcc_external_ip* address are required parameters.

  ```
  [--imm xcc_user_id:xcc_password@xcc_external_ip]
  ```

  or

  ```
  [--bmc xcc_user_id:xcc_password@xcc_external_ip]
  ```

  Where:

  xcc_external_ip
  The BMC/IMM/XCC external IP address. There is no default value. This parameter is required.

  xcc_user_id
  The BMC/IMM/XCC account name (1 of 12 accounts). The default value is USERID.

  xcc_password
  The BMC/IMM/XCC account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

Note: BMC, IMM, or XCC external IP address, account name, and password are all valid for this command.

Example that does use the user ID and password default values:
```
onecli config set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>
```

Step 3. Restart the Lenovo XClarity Controller.

Step 4. Restart the server.

Update the DMI/SMBIOS data

The Desktop Management Interface (DMI) must be updated when the system board is replaced. Use the Lenovo XClarity Provisioning Manager to update the DMI in the UEFI-based server. Lenovo XClarity Essentials OneCLIcan be used to update the UUID in the UEFI-based server as a command line option. Lenovo XClarity Essentials OneCLI is an online tool that supports several operating systems; make sure that you download the version for your operating system.

1. Start the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface.
2. From the System Summary page, click **Update VPD**.
3. Update the asset tag information.

Note: You can use Lenovo XClarity Essentials OneCLI to update the asset tag for the server.

To download Lenovo XClarity Essentials OneCLI, go to the following site:

https://datacentersupport.lenovo.com/solutions/HT116433

Lenovo XClarity Essentials OneCLI sets the DMI in the Lenovo XClarity Controller. Select one of the following methods to access the Lenovo XClarity Controller and set the DMI:

- Operate from the target system, such as LAN or keyboard console style (KCS) access
- Remote access to the target system (TCP/IP based)

Step 1. After you haveLenovo XClarity Essentials OneCLI in place, type the following commands to set the DMI:
```
onecli config set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model> [access_method]
onecli config set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n> [access_method]
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag> [access_method]
```

Where:

<m/t_model>
The server machine type and model number. Type `mtm xxxxyyy`, where *xxxx* is the machine type and *yyy* is the server model number.

<s/n>
The serial number on the server. Type `sn zzzzzzz`, where *zzzzzzz* is the serial number.

<asset_method>
The server asset tag number. Type `asset aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa`, where *aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa* is the asset tag number.

[access_method]
The access method that you select to use from the following methods:

- Online authenticated LAN access, type the command:

```
[--imm xcc_user_id:xcc_password@xcc_internal_ip]
```

or

```
[--bmc xcc_user_id:xcc_password@xcc_internal_ip]
```

Where:

xcc_internal_ip
The BMC/IMM/XCC internal LAN/USB IP address. The default value is 169.254.95.118.

xcc_user_id
The BMC/IMM/XCC account name (1 of 12 accounts). The default value is USERID.

xcc_password
The BMC/IMM/XCC account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

Notes:

1. BMC, IMM, or XCC internal LAN/USB IP address, account name, and password are all valid for this command.
2. If you do not specify any of these parameters, OneCLI will use the default values. When the default values are used and OneCLI is unable to access the Lenovo XClarity Controller using the online authenticated LAN access method, OneCLI will automatically use the unauthenticated KCS access method.

Examples that do use the user ID and password default values:

```
onecli config set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model>
onecli config set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n>
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
```

- Online KCS access (unauthenticated and user restricted): You do not need to specify a value for *access_method* when you use this access method.

  Note: The KCS access method uses the IPMI/KCS interface, which requires that the IPMI driver be installed.

  The following commands are examples of not using the user ID and password default values:

  ```
  onecli config set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model>
  onecli config set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n>
  onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
  ```

- Remote LAN access, type the command:

  Note: When using the remote LAN/WAN access method to access Lenovo XClarity Controller from a client, the *host* and the *xcc_external_ip* address are required parameters.

  ```
  [--imm xcc_user_id:xcc_password@xcc_external_ip]
  ```
  or
  ```
  [--bmc xcc_user_id:xcc_password@xcc_external_ip]
  ```

  Where:

  xcc_external_ip
  The BMC/IMM/XCC IP address. There is no default value. This parameter is required.

  xcc_user_id
  The BMC/IMM/XCC account (1 of 12 accounts). The default value is USERID.

  xcc_password

The BMC/IMM/XCC account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

Note: BMC, IMM, or XCC internal LAN/USB IP address, account name, and password are all valid for this command.

Examples that do use the user ID and password default values:

```
onecli config set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model> --host <xcc_ip>
onecli config set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n> --host <xcc_ip>
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag> --host <xcc_ip>
```

Step 2. Reset IMM to the factory defaults. Go to https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_resettingthexcc.html for more information.

Step 3. Reset the Lenovo XClarity Controller to the factory defaults. Go to https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_resettingthexcc.html for more information.

Enable TPM/TCM

The server supports Trusted Platform Module (TPM), Version 1.2 or Version 2.0.

Note: For customers in Chinese Mainland, integrated TPM is not supported. However, customers in Chinese Mainland can install a Trusted Cryptographic Module (TCM) adapter or a TPM adapter (sometimes called a daughter card).

When a system board is replaced, you must make sure that the TPM/TCM policy is set correctly.

CAUTION:
Take special care when setting the TPM/TCM policy. If it is not set correctly, the system board can become unusable.

Set the TPM/TCM policy

By default, a replacement system board is shipped with the TPM/TCM policy set to **undefined**. You must modify this setting to match the setting that was in place for the system board that is being replaced.

You can set the TPM/TCM policy from Lenovo XClarity Provisioning Manager.

Complete the following steps to set the TPM/TCM policy.

Step 1. Start the server and when prompted, press F1 to display Lenovo XClarity Provisioning Manager.

Step 2. If the power-on Administrator password is required, enter the password.

Step 3. From the System Summary page, click **Update VPD**.

Step 4. Set the policy to one of the following settings.

- **TCM enabled - China only**. Customers in Chinese Mainland should choose this setting if a TCM adapter is installed.
- **NationZ TPM 2.0 enabled - China only**. Customers in Chinese Mainland should choose this setting if a NationZ TPM 2.0 adapter is installed.
- **TPM enabled - ROW**. Customers outside of Chinese Mainland should choose this setting.
- **Permanently disabled**. Customers in Chinese Mainland should use this setting if no TPM or TCM adapter is installed.

Although the setting **undefined** is available as a policy setting, it should not be used.

Notes: You can use Lenovo XClarity Essentials OneCLI to update the TPM/TCM policy. Please note that a Local IPMI user and password must be setup in Lenovo XClarity Controller for remote accessing to the target system.

1. Read TpmTcmPolicyLock to check whether the TPM_TCM_POLICY has been locked:
   `OneCli.exe config show imm.TpmTcmPolicyLock --override --imm <userid>:<password>@<ip_address>`

   Note: The imm.TpmTcmPolicyLock value must be 'Disabled', which means TPM_TCM_POLICY is NOT locked and changes to the TPM_TCM_POLICY are permitted. If the return code is ‘Enabled’ then no changes to the policy are permitted. The planar may still be used if the desired setting is correct for the system being replaced.
2. Configure the TPM_TCM_POLICY into XCC:
   - For the customer in Chinese Mainland with no TCM:
     `OneCli.exe config set imm.TpmTcmPolicy "NeitherTpmNorTcm" --override --imm <userid>:<password>@<ip_address>`
   - For the customer in Chinese Mainland that has installed TCM module on the original system (TCM module should be moved to the FRU prior to changing policy)
     `OneCli.exe config set imm.TpmTcmPolicy "TcmOnly" --override --imm <userid>:<password>@<ip_address>`
   - For the customer outside of Chinese Mainland:
     `OneCli.exe config set imm.TpmTcmPolicy "TpmOnly" --override --imm <userid>:<password>@<ip_address>`
3. Issue reset command to reset system:
   `OneCli.exe misc ospower reboot --imm <userid>:<password>@<ip_address>`
4. Read back the value to check whether the change has been accepted:
   `OneCli.exe config show imm.TpmTcmPolicy --override --imm <userid>:<password>@<ip_address>`

   Notes:
   - If the read back value is matched it means the TPM_TCM_POLICY has been set correctly.

     imm.TpmTcmPolicy is defined as below:
     - Value 0 use string “Undefined” , which means UNDEFINED policy.
     - Value 1 use string “NeitherTpmNorTcm”, which means TPM_PERM_DISABLED.
     - Value 2 use string “TpmOnly”, which means TPM_ALLOWED.
     - Value 4 use string “TcmOnly”, which means TCM_ALLOWED.
   - Below 4 steps must also be used to ‘lock’ the TPM_TCM_POLICY when using OneCli/ASU commands:
5. Read TpmTcmPolicyLock to check whether the TPM_TCM_POLICY has been locked , command as below:

   `OneCli.exe config show imm.TpmTcmPolicyLock --override --imm <userid>:<password>@<ip_address>`

   The value must be 'Disabled', it means TPM_TCM_POLICY is NOT locked and must be set.
6. Lock the TPM_TCM_POLICY:
   `OneCli.exe config set imm.TpmTcmPolicyLock"Enabled"--override --imm <userid>:<password>@<ip_address>`
7. Issue reset command to reset system, command as below:
   `OneCli.exe misc ospower reboot --imm <userid>:<password>@<ip_address>`

   During the reset, UEFI will read the value from imm.TpmTcmPolicyLock, if the value is 'Enabled' and the imm.TpmTcmPolicy value is invalid, UEFI will lock the TPM_TCM_POLICY setting.

   The valid value for imm.TpmTcmPolicy includes 'NeitherTpmNorTcm', 'TpmOnly' and 'TpmOnly'.

If the imm.TpmTcmPolicy is set as 'Enabled' but imm.TpmTcmPolicy value is invalid, UEFI will reject the 'lock' request and change imm.TpmTcmPolicy back to 'Disabled'.

8. Read back the value to check whether the ‘Lock’ is accepted or rejected. command as below:

   ```
   OneCli.exe config show imm.TpmTcmPolicy --override --imm <userid>:<password>@<ip_address>
   ```

   Note: If the read back value is changed from'Disabled' to 'Enabled' that means the TPM_ TCM_POLICY has been locked successfully. There is no method to unlock a policy once it has been set other than replacing system board.

   imm.TpmTcmPolicyLockis defined as below:

   Value 1 use string “Enabled" , which means lock the policy. Other values are not accepted.

   Procedure also requires that Physical Presence is enabled. The Default value for FRU will be enabled.
   ```
   PhysicalPresencePolicyConfiguration.PhysicalPresencePolicy=Enable
   ```

Assert Physical Presence

Before you can assert Physical Presence, the Physical Presence Policy must be enabled. By default, the Physical Presence Policy is enabled with a timeout of 30 minutes.

If the Physical Presence Policy is enabled, you can assert Physical Presence through the Lenovo XClarity Controller or through hardware jumpers on the system board.

Notes: If the Physical Presence Policy has been disabled:

1. Set the hardware Physical Presence jumper on the system board to assert Physical Presence.
2. Enable the Physical Presence Policy using either F1 (UEFI Settings) or Lenovo XClarity Essentials OneCLI.

Assert Physical Presence through the Lenovo XClarity Controller

Complete the following steps to assert Physical Presence through the Lenovo XClarity Controller:

1. Log in to the Lenovo XClarity Controller interface.

   For information about logging in to the Lenovo XClarity Controller, see:

   http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/dw1lm_c_chapter2_openingandusing.html
2. Click **BMC Configuration → Security** and verify that Physical Presence is set to **assert**.

Assert Physical Presence through the hardware

You can also assert hardware Physical Presence through the use of a jumper on the system board. For more information about asserting hardware Physical Presence through the use of a jumper, see “System board switches and jumpers” on page 25

Set the TPM version

To be able to set the TPM version, Physical Presence must be asserted.

The Lenovo XClarity Provisioning Manager or the Lenovo XClarity Essentials OneCLI can be used to set the TPM version.

To set the TPM version:

1. Download and install Lenovo XClarity Essentials OneCLI.
   a. Go to http://datacentersupport.lenovo.com and navigate to the support page for your server.

b. Click **Drivers & Software**.

c. Navigate to the version of Lenovo XClarity Essentials OneCLI for your operating system and download the package.

2. Run the following command to set the TPM version:

   Note: You can change the TPM version from 1.2 to 2.0 and back again. However, you can toggle between versions a maximum of 128 times.

   To set the TPM version to version 2.0:
   ```
   OneCli.exe config set TrustedComputingGroup.DeviceOperation "Update to TPM2.0 compliant"
              --bmc userid:password@ip_address
   ```

   To set the TPM version to version 1.2:
   ```
   OneCli.exe config set TrustedComputingGroup.DeviceOperation "Update to TPM1.2 compliant"
             --bmc userid:password@ip_address
   ```

   where:

   - *<userid>:<password>* are the credentials used to access the BMC (Lenovo XClarity Controller interface) of your server. The default user ID is USERID, and the default password is PASSW0RD (zero, not an uppercase o)
   - *<ip_address>* is the IP address of the BMC.

   For more information about the Lenovo XClarity Essentials OneCLI **set** command, see:

   http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_set_command.html

3. Alternatively, you can use the following Advanced Settings Utility (ASU) commands:

   To set the TPM version to version 2.0:
   ```
   asu64 set TPMVersion.TPMVersion "Update to TPM2.0 compliant" --host <ip_address>
             --user <userid> --password <password>  --override
   ```

   To set the TPM version to version 1.2:
   ```
   asu64 set TPMVersion.TPMVersion "Update to TPM1.2 compliant" --host <ip_address>
             --user <userid> --password <password>  --override
   ```

   where:

   - *<userid>* and *<password>* are the credentials used to the BMC (Lenovo XClarity Controller interface) of your server. The default user ID is USERID, and the default password is PASSW0RD (zero, not an uppercase o)
   - *<ip_address>* is the IP address of the BMC.

Enable UEFI Secure Boot

Optionally, you can enable UEFI Secure Boot.

Physical Presence must be asserted if you are going to enable UEFI Secure Boot. See “Assert Physical Presence” on page 141.

For information about accessing the Lenovo XClarity Controller interface, see:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/dw1lm_c_chapter2_openingandusing.html

There are two methods available to enable UEFI Secure Boot:

- From Lenovo XClarity Provisioning Manager

  To enable UEFI Secure Boot from Lenovo XClarity Provisioning Manager:

1. Start the server and when prompted, press F1 to display Lenovo XClarity Provisioning Manager.
2. If the power-on Administrator password is required, enter the password.
3. From the UEFI Setup page, click **System Settings → Security → Secure Boot**.
4. Enable Secure Boot and save the settings.

- From Lenovo XClarity Essentials OneCLI

  To enable UEFI Secure Boot from Lenovo XClarity Essentials OneCLI:

  1. Download and install Lenovo XClarity Essentials OneCLI.

     To download Lenovo XClarity Essentials OneCLI, go to the following site:

     https://datacentersupport.lenovo.com/solutions/HT116433

  2. Run the following command to enable Secure Boot:

     ```
     OneCli.exe config set SecureBootConfiguration.SecureBootSetting Enabled  --override
                      --bmc <userid>:<password>@<ip_address>
     ```

     where:

     – *<userid>:<password>* are the credentials used to access the BMC (Lenovo XClarity Controller interface) of your server. The default user ID is USERID, and the default password is PASSW0RD (zero, not an uppercase o)

     – *<ip_address>* is the IP address of the BMC.

     For more information about the Lenovo XClarity Essentials OneCLI **set** command, see:

     http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_set_command.html

Complete the parts replacement

Use this information to complete the parts replacement.

To complete the parts replacement, do the following:

1. Ensure that all components have been reassembled correctly and that no tools or loose screws are left inside your server.
2. Properly route and secure the cables in the server. See “Internal cable routing” on page 28.
3. If you have removed the top cover, reinstall it. See “Install the top cover” on page 54.
4. Reconnect external cables and power cords to the server.

   Attention: To avoid component damage, connect the power cords last.
5. Update the server configuration if necessary.
   - Download and install the latest device drivers: http://datacentersupport.lenovo.com
   - Update the system firmware. See “Firmware updates” on page 7.
   - Use the Lenovo XClarity Provisioning Manager to update the UEFI configuration. For more information, see: http://sysmgt.lenovofiles.com/help/topic/LXPM/UEFI_setup.html
   - Use the Lenovo XClarity Provisioning Manager to configure the RAID if you have installed or removed a hot-swap drive, a RAID adapter, or the M.2 backplane and M.2 drive. For more information, see: http://sysmgt.lenovofiles.com/help/topic/LXPM/RAID_setup.html

Note: Make sure the latest version of ThinkSystem M.2 with Mirroring Enablement Kit Firmware is applied to avoid virtual disk/array missing after system board replacement.

Chapter 4. Problem determination

Use the information in this section to isolate and resolve issues that you might encounter while using your server.

Lenovo servers can be configured to automatically notify Lenovo Support if certain events are generated. You can configure automatic notification, also known as Call Home, from management applications, such as the Lenovo XClarity Administrator. If you configure automatic problem notification, Lenovo Support is automatically alerted whenever a server encounters a potentially significant event.

To isolate a problem, you should typically begin with the event log of the application that is managing the server:

- If you are managing the server from the Lenovo XClarity Administrator, begin with the Lenovo XClarity Administrator event log.
- If you are managing the server from the Chassis Management Module 2, begin with the Chassis Management Module 2 event log.
- If you are using some other management application, begin with the Lenovo XClarity Controller event log.

Event logs

An *alert* is a message or other indication that signals an event or an impending event. Alerts are generated by the Lenovo XClarity Controller or by UEFI in the servers. These alerts are stored in the Lenovo XClarity Controller Event Log. If the server is managed by the Chassis Management Module 2 or by the Lenovo XClarity Administrator, alerts are automatically forwarded to those management applications.

Note: For a listing of events, including user actions that might need to be performed to recover from an event, see the *Messages and Codes Reference*, which is available at:http://thinksystem.lenovofiles.com/help/topic/7X07/pdf_files.html

Lenovo XClarity Administrator event log

If you are using Lenovo XClarity Administrator to manage server, network, and storage hardware, you can view the events from all managed devices through the XClarity Administrator.

© Copyright Lenovo 2017, 2020

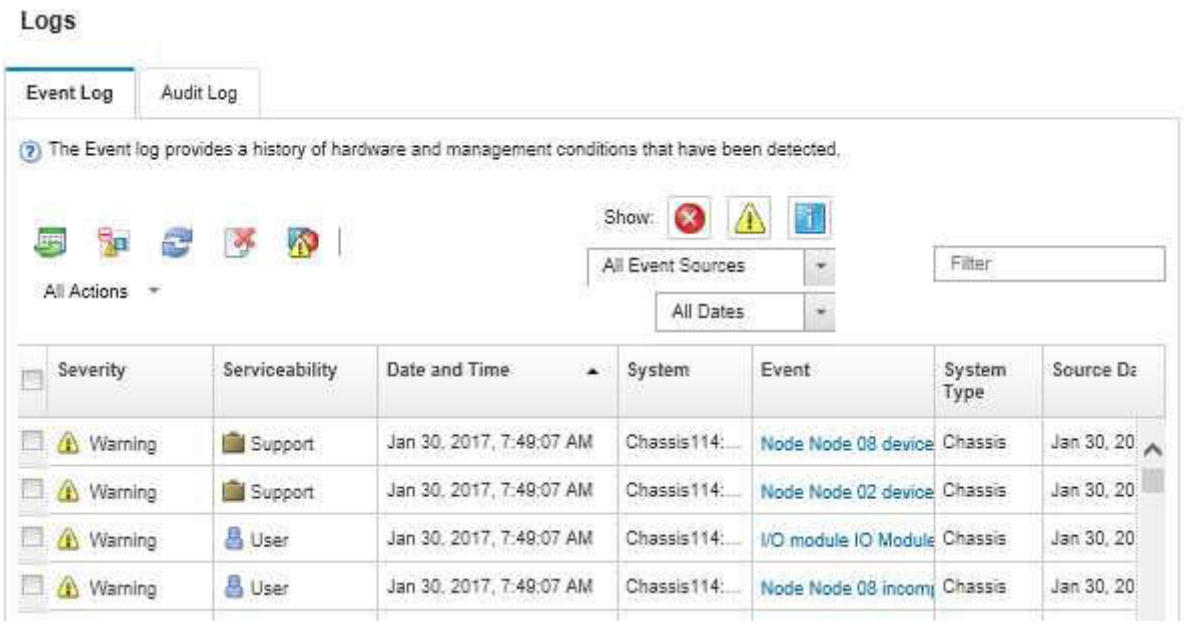


Figure 100. Lenovo XClarity Administrator event log

For more information about working with events from XClarity Administrator, see:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/events_vieweventlog.html

Lenovo XClarity Controller event log

The Lenovo XClarity Controller monitors the physical state of the server and its components using sensors that measure internal physical variables such as temperature, power-supply voltages, fan speeds, and component status. The Lenovo XClarity Controller provides various interfaces to systems management software and to system administrators and users to enable remote management and control of a server.

The Lenovo XClarity Controller monitors all components of the server and posts events in the Lenovo XClarity Controller event log.

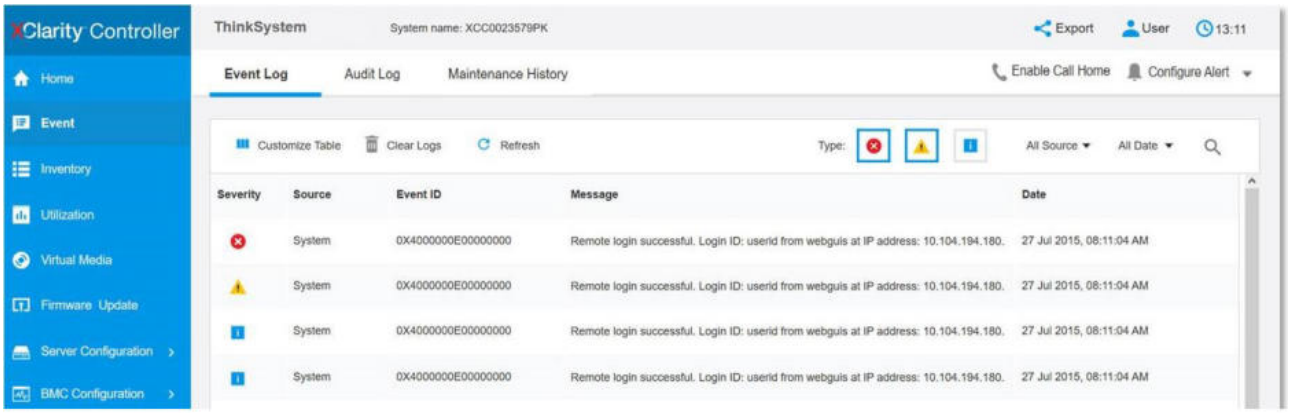


Figure 101. Lenovo XClarity Controller event log

For more information about accessing the Lenovo XClarity Controller event log, see:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/event_log.html

General problem determination procedures

Use the information in this section to resolve problems if the event log does not contain specific errors or the server is inoperative.

If you are not sure about the cause of a problem and the power supplies are working correctly, complete the following steps to attempt to resolve the problem:

1. Turn off the server.
2. Ensure that the server is cabled correctly.
3. Remove or disconnect the following devices, one at a time, until you find the failure. Turn on and configure the server each time you remove or disconnect a device.
   - Any external devices
   - Surge-suppressor device (on the server)
   - Printer, mouse, and non-Lenovo devices
   - Each adapter
   - Storage drives
   - DIMMs until you reach the minimum configuration that is supported for the server

   Note: For minimal configuration for debugging, see “Specifications” on page 2
4. Turn on the server.

If the problem is solved when you remove an adapter from the server, but the problem recurs when you install the same adapter again, suspect the adapter. If the problem recurs when you replace the adapter with a different one, try a different PCIe slot.

If the problem appears to be a networking problem and the server passes all system tests, suspect a network cabling problem that is external to the server.

Resolving suspected power problems

Power problems can be difficult to solve. For example, a short circuit can exist anywhere on any of the power distribution buses. Usually, a short circuit will cause the power subsystem to shut down because of an overcurrent condition.

Complete the following steps to diagnose and resolve a suspected power problem.

Step 1. Check the event log and resolve any errors related to the power.

Note: Start with the event log of the application that is managing the server. For more information about event logs, see “Event logs” on page 145.

Step 2. Check for short circuits, for example, if a loose screw is causing a short circuit on a circuit board.

Step 3. Remove the adapters and disconnect the cables and power cords to all internal and external devices until the server is at the minimum configuration that is required for the server to start. See “Specifications” on page 2 to determine the minimum configuration for your server.

Step 4. Reconnect all ac power cords and turn on the server. If the server starts successfully, reseat the adapters and devices one at a time until the problem is isolated.

If the server does not start from the minimum configuration, replace the components in the minimum configuration one at a time until the problem is isolated.

Resolving suspected Ethernet controller problems

The method that you use to test the Ethernet controller depends on which operating system you are using. See the operating-system documentation for information about Ethernet controllers, and see the Ethernet controller device-driver readme file.

Complete the following steps to attempt to resolve suspected problems with the Ethernet controller.

Step 1. Make sure that the correct device drivers, which come with the server are installed and that they are at the latest level.

Step 2. Make sure that the Ethernet cable is installed correctly.

- The cable must be securely attached at all connections. If the cable is attached but the problem remains, try a different cable.
- If you set the Ethernet controller to operate at 100 Mbps or 1000 Mbps, you must use Category 5 cabling.

Step 3. Determine whether the hub supports auto-negotiation. If it does not, try configuring the integrated Ethernet controller manually to match the speed and duplex mode of the hub.

Step 4. Check the Ethernet controller LEDs on the rear panel of the server. These LEDs indicate whether there is a problem with the connector, cable, or hub.

- The Ethernet link status LED is lit when the Ethernet controller receives a link pulse from the hub. If the LED is off, there might be a defective connector or cable or a problem with the hub.
- The Ethernet transmit/receive activity LED is lit when the Ethernet controller sends or receives data over the Ethernet network. If the Ethernet transmit/receive activity is off, make sure that the hub and network are operating and that the correct device drivers are installed.

Step 5. Check the LAN activity LED on the rear of the server. The LAN activity LED is lit when data is active on the Ethernet network. If the LAN activity LED is off, make sure that the hub and network are operating and that the correct device drivers are installed.

Step 6. Check for operating-system-specific causes of the problem, and also make sure that the operating system drivers are installed correctly.

Step 7. Make sure that the device drivers on the client and server are using the same protocol.

If the Ethernet controller still cannot connect to the network but the hardware appears to be working, the network administrator must investigate other possible causes of the error.

Troubleshooting by symptom

Use this information to find solutions to problems that have identifiable symptoms.

To use the symptom-based troubleshooting information in this section, complete the following steps:

1. Check the event log of the application that is managing the server and follow the suggested actions to resolve any event codes.
   - If you are managing the server from the Lenovo XClarity Administrator, begin with the Lenovo XClarity Administrator event log.
   - If you are using some other management application, begin with the Lenovo XClarity Controller event log.

   For more information about event logs, see “Event logs” on page 145.
2. Review this section to find the symptoms that you are experiencing and follow the suggested actions to resolve the issue.
3. If the problem persists, contact support (see “Contacting Support” on page 165).

Power on and power off problems

Use this information to resolve issues when powering on or powering off the server.

- “Embedded hypervisor is not in the boot list” on page 149
- “The power button does not work (server does not start)” on page 149
- “Server does not power on” on page 150
- “Server does not power off” on page 150

Embedded hypervisor is not in the boot list

Complete the following steps until the problem is solved.

1. If the server has been installed, moved, or serviced recently, or if this is the first time the embedded hypervisor is being used, make sure that the device is connected properly and that there is no physical damage to the connectors.
2. See the documentation that comes with the optional embedded hypervisor flash device for setup and configuration information.
3. Check http://www.lenovo.com/us/en/serverproven/ to validate that the embedded hypervisor device is supported for the server.
4. Make sure that the embedded hypervisor device is listed in the list of available boot options. From the management controller user interface, click **Server Configuration → Boot Options**.

   For information about accessing the management controller user interface, see the XClarity Controller product documentation:

   http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/dw1lm_c_chapter2_openingandusing.html
5. Check http://datacentersupport.lenovo.com for any tech tips (service bulletins) related to the embedded hypervisor and the server.
6. Make sure that other software works on the server to ensure that it is working properly.

The power button does not work (server does not start)

Note: The power button will not function until approximately 1 to 3 minutes after the server has been connected to ac power.

Complete the following steps until the problem is resolved:

1. Make sure that the power button on the server is working correctly:
   a. Disconnect the server power cords.
   b. Reconnect the server power cords.
   c. Reseat the operator information panel cable, and then repeat steps a and b.
      - If the server starts, reseat the operator information panel.
      - If the problem remains, replace the operator information panel.
2. Make sure that:
   - The power cords are correctly connected to the server and to a working electrical outlet.
   - The LEDs on the power supply do not indicate a problem.
3. Reseat the power supplies.
4. Replace each power supply, restarting the server each time:
   - DIMMs

- Power supplies

5. If you just installed an optional device, remove it, and restart the server. If the server starts, you might have installed more devices than the power supply supports.

Server does not power on

Complete the following steps until the problem is resolved:

1. Check the event log for any events related to the server not powering on.
2. Check for any LEDs that are flashing amber.
3. Check the power LED on the system board.
4. Reseat the power supply.
5. Replace the power supply.

Server does not power off

Complete the following steps until the problem is resolved:

1. Determine whether you are using an Advanced Configuration and Power Interface (ACPI) or a non-ACPI operating system. If you are using a non-ACPI operating system, complete the following steps:
   a. Press `Ctrl+Alt+Delete`.
   b. Turn off the server by pressing the power button and holding it down for 5 seconds.
   c. Restart the server.
   d. If the server fails POST and the power button does not work, disconnect the power cord for 20 seconds; then, reconnect the power cord and restart the server.
2. If the problem remains or if you are using an ACPI-aware operating system, suspect the system board.

Memory problems

Use this information to resolve issues related to memory.

- “Displayed system memory less than installed physical memory” on page 150
- “Multiple rows of DIMMs in a branch identified as failing” on page 151

Displayed system memory less than installed physical memory

Complete the following steps until the problem is resolved:

Note: Each time you install or remove a DIMM, you must disconnect the server from the power source; then, wait 10 seconds before restarting the server.

1. Make sure that:
   - No error LEDs are lit on the operator information panel.
   - Memory mirrored channel does not account for the discrepancy.
   - The DIMMs are seated correctly.
   - You have installed the correct type of DIMMs.
   - If you changed the DIMMs, you updated the memory configuration in the Setup utility.
   - All banks of memory are enabled. The server might have automatically disabled a memory bank when it detected a problem, or a memory bank might have been manually disabled.
   - There is no memory mismatch when the server is at the minimum memory configuration.
2. Reseat the DIMMs, and then restart the server.

3. Run memory diagnostics. When you start a server and press F1, the Lenovo XClarity Provisioning Manager interface is displayed by default. You can perform memory diagnostics from this interface. From the Diagnostic page, click **Run Diagnostic → Memory test**.
4. Check the POST error log:
   - If a DIMM was disabled by a systems-management interrupt (SMI), replace the DIMM.
   - If a DIMM was disabled by the user or by POST, reseat the DIMM; then, run the Setup utility and enable the DIMM.
5. Reseat the DIMM.
6. Restart the server.

Multiple rows of DIMMs in a branch identified as failing

1. Reseat the DIMMs; then, restart the server.
2. Remove the lowest-numbered DIMM pair of those that are identified and replace it with an identical known good DIMM; then, restart the server. Repeat as necessary. If the failures continue after all identified DIMMs are replaced, go to step 4.
3. Return the removed DIMMs, one at a time, to their original connectors, restarting the server after each DIMM, until a DIMM fails. Replace each failing DIMM with an identical known good DIMM, restarting the server after each DIMM replacement. Repeat step 3 until you have tested all removed DIMMs.
4. Replace the lowest-numbered DIMM of those identified; then, restart the server. Repeat as necessary.
5. Reverse the DIMMs between the channels (of the same processor), and then restart the server. If the problem is related to a DIMM, replace the failing DIMM.
6. (Trained technician only) Replace the system board.

Hard disk drive problems

Use this information to resolve issues related to the hard disk drives.

- “Server cannot recognize a hard drive” on page 151
- “Multiple hard drives fail” on page 152
- “Multiple hard drives are offline” on page 152
- “A replacement hard disk drive does not rebuild” on page 152
- “Green hard disk drive activity LED does not represent actual state of associated drive” on page 153
- “Yellow hard disk drive status LED does not represent actual state of associated drive” on page 153

Server cannot recognize a hard drive

Complete the following steps until the problem is solved.

1. Observe the associated yellow hard disk drive status LED. If the LED is lit, it indicates a drive fault.
2. If the LED is lit, remove the drive from the bay, wait 45 seconds, and reinsert the drive, making sure that the drive assembly connects to the hard disk drive backplane.
3. Observe the associated green hard disk drive activity LED and the yellow status LED:
   - If the green activity LED is flashing and the yellow status LED is not lit, the drive is recognized by the controller and is working correctly. Run the diagnostics tests for the hard disk drives. When you start a server and press F1, the Lenovo XClarity Provisioning Manager interface is displayed by default. You can perform hard drive diagnostics from this interface. From the Diagnostic page, click **Run Diagnostic → HDD test**.
   - If the green activity LED is flashing and the yellow status LED is flashing slowly, the drive is recognized by the controller and is rebuilding.

- If neither LED is lit or flashing, check the hard disk drive backplane.
- If the green activity LED is flashing and the yellow status LED is lit, replace the drive. If the activity of the LEDs remains the same, go to step Hard disk drive problems. If the activity of the LEDs changes, return to step 1.

4. Make sure that the hard disk drive backplane is correctly seated. When it is correctly seated, the drive assemblies correctly connect to the backplane without bowing or causing movement of the backplane.
5. Reseat the backplane power cable and repeat steps 1 through 3.
6. Reseat the backplane signal cable and repeat steps 1 through 3.
7. Suspect the backplane signal cable or the backplane:
   - Replace the affected backplane signal cable.
   - Replace the affected backplane.
8. Run the diagnostics tests for the hard disk drives. When you start a server and press F1, the Lenovo XClarity Provisioning Manager interface is displayed by default. You can perform hard drive diagnostics from this interface. From the Diagnostic page, click **Run Diagnostic → HDD test**.

   Based on those tests:
   - If the adapter passes the test but the drives are not recognized, replace the backplane signal cable and run the tests again.
   - Replace the backplane.
   - If the adapter fails the test, disconnect the backplane signal cable from the adapter and run the tests again.
   - If the adapter fails the test, replace the adapter.

Multiple hard drives fail

Complete the following steps until the problem is solved:

- View the Lenovo XClarity Controller event log for events related to power supplies or vibration issues and resolve those events.
- Make sure that the device drivers and firmware for the hard disk drive and server are at the latest level

Important: Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.

Multiple hard drives are offline

Complete the following steps until the problem is solved:

- View the Lenovo XClarity Controller event log for events related to power supplies or vibration issues and resolve those events.
- View the storage subsystem log for events related to the storage subsystem and resolve those events.

A replacement hard disk drive does not rebuild

Complete the following steps until the problem is solved:

1. Make sure that the hard disk drive is recognized by the adapter (the green hard disk drive activity LED is flashing).
2. Review the SAS/SATA RAID adapter documentation to determine the correct configuration parameters and settings.

Green hard disk drive activity LED does not represent actual state of associated drive

Complete the following steps until the problem is solved:

1. If the green hard disk drive activity LED does not flash when the drive is in use, run the diagnostics tests for the hard disk drives. When you start a server and press F1, the Lenovo XClarity Provisioning Manager interface is displayed by default. You can perform hard drive diagnostics from this interface. From the Diagnostic page, click **Run Diagnostic → HDD test**.
2. If the drive passes the test, replace the backplane.
3. If the drive fails the test, replace the drive.

Yellow hard disk drive status LED does not represent actual state of associated drive

Complete the following steps until the problem is solved:

1. Turn off the server.
2. Reseat the SAS/SATA adapter.
3. Reseat the backplane signal cable and backplane power cable.
4. Reseat the hard disk drive.
5. Power on the server and observe the activity of the hard disk drive LEDs.

Monitor and video problems

Use this information to solve problems related to a monitor or video.

- “Incorrect characters are displayed” on page 153
- “Screen is blank” on page 153
- “Screen goes blank when you start some application programs” on page 154
- “The monitor has screen jitter, or the screen image is wavy, unreadable, rolling, or distorted.” on page 154
- “The wrong characters appear on the screen” on page 154

Incorrect characters are displayed

Complete the following steps:

1. Verify that the language and locality settings are correct for the keyboard and operating system.
2. If the wrong language is displayed, update the server firmware to the latest level. See “Firmware updates” on page 7.

Screen is blank

1. If the server is attached to a KVM switch, bypass the KVM switch to eliminate it as a possible cause of the problem: connect the monitor cable directly to the correct connector on the rear of the server.
2. The management controller remote presence function is disabled if you install an optional video adapter. To use the management controller remote presence function, remove the optional video adapter.
3. If the server installed with the graphical adapters while turning on the server, the Lenovo logo displays on the screen after approximately 3 minutes. This is normal operation while the system loads.
4. Make sure that:
   - The server is turned on. If there is no power to the server.
   - The monitor cables are connected correctly.
   - The monitor is turned on and the brightness and contrast controls are adjusted correctly.
5. Make sure that the correct server is controlling the monitor, if applicable.
6. Make sure that corrupted server firmware is not affecting the video; see “Firmware updates” on page 7.
7. Observe the LEDs on the system board; if the codes are changing, go to step 6.

8. Replace the following components one at a time, in the order shown, restarting the server each time:
   a. Monitor
   b. Video adapter (if one is installed)
   c. (Trained technician only) System board

Screen goes blank when you start some application programs

1. Make sure that:
   - The application program is not setting a display mode that is higher than the capability of the monitor.
   - You installed the necessary device drivers for the application.

The monitor has screen jitter, or the screen image is wavy, unreadable, rolling, or distorted.

1. If the monitor self-tests show that the monitor is working correctly, consider the location of the monitor. Magnetic fields around other devices (such as transformers, appliances, fluorescents, and other monitors) can cause screen jitter or wavy, unreadable, rolling, or distorted screen images. If this happens, turn off the monitor.

   Attention: Moving a color monitor while it is turned on might cause screen discoloration.

   Move the device and the monitor at least 305 mm (12 in.) apart, and turn on the monitor.

   Notes:
   a. To prevent diskette drive read/write errors, make sure that the distance between the monitor and any external diskette drive is at least 76 mm (3 in.).
   b. Non-Lenovo monitor cables might cause unpredictable problems.
2. Reseat the monitor cable.
3. Replace the components listed in step 2 one at a time, in the order shown, restarting the server each time:
   a. Monitor cable
   b. Video adapter (if one is installed)
   c. Monitor
   d. (Trained technician only) System board

The wrong characters appear on the screen

Complete the following steps until the problem is solved:

1. Verify that the language and locality settings are correct for the keyboard and operating system.
2. If the wrong language is displayed, update the server firmware to the latest level. See “Firmware updates” on page 7.

Keyboard, mouse, or USB-device problems

Use this information to solve problems related to a keyboard, mouse, or USB device.

- “All or some keys on the keyboard do not work.” on page 154
- “Mouse does not work.” on page 155
- “USB-device does not work.” on page 155

All or some keys on the keyboard do not work.

1. Make sure that:

- The keyboard cable is securely connected.
- The server and the monitor are turned on.

2. If you are using a USB keyboard, run the Setup utility and enable keyboardless operation.
3. If you are using a USB keyboard and it is connected to a USB hub, disconnect the keyboard from the hub and connect it directly to the server.
4. Replace the keyboard.

Mouse does not work.

1. Make sure that:
   - The mouse cable is securely connected to the server.
   - The mouse device drivers are installed correctly.
   - The server and the monitor are turned on.
   - The mouse option is enabled in the Setup utility.
2. If you are using a USB mouse and it is connected to a USB hub, disconnect the mouse from the hub and connect it directly to the server.
3. Replace the mouse.

USB-device does not work.

1. Make sure that:
   - The correct USB device driver is installed.
   - The operating system supports USB devices.
2. Make sure that the USB configuration options are set correctly in system setup.

   Restart the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface. Then, click **System Settings → Devices and I/O Ports → USB Configuration**.
3. If you are using a USB hub, disconnect the USB device from the hub and connect it directly to the server.

Optional-device problems

Use this information to solve problems related to optional devices.

- “External USB device not recognized” on page 155
- “PCIe adapter is not recognized or is not functioning” on page 155
- “A Lenovo optional device that worked previously does not work now. ” on page 156
- “A Lenovo optional device that was just installed does not work.” on page 156
- “A Lenovo optional device that worked previously does not work now. ” on page 156

External USB device not recognized

Complete the following steps until the problem is resolved:

1. Make sure that the proper drivers are installed on the compute node. See the product documentation for the USB device for information about device drivers.
2. Use the Setup utility to make sure that the device is configured correctly.
3. If the USB device is plugged into a hub or the console breakout cable, unplug the device and plug it directly into the USB port on the front of the compute node.

PCIe adapter is not recognized or is not functioning

Complete the following steps until the problem is resolved:

1. Check the event log and resolve any issues related to the device.
2. Validate that the device is supported for the server (see http://www.lenovo.com/us/en/serverproven/).
3. Make sure that the adapter is installed in a correct slot.
4. Make sure that the proper device drivers are installed for the device.
5. Resolve any resource conflicts if running legacy mode (UEFI).
6. Check http://datacentersupport.lenovo.com for any tech tips (also known as retain tips or service bulletins) that might be related to the adapter.
7. Ensure any adapter external connections are correct and that the connectors are not physically damaged.

Insufficient PCIe resources are detected.

If you see an error message stating “Insufficient PCI Resources Detected,” complete the following steps until the problem is resolved:

1. Remove one of the PCIe adapters.
2. Restart the system and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface.
3. Click **UEFI Setup → System Settings → Devices and I/O Ports → MM Config Base**; then, modify the setting to the lower memory capacity. For example, modify 3 GB to 2 GB or modify 2 GB to 1 GB.
4. Save the settings and restart the system.
5. The action for this step will differ based on whether or not the reboot is successful.
   - If the reboot is successful, shut down the solution and reinstall the PCIe card you removed.
   - If the reboot failed, repeat step 2 to step 5.

A Lenovo optional device that was just installed does not work.

1. Make sure that:
   - The device is supported for the server (see http://www.lenovo.com/us/en/serverproven/).
   - You followed the installation instructions that came with the device and the device is installed correctly.
   - You have not loosened any other installed devices or cables.
   - You updated the configuration information in system setup. When you start a server and press F1 to display the system setup interface. Whenever memory or any other device is changed, you must update the configuration.
2. Reseat the device that you just installed.
3. Replace the device that you just installed.

A Lenovo optional device that worked previously does not work now.

1. Make sure that all of the cable connections for the device are secure.
2. If the device comes with test instructions, use those instructions to test the device.
3. If the failing device is a SCSI device, make sure that:
   - The cables for all external SCSI devices are connected correctly.
   - The last device in each SCSI chain, or the end of the SCSI cable, is terminated correctly.
   - Any external SCSI device is turned on. You must turn on an external SCSI device before you turn on the server.
4. Reseat the failing device.
5. Replace the failing device.

Serial-device problems

Use this information to solve problems with serial ports or devices.

- “Number of displayed serial ports is less than the number of installed serial ports” on page 157
- “Serial device does not work” on page 157

Number of displayed serial ports is less than the number of installed serial ports

Complete the following steps until the problem is solved.

1. Make sure that:
   - Each port is assigned a unique address in the Setup utility and none of the serial ports is disabled.
   - The serial-port adapter (if one is present) is seated correctly
2. Reseat the serial port adapter.
3. Replace the serial port adapter.

Serial device does not work

1. Make sure that:
   - The device is compatible with the server.
   - The serial port is enabled and is assigned a unique address.
   - The device is connected to the correct connector.
2. Reseat the following components:
   a. Failing serial device.
   b. Serial cable.
3. Replace the following components:
   a. Failing serial device.
   b. Serial cable.
4. (Trained technician only) Replace the system board.

Intermittent problems

Use this information to solve intermittent problems.

- “Intermittent external device problems” on page 157
- “Intermittent KVM problems” on page 158
- “Intermittent unexpected reboots” on page 158

Intermittent external device problems

Complete the following steps until the problem is solved.

1. Make sure that the correct device drivers are installed. See the manufacturer's website for documentation.
2. For a USB device:
   a. Make sure that the device is configured correctly.

      Restart the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface. Then, click **System Settings → Devices and I/O Ports → USB Configuration**.
   b. Connect the device to another port. If using a USB hub, remove the hub and connect the device directly to the compute node. Make sure that the device is configured correctly for the port.

Intermittent KVM problems

Complete the following steps until the problem is solved.

Video problems:

1. Make sure that all cables and the console breakout cable are properly connected and secure.
2. Make sure that the monitor is working properly by testing it on another compute node.
3. Test the console breakout cable on a working compute node to ensure that it is operating properly. Replace the console breakout cable if it is defective.

Keyboard problems:

Make sure that all cables and the console breakout cable are properly connected and secure.

Mouse problems:

Make sure that all cables and the console breakout cable are properly connected and secure.

Intermittent unexpected reboots

Note: Some correctable errors require that the server reboot so that it can disable a device, such as a memory DIMM or a processor to allow the machine to boot up properly.

1. If the reset occurs during POST and the POST watchdog timer is enabled, make sure that sufficient time is allowed in the watchdog timeout value (POST Watchdog Timer).

   To check the POST watchdog time, restart the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface. Then, click **BMC Settings → POST Watchdog Timer**.
2. If the reset occurs after the operating system starts, disable any automatic server restart (ASR) utilities, such as the Automatic Server Restart IPMI Application for Windows, or any ASR devices that are installed.
3. See the management controller event log to check for an event code that indicates a reboot. See “Event logs” on page 145 for information about viewing the event log.

Power problems

Use this information to resolve issues related to power.

System error LED is on and event log "Power supply has lost input" is displayed

To resolve the problem, ensure that:

1. The power supply is properly connected to a power cord.
2. The power cord is connected to a properly grounded electrical outlet for the server.

Network problems

Use this information to resolve issues related to networking.

- “Cannot wake server using Wake on LAN” on page 158
- “Could not log in using LDAP account with SSL enabled” on page 159

Cannot wake server using Wake on LAN

Complete the following steps until the problem is resolved:

1. If you are using the dual-port network adapter and the server is connected to the network using Ethernet 5 connector, check the system-error log or IMM2 system event log (see “Event logs” on page 145), make sure:
   a. The room temperature is not too high (see “Specifications” on page 2).
   b. The air vents are not blocked.
   c. The air baffle is installed securely.
2. Reseat the dual-port network adapter.
3. Turn off the server and disconnect it from the power source; then, wait 10 seconds before restarting the server.
4. If the problem still remains, replace the dual-port network adapter.

Could not log in using LDAP account with SSL enabled

Complete the following steps until the problem is resolved:

1. Make sure that the license key is valid.
2. Generate a new license key and log in again.

Observable problems

Use this information to solve observable problems.

- “The server immediately displays the POST Event Viewer when it is turned on” on page 159
- “Server is unresponsive (POST is complete and operating system is running)” on page 159
- “Server is unresponsive (cannot press F1 to start System Setup)” on page 160
- “Voltage planar fault is displayed in the event log” on page 160
- “Unusual smell” on page 161
- “Server seems to be running hot” on page 161
- “Cracked parts or cracked chassis” on page 161

The server immediately displays the POST Event Viewer when it is turned on

Complete the following steps until the problem is solved.

1. Correct any errors that are indicated by the light path diagnostics LEDs.
2. Make sure that the server supports all the processors and that the processors match in speed and cache size.

   You can view processor details from system setup.

   To determine if the processor is supported for the server, see http://www.lenovo.com/us/en/serverproven/ .
3. (Trained technician only) Make sure that processor 1 is seated correctly.
4. (Trained technician only) Remove processor 2 and restart the server.
5. Replace the following components one at a time, in the order shown, restarting the server each time:
   a. (Trained technician only) Processor
   b. (Trained technician only) System board

Server is unresponsive (POST is complete and operating system is running)

Complete the following steps until the problem is solved.

- If you are in the same location as the compute node, complete the following steps:

1. If you are using a KVM connection, make sure that the connection is operating correctly. Otherwise, make sure that the keyboard and mouse are operating correctly.
2. If possible, log in to the compute node and verify that all applications are running (no applications are hung).
3. Restart the compute node.
4. If the problem remains, make sure that any new software has been installed and configured correctly.
5. Contact your place of purchase of the software or your software provider.

- If you are accessing the compute node from a remote location, complete the following steps:
  1. Make sure that all applications are running (no applications are hung).
  2. Attempt to log out of the system and log back in.
  3. Validate the network access by pinging or running a trace route to the compute node from a command line.
     a. If you are unable to get a response during a ping test, attempt to ping another compute node in the enclosure to determine whether it is a connection problem or compute node problem.
     b. Run a trace route to determine where the connection breaks down. Attempt to resolve a connection issue with either the VPN or the point at which the connection breaks down.
  4. Restart the compute node remotely through the management interface.
  5. If the problem remains, verify that any new software has been installed and configured correctly.
  6. Contact your place of purchase of the software or your software provider.

Server is unresponsive (cannot press F1 to start System Setup)

Configuration changes, such as added devices or adapter firmware updates, and firmware or application code problems can cause the server to fail POST (the power-on self-test).

If this occurs, the server responds in either of the following ways:

- The server restarts automatically and attempts POST again.
- The server hangs, and you must manually restart the server for the server to attempt POST again.

After a specified number of consecutive attempts (automatic or manual), the server to reverts to the default UEFI configuration and starts System Setup so that you can make the necessary corrections to the configuration and restart the server. If the server is unable to successfully complete POST with the default configuration, there might be a problem with the system board.

You can specify the number of consecutive restart attempts in System Setup. Restart the server and press F1 to display the Lenovo XClarity Provisioning Manager system setup interface. Then, click **System Settings → Recovery and RAS → POST Attempts → POST Attempts Limit**. Available options are 3, 6, 9, and disable.

Voltage planar fault is displayed in the event log

Complete the following steps until the problem is solved.

1. Revert the system to the minimum configuration. See “Specifications” on page 2 for the minimally required number of processors and DIMMs.
2. Restart the system.
   - If the system restarts, add each of the items that you removed one at a time, restarting the system each time, until the error occurs. Replace the item for which the error occurs.
   - If the system does not restart, suspect the system board.

Unusual smell

Complete the following steps until the problem is solved.

1. An unusual smell might be coming from newly installed equipment.
2. If the problem remains, contact Lenovo Support.

Server seems to be running hot

Complete the following steps until the problem is solved.

Multiple compute nodes or chassis:

1. Make sure that the room temperature is within the specified range (see “Specifications” on page 2).
2. Check the management processor event log for rising temperature events. If there are no events, the compute node is running within normal operating temperatures. Note that you can expect some variation in temperature.

Cracked parts or cracked chassis

Contact Lenovo Support.

Software problems

Use this information to solve software problems.

1. To determine whether the problem is caused by the software, make sure that:
   - The server has the minimum memory that is needed to use the software. For memory requirements, see the information that comes with the software.

     Note: If you have just installed an adapter or memory, the server might have a memory-address conflict.
   - The software is designed to operate on the server.
   - Other software works on the server.
   - The software works on another server.
2. If you receive any error messages while you use the software, see the information that comes with the software for a description of the messages and suggested solutions to the problem.
3. Contact your place of purchase of the software.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support are available at:

http://datacentersupport.lenovo.com

Note: IBM is Lenovo's preferred service provider for ThinkSystem.

Before you call

Before you call, there are several steps that you can take to try and solve the problem yourself. If you decide that you do need to call for assistance, gather the information that will be needed by the service technician to more quickly resolve your problem.

Attempt to resolve the problem yourself

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

You can find the product documentation for your ThinkSystem products at the following location:

http://thinksystem.lenovofiles.com/help/index.jsp

You can take these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.lenovo.com/us/en/serverproven/ to make sure that the hardware and software is supported by your product.
- Go to http://datacentersupport.lenovo.com and check for information to help you solve the problem.
  - Check the Lenovo forums at https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg to see if someone else has encountered a similar problem.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

© Copyright Lenovo 2017, 2020

Gathering information needed to call Support

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call. You can also see http://datacentersupport.lenovo.com/warrantylookup for more information about your product warranty.

Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.

- Hardware and Software Maintenance agreement contract numbers, if applicable
- Machine type number (Lenovo 4-digit machine identifier)
- Model number
- Serial number
- Current system UEFI and firmware levels
- Other pertinent information such as error messages and logs

As an alternative to calling Lenovo Support, you can go to https://support.lenovo.com/servicerequest to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The Lenovo service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

Collecting service data

To clearly identify the root cause of a server issue or at the request of Lenovo Support, you might need collect service data that can be used for further analysis. Service data includes information such as event logs and hardware inventory.

Service data can be collected through the following tools:

- **Lenovo XClarity Provisioning Manager**

  Use the Collect Service Data function of Lenovo XClarity Provisioning Manager to collect system service data. You can collect existing system log data or run a new diagnostic to collect new data.

- **Lenovo XClarity Controller**

  You can use the Lenovo XClarity Controller web interface or the CLI to collect service data for the server. The file can be saved and sent to Lenovo Support.

  - For more information about using the web interface to collect service data, see http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_servicesandsupport.html.
  - For more information about using the CLI to collect service data, see http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator can be set up to collect and send diagnostic files automatically to Lenovo Support when certain serviceable events occur in Lenovo XClarity Administrator and the managed endpoints. You can choose to send diagnostic files to Lenovo Support using Call Home or to another service provider using SFTP. You can also manually collect diagnostic files, open a problem record, and send diagnostic files to the Lenovo Support Center.

  You can find more information about setting up automatic problem notification within the Lenovo XClarity Administrator at http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html.

- **Lenovo XClarity Essentials OneCLI**

Lenovo XClarity Essentials OneCLI has inventory application to collect service data. It can run both in-band and out-of-band. When running in-band within the host operating system on the server, OneCLI can collect information about the operating system, such as the operating system event log, in addition to the hardware service data.

To obtain service data, you can run the **getinfor** command. For more information about running the **getinfor**, see http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_getinfor_command.html.

Contacting Support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/supportphonelist for your region support details.

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo s are provided for convenience only and do not in any manner serve as an endorsement of those s. The materials at those s are not part of the materials for this Lenovo product, and use of those s is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2017, 2020

Trademarks

LENOVO, XCLARITY, and THINKSYSTEM are trademarks of Lenovo.

Intel and Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

All other trademarks are the property of their respective owners. © 2020 Lenovo.

Important notes

Processor speed indicates the internal clock speed of the processor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This

specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 20. Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Additional electronic emissions notices are available at:

http://thinksystem.lenovofiles.com/help/index.jsp

Taiwan BSMI RoHS declaration

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (PB)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模組	–	○	○	○	○	○
處理器模組	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源供應器	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電路卡	–	○	○	○	○	○
光碟機	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : "exceeding 0.1wt%" and "exceeding 0.01 wt%" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : "○"indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝-〞係指該項限用物質為排除項目。

Note3 : The "-" indicates that the restricted substance corresponds to the exemption.

Taiwan import and export contact information

Contacts are available for Taiwan import and export information.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Index

A

air baffle
  removing 55
  replacing 55, 57
assert
  physical presence 141

B

backplane for eight 2.5-inch hot-swap drives
  removing 69
  replacing 70
backplane for four 3.5-inch hot-swap drives
  removing 67
  replacing 68
backplanes 33

C

cable routing
  front I/O assembly 31
  RAID super capacitor module 32
  VGA connector 29
cable routing for the server model with eight 2.5-inch hot-swap drives 33
cable routing for the server model with four 3.5-inch hot-swap drives 34
cable routing for the server model with four 3.5-inch simple-swap drives 35
CMOS battery
  install 89
  remove 87
  replacing 87
collecting service data 164
completing
  parts replacement 143
configuring
  LAN over USB manually 10
contamination, particulate and gaseous 168
cover
  installing 54
  removing 52
  replacing 52
CPU
  installing 126
  removing 123
  replacing 123
creating a personalized support web page 163
custom support web page 163

D

devices, static-sensitive
  handling 43
DIMM, install 85

E

enable
  TPM 139
Ethernet
  controller
    troubleshooting 148
Ethernet controller problems
  solving 148
event logs 145

F

firmware updates 7
front I/O assembly
  installing 66
  removing 65
  replacing 65

G

gaseous contamination 168
general problem determination procedures 147
Getting help 163
guidelines
  options installation 41
  system reliability 42

H

handling static-sensitive devices 43
hard disk drive
  installing 74
  replacing 73
hard disk drive problems 151
hard disk drives
  removing 73
hardware service and support telephone numbers 165
heat sink
  installing 126
  removing 123
  replacing 123
help 163
hot-swap drive
  installing 74
  replacing 73
hot-swap drive backplane
  replacing 67
hot-swap drives
  removing 73
hot-swap power supply
  remove 93
  replacing 93
hot-swap power supply, install 99

I

important notices 168
install
  CMOS battery 89
  hot-swap power supply 99
installation
  guidelines 41
installation guidelines 41
installing
  CPU 126
  front I/O assembly 66
  hard disk drive 74
  heat sink 126

© Copyright Lenovo 2017, 2020

hot-swap drive 74
LOM adapter 122
memory module 85
microprocessor 126
microprocessor heat sink module 126
PCIe adapter 106
PHM 126
processor 126
processor-heat-sink module 126
rack latches 46
riser card 109
security bezel 50
serial port module 119
simple-swap drive 78
system board 134
system fan 64
TCM/TPM adapter 91
top cover 54
insufficient PCIe resource
solving 155
intermittent problems 157
internal cable routing 28
introduction 1

K

keyboard problems 154

L

LAN over USB
configuring manually 10
Windows driver installation 10
LOM adapter
installing 122
removing 121
replacing 121

M

M.2 backplane and M.2 drive
installing 114
removing 111
replacing 111
memory
problems 150
memory module
removing 79
replacing 79
Memory module installation order 80
Memory module installation rules 80
memory modules
removal 79
microprocessor
installing 126
removing 123
replacing 123
microprocessor heat sink module
installing 126
removing 123
replacing 123
monitor problems 153
mouse problems 154

N

network
problems 158
notes, important 168
notices 167

O

observable problems 159
operator information panel 15
optional-device problems 155

P

particulate contamination 168
parts list 36
parts replacement, completing 143
PCIe
troubleshooting 155
PCIe adapter
installing 106
removing 105
replacing 105
PHM
installing 126
removing 123
replacing 123
physical presence 141
power
problems 158
power cords 39
power off the server 11
power on the server 11
power problems 147
problem determination 145
problems
Ethernet controller 148
hard disk drive 151
intermittent 157
keyboard 154
memory 150
monitor 153
mouse 154
network 158
observable 159
optional devices 155
PCIe 155
power 147, 158
power on and power off 149
serial-device 157
software 161
USB device 154
video 153
processor
installing 126
removing 123
replacing 123
processor heat sink module
replacing 123
processor-heat-sink module
installing 126
removing 123

R

rack latches
installing 46
removing 44
replacing 44
RAID super capacitor module
removing 58
replacing 58, 60
rear view 17
remove

CMOS battery 87
hot-swap power supply 93
removing
air baffle 55
backplane for eight 2.5-inch hot-swap drives 69
backplane for four 3.5-inch hot-swap drives 67
CPU 123
front I/O assembly 65
hard disk drive 73
heat sink 123
hot-swap drive 73
LOM adapter 121
memory modules 79
microprocessor 123
microprocessor heat sink module 123
PCIe adapter 105
PHM 123
processor 123
processor-heat-sink module 123
rack latches 44
RAID super capacitor module 58
riser card 107
security bezel 48
serial port module 117
simple-swap drive 76
simple-swap drive backplate assembly 71
system board 131
system fan 62
TCM/TPM adapter 90
top cover 52
removing, memory modules 79
replacing
air baffle 55, 57
backplane for eight 2.5-inch hot-swap drives 70
backplane for four 3.5-inch hot-swap drives 68
CMOS battery 87
CPU 123
front I/O assembly 65
hard disk drive 73
heat sink 123
hot-swap drive 73
hot-swap drive backplane 67
hot-swap power supply 93
LOM adapter 121
M.2 module 111
memory module 79
microprocessor 123
microprocessor heat sink module 123
PCIe adapter 105
PHM 123
processor 123
processor heat sink module 123
rack latches 44
RAID super capacitor module 58, 60
riser card 107
security bezel 48
serial port module 117
simple-swap drive 76
simple-swap drive backplate assembly 71–72
system board 131
system fan 62
TCM/TPM adapter 90
top cover 52
retainer on M.2 backplane
adjustment 113
riser card
installing 109
removing 107
replacing 107

S

safety iii
safety inspection checklist iv
Secure Boot 142
security advisories 11
security bezel
installing 50
removing 48
replacing 48
serial port module
installing 119
removing 117
replacing 117
serial-device problems 157
server components 13
server power on or power off problems 149
service and support
before you call 163
hardware 165
software 165
service data 164
simple-swap drive
installing 78
replacing 76
simple-swap drive backplate assembly
removing 71
replacing 71–72
simple-swap drives
removing 76
software problems 161
software service and support telephone numbers 165
solving
Ethernet controller problems 148
insufficient PCIe resource 155
solving power problems 147
specifications 2
static-sensitive devices
handling 43
support web page, custom 163
system board
installing 134
removing 131
replacing 131
system board components 23
system board LEDs 27
system board switches and jumpers 25
system fan
installing 64
removing 62
replacing 62
system reliability guidelines 42

T

Taiwan BSMI RoHS declaration 170
Taiwan import and export contact information 170
TCM 139
TCM policy 139
TCM/TPM adapter
installing 91
removing 90
replacing 90
Tech Tips 11
telecommunication regulatory statement 169
telephone numbers 165
top cover
installing 54
removing 52
replacing 52
TPM 139
TPM 1.2 141
TPM 2.0 141
TPM policy 139
TPM version 141
trademarks 168

© Copyright Lenovo 2017, 2020

troubleshooting 153, 155, 161
by symptom 148
hard disk drive problems 151
intermittent problems 157
keyboard problems 154
memory problems 150
mouse problems 154
network problems 158
observable problems 159
power on and power off problems 149
power problems 158
serial-device problems 157
symptoms-based troubleshooting 148
USB-device problems 154
video 153
Trusted Cryptographic Module 139
Trusted Platform Module 139

U

UEFI Secure Boot 142
update firmware 7
updating
DMI/SMBIOS 137
Universal Unique Identifier (UUID) 135
USB-device problems 154

V

video problems 153

W

Windows driver, LAN over USB 10
working inside the server
power on 43

Lenovo ThinkSystem SR530 Server (Xeon SP Gen 2)

Product Guide

Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.

Featuring the second generation of the Intel Xeon Processor Scalable Family (Xeon SP Gen 2), the SR530 server offers a balance of performance, capacity and value. The SR530 server supports up to two processors, up to 768 GB of 2933 MHz TruDDR4 memory, 8x 2.5-inch or 4x 3.5-inch drive bays with an extensive choice of SAS/SATA SSDs and SAS/SATA HDDs, and flexible I/O expansion options with a LOM slot and up to 3x PCIe slots.

The SR530 server offers basic software RAID or advanced hardware RAID protection and a wide range of networking options, including embedded LOM, selectable LOM, ML2, and PCIe network adapters. The next-generation Lenovo XClarity Controller, which is built into the SR530 server, provides advanced service processor control, monitoring, and alerting functions.

The following figure shows the ThinkSystem SR530 server with 3.5-inch front hot-swap drives. Other drive configurations are also available.



Figure 1. Lenovo ThinkSystem SR530 with 3.5-inch hot-swap drives

Did you know?

The SR530 server delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies that can deliver 96% (Titanium) or 94% (Platinum) efficiency at 50% load when connected to a 200 - 240 V AC power source.

The SR530 server is designed to meet ASHRAE A4 standards (up to 45 °C) in select configurations, which enable customers to lower energy costs, while still maintaining world-class reliability.

Key features

The SR530 server offers a balance of processing power, expandability, and cost for small and medium businesses up to the large enterprise. Ease of use and comprehensive systems management tools help make deployment easier and efficient design improves your business environment and helps save operational costs.

Scalability and performance

The SR530 server offers numerous features to boost performance, improve scalability, and reduce costs:

- Improves productivity by offering superior system performance with the second generation of the Intel Xeon Processor Scalable Family with up to 22-core processors, up to 30.25 MB of last level cache (LLC), up to 2933 MHz memory speeds, and up to 10.4 GT/s Ultra Path Interconnect (UPI) links.
    - Support for up to two processors, 44 cores, and 88 threads allows to maximize the concurrent execution of multithreaded applications.
    - Intelligent and adaptive system performance with energy efficient Intel Turbo Boost 2.0 Technology allows CPU cores to run at maximum speeds during peak workloads by temporarily going beyond processor thermal design power (TDP).
    - Intel Hyper-Threading Technology boosts performance for multithreaded applications by enabling simultaneous multithreading within each processor core, up to two threads per core.
    - Intel Virtualization Technology integrates hardware-level virtualization hooks that allow operating system vendors to better utilize the hardware for virtualization workloads.
    - Intel Speed Select Technology provides improvements in server utilization and guaranteed per-core performance service levels with more granular control over processor performance.
    - Intel Deep Learning Boost (Vector Neural Network Instruction set [VNNI]) is designed to deliver significant, more efficient Deep Learning (Inference) acceleration for high-performance Artificial Intelligence (AI) workloads.
    - Intel Advanced Vector Extensions 512 (AVX-512) enable acceleration of enterprise-class and high performance computing (HPC) workloads.
- Helps maximize system performance for data intensive applications with up to 2933 MHz memory speeds and up to 768 GB of memory capacity.
- Offers flexible and scalable internal storage in a 1U rack form factor with up to 8x 2.5-inch drives for performance-optimized configurations or up to 4x 3.5-inch drives for capacity-optimized configurations, providing a wide selection of SAS/SATA HDDs/SSDs.
- Provides I/O scalability with a LOM slot and up to three PCI Express (PCIe) 3.0 I/O expansion slots in a 1U rack form factor.
- Reduces I/O latency and increases overall system performance with Intel Integrated I/O Technology that embeds the PCI Express 3.0 controller into the Intel Xeon Processor Scalable Family.

Availability and serviceability

The SR530 server provides many features to simplify serviceability and increase system uptime:

- Offers protection in the event of a non-correctable memory failure with Single Device Data Correction (SDDC, also known as Chipkill, requires x4-based DIMMs), Adaptive Double Device Data Correction (ADDDC, also known as Redundant Bit Steering [RBS], requires x4-based DIMMs and Intel Xeon Gold or Platinum processors), memory mirroring, and memory rank sparing.
- Provides easy access to upgrades and serviceable parts (such as processors, memory DIMMs, and adapter cards) with tool-less cover removal.
- Offers affordable data protection with software RAID and Simple Swap drives and advanced hardware RAID data redundancy with hot-swap drives.
- Provides availability for applications with redundant hot-swap power supplies and redundant non-hot-swap fans.
- Speeds up troubleshooting tasks to reduce service time with diagnostics built into the XClarity Provisioning Manager.

- Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
- Continuously monitors system parameters, triggers alerts, and performs recovery actions in case of failure to minimize downtime with Built-in XClarity Controller (XCC).
- Provides quick access to system status, firmware, network, health, and alerts information via Virtual Operator Panel from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access.

Manageability and security

Powerful systems management features simplify local and remote management of the SR530 server and deliver enterprise-class data protection:

- Provides advanced service processor control, monitoring, and alerting functions with XClarity Controller, a next generation service processor.
- Improves Unified Extensible Firmware Interface (UEFI) system setup, configuration, updates, simplified error handling, and operating system deployment with the embedded XClarity Provisioning Manager.
- Offers XClarity Essentials software tools that can help you set up, use, and maintain the server.
- Increases uptime, reduces costs, and improves productivity through advanced server management capabilities with Lenovo XClarity Administrator that provides comprehensive hardware management.
- Provides on-the-go monitoring and management of devices in XClarity Administrator from anywhere with the Lenovo XClarity mobile app, which can help improve efficiency and reduce downtime risks.
- Centralizes infrastructure resource management with Lenovo XClarity Integrators for VMware vCenter and Microsoft System Center, extending XClarity Administrator features to virtualization management software tools and enabling users to deploy and manage infrastructure end-to-end.
- Offers advanced cryptographic functionality (such as digital signatures and remote attestation) with an integrated Trusted Platform Module (TPM) or optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC).
- Keeps user data safe with Lenovo Business Vantage, a security software tool suite designed to work with the Trusted Cryptographic Module (available only in PRC).
- Offers enterprise-class data protection with advanced RAID and optional self-encrypting drives.
- Provides faster, stronger encryption with industry-standard AES NI support.
- Helps prevent certain classes of malicious buffer overflow attacks with Intel Execute Disable Bit functionality, when combined with a supporting operating system.
- Enhances security through hardware-based resistance to malicious software attacks with Intel Trusted Execution Technology, allowing an application to run in its own isolated space, protected from all other software running on a system.

Energy efficiency

The SR530 server offers the following energy-efficiency features to save energy, reduce operational costs, increase energy availability, and contribute to the green environment:

- Delivers impressive compute power per watt, featuring 80 PLUS Titanium and Platinum redundant power supplies.
- Enables customers to lower energy costs with design to meet ASHRAE A4 standards in select configurations.
- Reduces power drawn with Intel Intelligent Power Capability that powers individual processor elements on and off as needed.
- Helps reduce power consumption with variable speed fans.
- Helps achieve lower heat output and reduced cooling needs with Lenovo XClarity Energy Manager that provides advanced data center power notification, analysis, and policy-based management.

Components and connectors

The following figure shows the front of the SR530 server with four 3.5-inch drive bays.

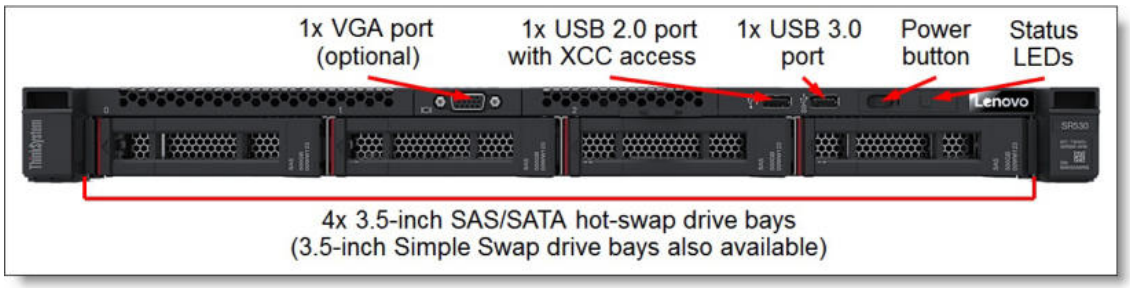


Figure 2. Front view of the SR530: 4x 3.5-inch drive bays

The following figure shows the front of the SR530 server with eight 2.5-inch drive bays.

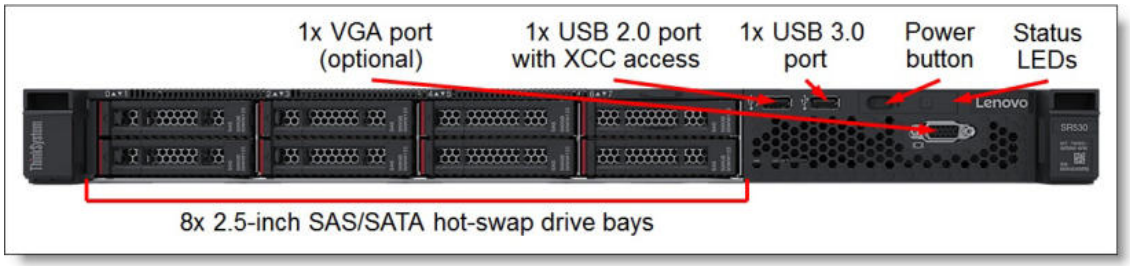


Figure 3. Front view of the SR530: 8x 2.5-inch drive bays

The front of the SR530 server includes the following components:

- Up to 8x 2.5-inch or 4x 3.5-inch hot-swap drive bays, or 4x 3.5-inch Simple Swap drive bays.
- One VGA port (optional).
- One USB 3.0 port.
- One USB 2.0 port with XClarity Controller access.
- Power button.
- Status LEDs.

The following figure shows the rear of the SR530 server with three PCIe low profile slots.

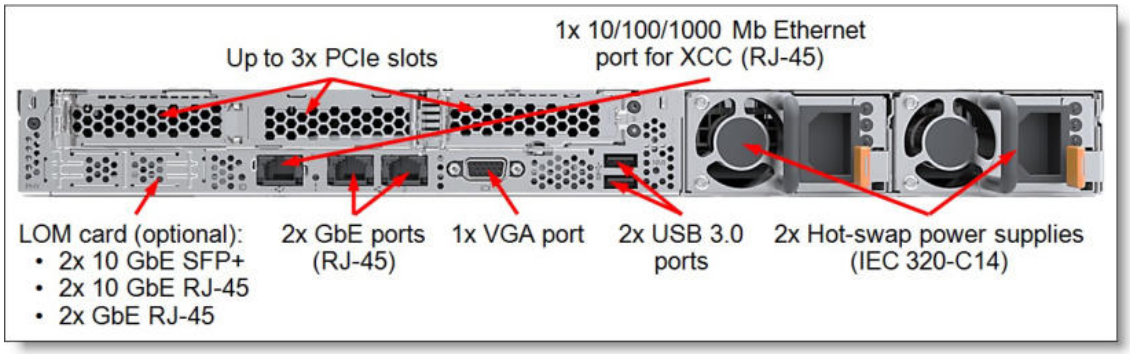


Figure 4. Rear view of the SR530

The rear of the SR530 server includes the following components:

- Up to three PCIe expansion slots (depending on the riser cards selected).
- One LOM card slot.
- One 1 GbE port for XClarity Controller.
- One VGA port.
- Two USB 3.0 ports.
- Up to two hot-swap power supplies.

The following figure shows the locations of key components inside the SR530 server.

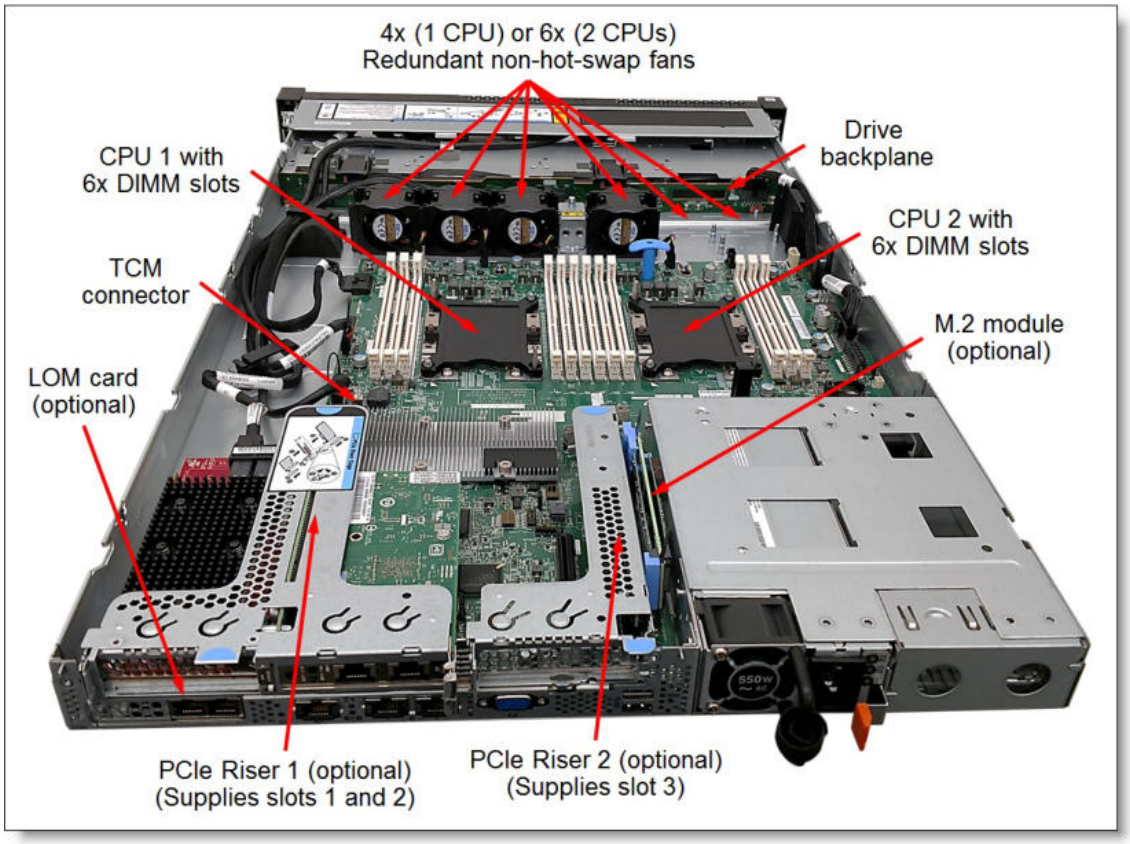


Figure 5. Internal view of the SR530

The following key components are located inside the SR530 server:

- Up to two processors.
- 12 DIMM slots (6 DIMM slots per processor).
- Drive backplanes.
- One M.2 module connector.
- One LOM card connector.
- Two slots for PCIe riser cards.
- One TCM connector.
- Four (one processor) or six (two processors) non-hot-swap system fans.

System specifications

The following table lists the system specifications for the SR530 server.

Table 1. SR530 system specifications

Attribute	Specification
Machine types	7X07 - 1 year warranty 7X08 - 3 year warranty
Form factor	1U rack-mount.
Processor	Up to two Intel Xeon Gen 2 Bronze, Silver, Gold, or Platinum processors: • Up to 22 cores (1.9 GHz core speeds) • Up to 3.8 GHz core speeds (4 cores) • Two UPI links up to 10.4 GT/s each • Up to 30.25 MB cache • Up to 2933 MHz memory speed

Attribute	Specification
Chipset	Intel C622.
Memory	Up to 12 DIMM sockets (6 DIMMs per processor; six memory channels per processor with one DIMM per channel) with support for the following TruDDR4 RDIMM types and capacities: • 8 GB, 16 GB, 32 GB, and 64 GB 2933 MHz. • 16 GB and 32 GB 2666 MHz.
Memory protection	Error correction code (ECC), SDDC (for x4-based memory DIMMs), ADDDC (for x4-based memory DIMMs, requires Intel Xeon Gold or Platinum processors), memory mirroring, memory rank sparing, patrol scrubbing, and demand scrubbing.
Memory capacity	Up to 768 GB with 12x 64 GB RDIMMs (Up to 384 GB per processor).
Drive bays	• 4 LFF SATA Simple Swap drive bays • 4 LFF SAS/SATA hot-swap drive bays • 8 SFF SAS/SATA hot-swap drive bays

Internal storage capacity	• 2.5-inch drives:
	  ◦ 122.88TB using 8x 15.36TB 2.5-inch SAS/SATA SSDs
	  ◦ 19.2TB using 8x 2.4TB 2.5-inch HDDs
	• 3.5-inch drives:
	  ◦ 72TB using 4x 18TB 3.5-inch HDDs
	  ◦ 30.72TB using 4x 7.68TB 3.5-inch SAS/SATA SSDs

Storage controller	6 Gbps SATA
	• Non-RAID: Onboard SATA AHCI
	• RAID 0/1/10/5: Onboard SATA RAID (Intel RSTe)
	
	12 Gbps SAS/6 Gbps SATA RAID
	• RAID 0/1/10/5/50:
	  ◦ RAID 530-8i
	  ◦ RAID 730-8i 1GB Cache
	• RAID 0/1/10/5/50/6/60:
	  ◦ RAID 730-8i 2GB Flash
	  ◦ RAID 930-8i 2GB Flash
	  ◦ RAID 930-16i 4GB or 8GB Flash
	
	12 Gbps SAS/6 Gbps SATA non-RAID: 430-8i HBA

Optical drive bays	None. Support for an external USB DVD RW Optical Disk Drive (SeeOptical drives).

Network interfaces	• 2x Integrated 1 GbE RJ-45 ports (no 10/100 Mb support)
	• Onboard LOM slot for up to two additional 1/10 Gb Ethernet ports:
	  ◦ 2x 1 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE RJ-45 ports (no 10/100 Mb support)
	  ◦ 2x 10 GbE SFP+ ports (no 10/100 Mb support)
	• Optional Mezzanine LOM (ML2) slot for dual-port 10 GbE cards with SFP+ or RJ-45 connectors.
	• 1x RJ-45 10/100/1000 Mb Ethernet systems management port.

I/O expansion slots	Up to three slots depending on the riser cards installed. The slots are as follows: • Slot 1: PCIe 3.0 x8; low profile • Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length • Slot 3: PCIe 3.0 x8 or x16; low profile PCIe x16 slot 3 requires the second processor to be installed.
Ports	• Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. • Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
Cooling	Four (one processor) or six (two processors) non-hot-swap system fans with N+1 redundancy.
Power supply	Up to two redundant hot-swap 550 W or 750 W (100 - 240 V) High Efficiency Platinum or 750 W (200 - 240 V) High Efficiency Titanium AC power supplies. HVDC support (PRC only).

Attribute	Specification
Video	Matrox G200 with 16 MB memory integrated into the XClarity Controller. Maximum resolution is 1920x1200 at 60 Hz with 32 bits per pixel.
Hot-swap parts	Drives (select models) and power supplies.
Systems management	XClarity Controller (XCC) Standard, Advanced, or Enterprise (Pilot 4 chip), proactive platform alerts, XClarity Provisioning Manager, XClarity Essentials, XClarity Administrator, XClarity Integrators for VMware vCenter and Microsoft System Center, XClarity Energy Manager, Capacity Planner.
Security features	Power-on password, administrator's password, secure firmware updates, Trusted Platform Module (TPM) 1.2 or 2.0 (configurable UEFI setting). Optional lockable front bezel. Optional Trusted Cryptographic Module (TCM) or Nationz TPM (available only in PRC). Optional Lenovo Business Vantage security software (available only in PRC).
Operating systems	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. See the Operating systems section for specifics.
Warranty	One-year (7X07) or three-year (7X08) customer-replaceable unit (CRU) and onsite limited warranty with 9x5 Next Business Day Parts Delivered.
Service and support	Optional service upgrades are available through Lenovo Services: 2-hour or 4-hour response time, 6-hour or 24-hour committed service repair, warranty extension up to 5 years, 1-year or 2-year post-warranty extensions, YourDrive Your Data, Enterprise Software Support, and Basic Hardware Installation Services.
Dimensions	Width: 435 mm (17.1 in.), height: 43 mm (1.7 in.), depth: 750 mm (29.5 in.). See Physical specifications for details.
Weight	Minimum configuration: 10.2 kg (22.5 lb), maximum: 16 kg (35.3 lb)

Models

ThinkSystem SR530 models can be configured by using the Lenovo Data Center Solution Configurator (DCSC).

Configure-to-order (CTO) models are used to create models with factory-integrated server customizations. For CTO models, two base CTO models are available for the SR530 as listed in the following table, CTO1WW and CTOLWW:

- The CTO1WW base CTO model is for general business and is selectable by choosing **General Purpose** mode in DCSC.
- The CTOLWW base model is intended for High Performance Computing (HPC) and Artificial Intelligence (AI) configurations and solutions, including configurations for Lenovo Scalable Infrastructure (LeSI), and is enabled using either the **HPC & AI LeSI Solutions** mode or **HPC & AI ThinkSystem Hardware** mode in DCSC. CTOLWW configurations can also be built using System x and Cluster Solutions Configurator (x-config).

Preconfigured server models may also be available for the SR530, however these are region-specific; that is, each region may define their own server models, and not all server models are available in every region.

The following table lists the base CTO models of the ThinkSystem SR530 server.

Table 2. Base CTO models

Description	Machine Type/Model General purpose	Machine Type/Model for HPC and AI
ThinkSystem SR530 - 3 year Warranty	7X08CTO1WW	7X08CTOLWW
ThinkSystem SR530 - 1 year Warranty	7X07CTO1WW	7X07CTOLWW

The following table lists the base chassis for CTO models of the SR530 server.

Table 3. Base chassis for CTO models

Feature code	Description
AV0T	ThinkSystem SR530 3.5" Chassis with 4 Bays
AV0S	ThinkSystem SR530 2.5" Chassis with 8 Bays

All models of the SR530 server are shipped with the following items:

- *Rack Installation Guide*
- *Electronic Publications Flyer*

Models table conventions: The model tables shown in this section use the following conventions:

- XClarity Controller: "S" = Standard, "A" = Advanced, "E" = Enterprise.
- Front VGA port: "Y" = Included; "N" = Not included, optional.
- Tool-less Rail Kit: "Y" = Included; "N" = Not included, optional.
- Cable Management Arm (CMA): "Y" = Included; "N" = Not included, optional.
- Power cord:
  - "R1" = 1.5 m C13-C14 rack power cable.
  - "R2" = 2.8 m C13-C14 rack power cable.
  - "L2" = 2.8 m line cord.
  - "N" = Not included; see Power supplies and cables for the ordering information.

The following tables list the models of the SR530 server for the following regions:

- Brazil
- Latin America (except Brazil)
- Europe, Middle East, and Africa (EMEA)
- India
- Hong Kong, Taiwan, Korea
- Japan
- Association of Southeast Asian Nations (ASEAN)
- Australia and New Zealand

Table 4. SR530 server models: Brazil

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Brazil													
7X08A0A1BR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
TopSeller models - Brazil													
7X08100QBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x SATA AHCI	4 / 4 SS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A0A2BR	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2
7X08A09YBR	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09ZBR	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0APBR	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	N	Y	N	L2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 5. SR530 server models: Latin America (except Brazil)

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
TopSeller models - Latin America (except Brazil)													
7X08A09WLA	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A09XLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 FH	1x 550W	S	Y	Y	N	R2
7X08A0AQLA	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2933MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	2x 1Gb RJ-45	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	Y	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 6. SR530 server models: EMEA

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - EMEA													
7X08A0ACEA	1x 3206R 8C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	R2
7X08A075EA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AZEA	1x 4208 8C 85W 2.1GHz	1x 32GB (x4) 2933MHz	None	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	N	R2
7X08A0ADEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AHEA	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A078EA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A06WEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	S	N	Y	N	R2
7X08A07FEA	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AEEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AJEA	1x 4210R 10C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A07CEA	1x 4214 12C 85W 2.2GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0AKEA	1x 4214R 12C 100W 2.4GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A070EA	1x 4216 16C 100W 2.1GHz	1x 16GB (x8) 2666MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2
7X08A0ALEA	1x 5218R 20C 125W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	A	N	Y	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 7. SR530 server models: India

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - India													
7X08A08TSG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07USG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A07WSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A084SG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07YSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A079SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06VSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07SSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07JSG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ASG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08PSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A098SG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A077SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A095SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A07RSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08VSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08WSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A06USG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A094SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A089SG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A09ESG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2
7X08A08KSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	R2

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 8. SR530 server models: Hong Kong, Taiwan, Korea

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Hong Kong, Taiwan, Korea													
7X08A09CCN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085CN	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08100VCN	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	Y	N	Y
7X08A071CN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YCN	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09BCN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080CN	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CCN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A082CN	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NCN	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09DCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07NCN	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A088CN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GCN	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GCN	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A087CN	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08MCN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092CN	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06XCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07KCN	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 9. SR530 server models: Japan

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Japan													
7X08A0AWJP	1x 5218R 20C 125W 2.1GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
TopSeller models - Japan													
7X08A08AJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08DJP	1x 3204 6C 85W 1.9GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08EJP	1x 4208 8C 85W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07HJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08SJP	1x 4210 10C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08QJP	1x 4214 12C 85W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07QJP	1x 4215 8C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07LJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A07MJP	1x 4216 16C 100W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08HJP	1x 5215 10C 85W 2.5GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08FJP	1x 5217 8C 115W 3.0GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08YJP	1x 5218 16C 125W 2.3GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A090JP	1x 5220 18C 125W 2.2GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A08UJP	1x 5222 4C 105W 3.8GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A096JP	1x 6230 20C 125W 2.1GHz	1x 16GB (x4) 2666MHz	1x RAID 730-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W	A	N	Y	N	N
7X08A0AXJP	1x 3206R 8C 85W 1.9GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AYJP	1x 4210R 10C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N
7X08A0AVJP	1x 4214R 12C 100W 2.4GHz	1x 16GB (x4) 2666	None	None / 8 SFF	Open bay	Open slot	None	1x 550W Platinum	A	N	Y	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 10. SR530 server models: ASEAN

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - ASEAN													
7X08A099SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A086SG	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06ZSG	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XSG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A081SG	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ZSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DSG	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A083SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A093SG	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07VSG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07ESG	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RSG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A073SG	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A097SG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07PSG	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07TSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BSG	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A09FSG	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A091SG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BSG	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Table 11. SR530 server models: Australia and New Zealand

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
Relationship models - Australia and New Zealand (1-year warranty)													
7X07A00VAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2666MHz	None	No bays / 8 HS SFF	Open bay	Open slot	None	1x 550W	S	Y	Y	N	R2
Relationship models - Australia and New Zealand (3-year warranty)													
7X08A099AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A085AU	1x 3204 6C 85W 1.9GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A071AU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A06YAU	1x 4208 8C 85W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08XAU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A080AU	1x 4210 10C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08CAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07DAU	1x 4214 12C 85W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07XAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08NAU	1x 4215 8C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A0B0AU	1x 4216 16C 100W 2.1GHz	1x 32GB(x4) 2933MHz	1x RAID 930-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 550W Platinum	E	Y	Y	N	Y
7X08A07VAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07EAU	1x 4216 16C 100W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08RAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08GAU	1x 5215 10C 85W 2.5GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08JAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07GAU	1x 5217 8C 115W 3.0GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A076AU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08BAU	1x 5218 16C 125W 2.3GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A08LAU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A092AU	1x 5220 18C 125W 2.2GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N

Model number	Intel Xeon processor* (2 max)	Memory DIMM (12 max)	Storage controller	Drive bays (std / max)	Drives	Eth. LOM	I/O slots (3 max)^	Power supply (2 max)	XClarity Controller	Front VGA port	Tool-less Rail Kit	CMA	Power cord
7X08A06XAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	4 / 4 HS LFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
7X08A07BAU	1x 6230 20C 125W 2.1GHz	1x 8GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	S	N	N	N	N
TopSeller models - Australia and New Zealand (3-year warranty)													
7X08A09GAU	1x 3204 6C 85W 1.9GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09HAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09LAU	1x 4208 8C 85W 2.1GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09KAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09NAU	1x 4210 10C 85W 2.2GHz	1x 16GB (x8) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09MAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 530-8i	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N
7X08A09JAU	1x 4210 10C 85W 2.2GHz	1x 32GB (x4) 2933MHz	1x RAID 930-8i 2GB	8 / 8 HS SFF	Open bay	Open slot	1x PCIe x8 1x PCIe x16 LP	1x 750W Platinum	E	N	Y	Y	N

* Processor details: Processor quantity and model, cores, thermal design power (TDP), and core speed.
^ The server supports up to three I/O slots on the riser cards. An internal PCIe storage controller occupies the PCIe slot 1. The onboard SATA RAID controller does not consume a PCIe slot.

Processors

The SR530 server supports one or two Intel Xeon Bronze, Silver, Gold, or Platinum processors of up to 125 W TDP. The following table lists the specifications of the processors for the SR530 server.

Processor specifications table abbreviations:

- UPI: Ultra Path Interconnect
- TDP: Thermal Design Power
- HT: Hyper-Threading
- TB: Turbo Boost 2.0
- VT-x: Virtualization Technology
- VT-d: Virtualization Technology for Directed I/O
- SST-PP: Speed Select Technology - Performance Profile
- FMA: Fused-Multiply Add (AVX-512)
- RAS: Reliability, Availability, and Serviceability
    - Std: Standard RAS
    - Adv: Advanced RAS

Table 12. Processor specifications

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
Intel Xeon Bronze processors														
3204	6 / 6	1.9 / 1.9 GHz	8.25 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	Std

CPU model	Cores / threads	Core speed (Base / TB Max)	Cache	Max DDR4 speed	Max memory capacity per socket	UPI speed	TDP	HT	TB	VT-x	VT-d	SST-PP	FMA units	RAS
3206R	8 / 8	1.9 / 1.9 GHz	11 MB	2133 MHz	1 TB	9.6 GT/s	85 W	N	N	Y	Y	N	1	
Intel Xeon Silver processors														
4208	8 / 16	2.1 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4209T	8 / 16	2.2 / 3.2 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	70 W	Y	Y	Y	Y	N	1	Std
4210	10 / 20	2.2 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4210R	10 / 20	2.4 / 3.2 GHz	13.75 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4214R	12 / 24	2.4 / 3.5 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
4214Y	12 / 24	2.2 / 3.2 GHz	16.5 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	Y	1	Std
	10 / 20	2.3 / 3.2 GHz												
	8 / 16	2.4 / 3.2 GHz												
4215	8 / 16	2.5 / 3.5 GHz	11 MB	2400 MHz	1 TB	9.6 GT/s	85 W	Y	Y	Y	Y	N	1	Std
4216	16 / 32	2.1 / 3.2 GHz	22 MB	2400 MHz	1 TB	9.6 GT/s	100 W	Y	Y	Y	Y	N	1	Std
Intel Xeon Gold processors														
5215	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	1 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5215L	10 / 20	2.5 / 3.4 GHz	13.75 MB	2666 MHz	4.5 TB	10.4 GT/s	85 W	Y	Y	Y	Y	N	1	Adv
5217	8 / 16	3.0 / 3.7 GHz	11 MB	2666 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	1	Adv
5218	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218B	16 / 32	2.3 / 3.9 GHz	22 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218R	20 / 40	2.1 / 4.0 GHz	27.5 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5218T	16 / 32	2.1 / 3.8 GHz	22 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5220	18 / 36	2.2 / 3.9 GHz	24.75 MB	2666 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220S	18 / 36	2.7 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	1	Adv
5220T	18 / 36	1.9 / 3.9 GHz	24.75 MB	2667 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	1	Adv
5222	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv
6209U	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	N/A	125 W	Y	Y	Y	Y	N	2	Adv
6222V	20 / 40	1.8 / 3.6 GHz	27.5 MB	2400 MHz	1 TB	10.4 GT/s	115 W	Y	Y	Y	Y	N	2	Adv
6226	12 / 24	2.7 / 3.7 GHz	19.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230N	20 / 40	2.3 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6230T	20 / 40	2.1 / 3.9 GHz	27.5 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
6238T	22 / 44	1.9 / 3.7 GHz	30.25 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
Intel Xeon Platinum processors														
8253	16 / 32	2.2 / 3.0 GHz	22 MB	2933 MHz	1 TB	10.4 GT/s	125 W	Y	Y	Y	Y	N	2	Adv
8256	4 / 8	3.8 / 3.9 GHz	16.5 MB	2933 MHz	1 TB	10.4 GT/s	105 W	Y	Y	Y	Y	N	2	Adv

Configuration notes:

- The Intel Xeon Gold 5218 and 5218B processors have similar specifications; however, they use different silicon designs and cannot be mixed in the same system.
- The processors that support SST-PP offer three distinct operating points that are defined by a core count with a base speed associated with that core count. The operating point is static, it is selected during the boot process and cannot be changed at runtime.

For the SR530 server models that come with one processor, the second processor can be ordered, if required (see the following table for ordering information). The second processor must be of the same model as the first processor. The second processor option includes a processor and a heatsink; two additional system fans are not included and need to be purchased with the second processor (see Cooling for details).

Table 13. Processor options

Description	Part number	Feature code*
Intel Xeon Bronze processors		
SR530/SR570/SR630 Intel Xeon Bronze 3204 6C 85W 1.9GHz Processor w/o FAN	4XG7A37939	B4HU
SR530/SR570/SR630 Intel Xeon Bronze 3206R 8C 85W 1.9GHz Processor w/o FAN	4XG7A37990	B7N3
Intel Xeon Silver processors		
SR530/SR570/SR630 Intel Xeon Silver 4208 8C 85W 2.1GHz Processor w/o FAN	4XG7A37936	B4HT
SR530/SR570/SR630 Intel Xeon Silver 4209T 8C 70W 2.2GHz Processor w/o FAN	4XG7A37945	B4P4
SR530/SR570/SR630 Intel Xeon Silver 4210 10C 85W 2.2GHz Processor w/o FAN	4XG7A37933	B4HS
SR530/SR570/SR630 Intel Xeon Silver 4210R 10C 100W 2.4GHz Processor w/o FAN	4XG7A37988	B7N5
SR530/SR570/SR630 Intel Xeon Silver 4214 12C 85W 2.2GHz Processor w/o FAN	4XG7A37930	B4HR
SR530/SR570/SR630 Intel Xeon Silver 4214R 12C 100W 2.4GHz Processor w/o FAN	4XG7A37987	B7N6
SR530/SR570/SR630 Intel Xeon Silver 4214Y 12/10/8C 85W 2.2GHz Processor w/o FAN	4XG7A37942	B4NW
SR530/SR570/SR630 Intel Xeon Silver 4215 8C 85W 2.5GHz Processor w/o FAN	4XG7A37927	B4HQ
SR530/SR570/SR630 Intel Xeon Silver 4216 16C 100W 2.1GHz Processor w/o FAN	4XG7A37924	B4HP
Intel Xeon Gold processors		
SR530/SR570/SR630 Intel Xeon Gold 5215 10C 85W 2.5GHz Processor w/o FAN	4XG7A37917	B4HN
SR530/SR570/SR630 Intel Xeon Gold 5215L 10C 85W 2.5GHz Processor w/o FAN	4XG7A37911	B4P9
SR530/SR570 Intel Xeon Gold 5217 8C 115W 3.0GHz Processor w/o FAN	4XG7A37921	B4HM
SR530/SR570/SR630 Intel Xeon Gold 5218 16C 125W 2.3GHz Processor w/o FAN	4XG7A37896	B4HL
SR530/SR570/SR630 Intel Xeon Gold 5218B 16C 125W 2.3GHz Processor w/o FAN	4XG7A37959	B6BS
SR530/SR570/SR630 Intel Xeon Gold 5218R 20C 125W 2.1GHz Processor w/o FAN	4XG7A63296	BAZS
SR530/SR570 Intel Xeon Gold 5218T 16C 105W 2.1GHz Processor w/o FAN	4XG7A38017	B4P3
SR530/SR570/SR630 Intel Xeon Gold 5220 18C 125W 2.2GHz Processor w/o FAN	4XG7A37893	B4HK
SR530/SR570/SR630 Intel Xeon Gold 5220S 18C 125W 2.7GHz Processor w/o FAN	4XG7A38018	B6CW
SR530/SR570 Intel Xeon Gold 5220T 18C 105W 1.9GHz Processor w/o FAN	4XG7A38004	B6CQ
SR530/SR570 Intel Xeon Gold 5222 4C 105W 3.8GHz Processor w/o FAN	4XG7A37953	B5S1
Intel Xeon Gold 6209U 20C 125W 2.1GHz Processor	None**	B6CX
SR530/SR570/SR630 Intel Xeon Gold 6222V 20C 115W 1.8GHz Processor w/o FAN	4XG7A38022	B6CV
SR530/SR570/SR630 Intel Xeon Gold 6226 12C 125W 2.7GHz Processor w/o FAN	4XG7A38020	B6CL
SR530/SR570/SR630 Intel Xeon Gold 6230 20C 125W 2.1GHz Processor w/o FAN	4XG7A37890	B4HJ
SR530/SR570 Intel Xeon Gold 6230N 20C 125W 2.3GHz Processor w/o FAN	4XG7A38029	B5RY
SR530/SR570 Intel Xeon Gold 6230T 20C 125W 2.1GHz Processor w/o FAN	4XG7A38007	B6CP
SR530/SR570 Intel Xeon Gold 6238T 22C 125W 1.9GHz Processor w/o FAN	4XG7A37908	B4P2
Intel Xeon Platinum processors		
SR530/SR570/SR630 Intel Xeon Platinum 8253 16C 125W 2.2GHz Processor w/o FAN	4XG7A37899	B5RZ
SR530/SR570 Intel Xeon Platinum 8256 4C 105W 3.8GHz Processor w/o FAN	4XG7A37949	B5S2

* For CTO configurations, the feature code represents a processor, and fans and heatsinks are derived by the configuration tool.
** Factory-installed only; no field upgrade. Supported in the uniprocessor configurations only.

Memory

The SR530 server supports up to 6 TruDDR4 memory RDIMMs when one processor is installed and up to 12 RDIMMs when two processors are installed for a total of up to 768 GB of memory capacity (up to 384 TB per processor). Each processor has six memory channels, and there is a one DIMM per channel.

Lenovo TruDDR4 memory uses the highest-quality components sourced from Tier 1 DRAM suppliers and only memory that meets strict requirements is selected. It is compatibility tested and tuned on every ThinkSystem server to maximize performance and reliability.

TruDDR4 memory has a unique signature programmed into the DIMM, which enables Lenovo servers to verify whether the memory installed is qualified and supported. Lenovo qualified and supported TruDDR4 memory is covered by Lenovo warranty, and service and support provided worldwide.

The following memory protection technologies are supported by the processor's integrated memory controllers:

- ECC
- SDDC (for x4-based memory DIMMs)
- ADDDC (for x4-based memory DIMMs; Gold and Platinum processors only)
- Memory mirroring
- Memory rank sparing
- Patrol scrubbing
- Demand scrubbing

The following table lists memory options available for the SR530 server.

Table 14. Memory options

Description	Part number	Feature code	Maximum quantity*
RDIMMs - 2933 MHz			
ThinkSystem 8GB TruDDR4 2933MHz (1Rx8 1.2V) RDIMM	4ZC7A08706	B4H1	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (1Rx4 1.2V) RDIMM	4ZC7A08707	B4LY	6 / 12
ThinkSystem 16GB TruDDR4 2933MHz (2Rx8 1.2V) RDIMM	4ZC7A08708	B4H2	6 / 12
ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08709	B4H3	6 / 12
ThinkSystem 64GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM	4ZC7A08710	B4H4	6 / 12
RDIMMs - 2666 MHz			
ThinkSystem 16GB TruDDR4 2666 MHz (1Rx4 1.2V) RDIMM	7X77A01302	AUNB	6 / 12
ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM	7X77A01303	AUNC	6 / 12
ThinkSystem 32GB TruDDR4 2666 MHz (2Rx4 1.2V) RDIMM	7X77A01304	AUND	6 / 12

* The maximum quantity shown is with one processor / two processors.

Configuration notes:

- All RDIMMs in the server operate at the same speed, which is determined as the lowest value of:
  - RDIMM rated speed (2666 MHz or 2933 MHz).
  - Memory speed supported by the specific processor (2133 MHz, 2400 MHz, 2666 MHz, or 2933 MHz).

  Note: Maximum memory speed can be achieved when Max performance mode is enabled in UEFI.
- Mixing RDIMMs of different ranks (single- or dual-rank), DRAM chip types (x4 or x8), speeds (2666 MHz or 2933 MHz), and capacities (8 GB, 16 GB, 32 GB, or 64 GB) is supported in the independent channel mode (the default operational mode).
- For server configurations with memory protection, the following rules apply:
  - Single Device Data Correction (SDDC) works only in the independent channel mode and supports only x4-based memory DIMMs.
  - Adaptive Double Device Data Correction (ADDDC) works with x4-based memory DIMMs and requires two DIMM ranks per channel, Intel Xeon Gold or Platinum processors, and the Closed Page memory access mode.
  - If memory mirroring is used, then DIMMs must be installed in quantities of 2 or 4 per processor for mirroring across two memory channels, or in quantities of 3 or 6 per processor for mirroring across three memory channels. Mixing two- and three-channel mirroring in the server is allowed (one processor uses two-channel mirroring, and another processor uses three-channel mirroring). All DIMMs in the server must be identical in type and size.
  - If memory rank sparing is used, then a minimum of two ranks must be installed per populated channel (a least one dual-rank or quad-rank DIMM; single-rank DIMMs are not supported). With rank sparing, one rank in each populated channel is reserved as spare memory for other ranks on the same channel. All DIMMs in the server must be identical in type and size.
  - SDDC, memory mirroring, and memory rank sparing modes are mutually exclusive. Only one operational memory mode can be enabled on the server.

Internal storage

The SR530 server supports the following internal drive bay configurations:

1. 4 LFF SATA Simple Swap drive bays
2. 4 LFF SAS/SATA hot-swap drive bays
3. 8 SFF SAS/SATA hot-swap drive bays

In addition, the SR530 server models can be configured with one or two internal M.2 SATA SSDs. The server also supports configurations without drive bays.

The following figure shows the internal drive bay configurations.

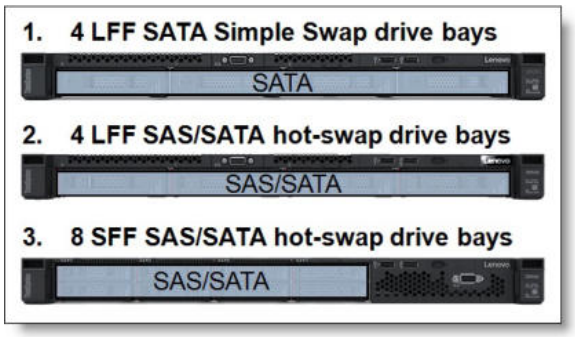


Figure 6. Internal drive bay configurations

The following table lists the internal storage options for the SR530 server.

Table 15. Internal storage options

Description	Part number	Feature code	Maximum quantity
Factory-installed backplane kits			
ThinkSystem 1U 3.5" SATA/SAS 4-Bay Backplane	None*	AUW8	1
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane	None*	AUWB	1
Backplane kit field upgrade options			
ThinkSystem 1U 2.5" SATA/SAS 8-Bay Backplane Kit	7XH7A05896	None**	1
M.2 enablement kits			
ThinkSystem M.2 Enablement Kit	7Y37A01092	AUMU	1
ThinkSystem M.2 with Mirroring Enablement Kit	7Y37A01093	AUMV	1

* These backplane kits can be factory-installed in standard or custom (CTO or Special Bid) models, and they might not have an option part number assigned.
** Field upgrade only; used for upgrading models without any drive bays to 8x 2.5" SAS/SATA hot-swap drive bays.

M.2 Enablement Kit configuration notes:

- The M.2 Enablement Kit (7Y37A01092) supports one M.2 SATA SSD which is connected to the SATA port on the Intel Platform Controller Hub (PCH).
- The M.2 with Mirroring Enablement Kit (7Y37A01093) is connected to the Intel PCH via the PCIe link, and the kit supports two M.2 SATA SSDs that can be configured in a RAID-1 or RAID-0 drive group, or they can operate as two separate drives.

The following tables list supported internal storage configurations with the SAS/SATA backplanes.

Table 16. Internal storage configurations

Drive bay configuration	Backplane kit type and quantity		Storage controller type and quantity*
	4x 3.5" SATA/SAS	8x 2.5" SATA/SAS	
4x 3.5" chassis (Feature code AV0T)			
4x 3.5-in. SATA Simple Swap	0	0	Onboard AHCI (non-RAID) / Intel RSTe (RAID) (4)
4x 3.5-in. SAS/SATA hot-swap	1	0	1x RAID 530-8i/730-8i 1GB (4)
			1x RAID 730-8i 2GB/930-8i (4)
			1x 430-8i HBA (4)
8x 2.5" chassis (Feature code AV0S)			
8x 2.5-in. SAS/SATA hot-swap	0	1	1x RAID 530-8i/730-8i 1GB (8)
			1x RAID 730-8i 2GB/930-8i/930-16i (8)
			1x 430-8i HBA (8)

* The number in brackets (x) specifies the quantity of drive bays connected to each of the controllers.

Configuration note: Models without any drive bays are based on the 8x 2.5" chassis (feature code AV0S), and they support adding drive bays by using the 2.5" 8-drive backplane kit (7XH7A05896).

Controllers for internal storage

The following table lists the storage controllers and options for internal storage of the SR530 server.

Table 17. RAID controllers and HBAs for internal storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
6 Gbps SATA controllers				
Onboard AHCI (non-RAID) / Intel RSTe (RAID)	Onboard*	Onboard*	1	-
12 Gb SAS/SATA RAID controllers				
ThinkSystem RAID 530-8i PCIe 12Gb Adapter	7Y37A01082	AUNG	1	1
ThinkSystem RAID 730-8i 1GB Cache PCIe 12Gb Adapter	7Y37A01083	AUNH	1	1
ThinkSystem RAID 730-8i 2GB Flash PCIe 12Gb Adapter	4Y37A09722	B4RQ	1	1
ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter	7Y37A01084	AUNJ	1	1
ThinkSystem RAID 930-16i 4GB Flash PCIe 12Gb Adapter	7Y37A01085	AUNK	1	1
ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter	4Y37A09721	B31E	1	1
12 Gb SAS/SATA non-RAID HBAs				
ThinkSystem 430-8i SAS/SATA 12Gb HBA	7Y37A01088	AUNL	1	1

* The onboard SATA controller integrated into the Intel C622 Platform Controller Hub (PCH) supports non-RAID (JBOD) AHCI mode or a hardware-assist, software RAID feature (Intel Rapid Storage Technology Enterprise [RSTe]).

Configuration note: Low profile SAS RAID controllers and HBAs for internal storage are supported in the PCIe x8 slot 1 supplied by the riser card 1.

The following table summarizes features of supported SAS/SATA storage controllers.

Table 18. Storage controller features and specifications (LP = Low profile, FHHL = Full-height half-length)

Feature	Intel RSTe	RAID 530-8i	RAID 730-8i 1GB	RAID 730-8i 2GB	RAID 930-8i	RAID 930-16i	430-8i HBA
Form factor	Onboard	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP	PCIe LP
SAS controller	None	SAS3408	SAS3108	SAS3108	SAS3508	SAS3516	SAS3408
Host interface	PCH	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	6 Gb SATA	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	8	8	8	16	8
Connector type	SATA x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4	SFF-8643 x4
Number of connectors	2	2	2	2	2	4	2
Drive interface	SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD	HDD, SSD, SED	HDD, SSD	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED	HDD, SSD, SED*
Hot-swap drive support	No	Yes	Yes	Yes	Yes	Yes	Yes
Number of drives	8	8	8	8	8	16^	8
RAID levels	0/1/10/5	0/1/10/5/50	0/1/10/5/50	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	0/1/10/5/ 50/6/60	None
JBOD mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cache	None	None	1 GB	2 GB	2 GB	4 GB; 8 GB	None
Cache protection	None	None	None	Flash backup (Included)	Flash backup (Included)	Flash backup (Included)	None
SED key management (SafeStore)	No	Yes	No	Yes	Yes	Yes	No
SSD I/O acceleration (FastPath)	No	Yes	No	Yes	Yes	Yes	No
SSD Caching (CacheCade Pro 2.0)	No	No	No	No	No**	No**	No
Consistency check	Yes	Yes	Yes	Yes	Yes	Yes	No
Patrol read	Yes	Yes	Yes	Yes	Yes	Yes	No
Online capacity expansion	Yes	Yes	Yes	Yes	Yes	Yes	No
Online RAID level migration	Yes	Yes	Yes	Yes	Yes	Yes	No
Global Hot Spare	Yes	Yes	Yes	Yes	Yes	Yes	No
Auto-rebuild	Yes	Yes	Yes	Yes	Yes	Yes	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
^ Up to 8 drives is supported by the RAID 930-16i in the SR530 server.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

Important: The onboard Intel RSTe is not supported by virtualization hypervisors, including VMware vSphere (ESXi), Linux KVM, Xen, and Microsoft Hyper-V.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Drives for internal storage

The following tables list the hard disk drive and solid-state drive options for the internal disk storage of the server.

2.5-inch hot-swap drives:

- 2.5-inch hot-swap 12 Gb SAS HDDs
- 2.5-inch hot-swap 6 Gb SATA HDDs
- 2.5-inch hot-swap 12 Gb SAS SSDs
- 2.5-inch hot-swap 6 Gb SATA SSDs

3.5-inch hot-swap drives:

- 3.5-inch hot-swap 12 Gb SAS HDDs
- 3.5-inch hot-swap 6 Gb SATA HDDs
- 3.5-inch hot-swap 12 Gb SAS SSDs
- 3.5-inch hot-swap 6 Gb SATA SSDs

Simple-swap drives:

- 3.5-inch simple-swap 6 Gb SATA HDDs

M.2 drives:

- M.2 SATA drives

M.2 drive support: The use of M.2 drives requires an additional adapter as described in the Internal storage section.

Table 19. 2.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00024	AULY	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00025	AULZ	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00026	AUM0	ThinkSystem 2.5" 900GB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00027	AUM1	ThinkSystem 2.5" 1.2TB 10K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00028	AUM2	ThinkSystem 2.5" 1.8TB 10K SAS 12Gb Hot Swap 512e HDD	8
7XB7A00069	B0YS	ThinkSystem 2.5" 2.4TB 10K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00021	AULV	ThinkSystem 2.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00022	AULW	ThinkSystem 2.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00023	AULX	ThinkSystem 2.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	8
2.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00034	AUM6	ThinkSystem 2.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
7XB7A00035	AUM7	ThinkSystem 2.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	8
2.5-inch hot-swap SED HDDs - 12 Gb SAS 10K			
7XB7A00030	AUM4	ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD SED	8
7XB7A00031	AUM5	ThinkSystem 2.5" 600GB 10K SAS 12Gb Hot Swap 512n HDD SED	8

Table 20. 2.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00036	AUUE	ThinkSystem 2.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	8
7XB7A00037	AUUJ	ThinkSystem 2.5" 2TB 7.2K SATA 6Gb Hot Swap 512e HDD	8

Table 21. 2.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17062	B8HU	ThinkSystem 2.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17063	B8J4	ThinkSystem 2.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17064	B8JD	ThinkSystem 2.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A17065	B8JA	ThinkSystem 2.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13654	B4A1	ThinkSystem 2.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	8
4XB7A13655	B4A2	ThinkSystem 2.5" PM1645 3.2TB Mainstream SAS 12Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A38175	B91A	ThinkSystem 2.5" PM1643a 960GB Entry SAS 12Gb Hot Swap SSD	8
4XB7A38176	B91B	ThinkSystem 2.5" PM1643a 1.92TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17054	B91C	ThinkSystem 2.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17055	B91D	ThinkSystem 2.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A17056	BC4R	ThinkSystem 2.5" PM1643a 15.36TB Entry SAS 12Gb Hot Swap SSD	8
4XB7A13645	B4A7	ThinkSystem 2.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	8

Table 22. 2.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
2.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17087	B8J1	ThinkSystem 2.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17088	B8HY	ThinkSystem 2.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17089	B8J6	ThinkSystem 2.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17090	B8JE	ThinkSystem 2.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A17091	B8J7	ThinkSystem 2.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13633	B49L	ThinkSystem 2.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13634	B49M	ThinkSystem 2.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13635	B49N	ThinkSystem 2.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13636	B49P	ThinkSystem 2.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A13637	B49Q	ThinkSystem 2.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10237	B488	ThinkSystem 2.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10239	B48A	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10240	B48B	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	8
4XB7A10241	B48C	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	8
2.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			

Part number	Feature	Description	Maximum supported
4XB7A38271	BCTC	ThinkSystem 2.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38272	BCTD	ThinkSystem 2.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38273	BCTE	ThinkSystem 2.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38274	BCTF	ThinkSystem 2.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38275	BCTG	ThinkSystem 2.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17075	B8HV	ThinkSystem 2.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17076	B8JM	ThinkSystem 2.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17077	B8HP	ThinkSystem 2.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17078	B8J5	ThinkSystem 2.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17079	B8JP	ThinkSystem 2.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A17080	B8J2	ThinkSystem 2.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A38185	B9AC	ThinkSystem 2.5" 5210 960GB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38144	B7EW	ThinkSystem 2.5" 5210 1.92TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38145	B7EX	ThinkSystem 2.5" 5210 3.84TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A38146	B7EY	ThinkSystem 2.5" 5210 7.68TB Entry SATA 6Gb Hot Swap QLC SSD	8
4XB7A10247	B498	ThinkSystem 2.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10248	B499	ThinkSystem 2.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10249	B49A	ThinkSystem 2.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13622	B49B	ThinkSystem 2.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A13623	B49C	ThinkSystem 2.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10195	B34H	ThinkSystem 2.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10196	B34J	ThinkSystem 2.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10197	B34K	ThinkSystem 2.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10198	B34L	ThinkSystem 2.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10199	B34M	ThinkSystem 2.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10200	B4D2	ThinkSystem 2.5" PM883 7.68TB Entry SATA 6Gb Hot Swap SSD	8
7SD7A05740	B0Z0	ThinkSystem 2.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10155	B2X4	ThinkSystem 2.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	8
4XB7A10157	B2X6	ThinkSystem 2.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	8

Table 23. 3.5-inch hot-swap 12 Gb SAS HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 12 Gb SAS 10K			
7XB7A00063	B1JJ	ThinkSystem 3.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD	4
3.5-inch hot-swap HDDs - 12 Gb SAS 15K			
7XB7A00038	AUU2	ThinkSystem 3.5" 300GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00039	AUU3	ThinkSystem 3.5" 600GB 15K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00040	AUUC	ThinkSystem 3.5" 900GB 15K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap HDDs - 12 Gb NL SAS			
7XB7A00041	AUU4	ThinkSystem 3.5" 1TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00042	AUU5	ThinkSystem 3.5" 2TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00043	AUU6	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD	4
7XB7A00044	AUU7	ThinkSystem 3.5" 6TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00045	B0YR	ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00046	AUUG	ThinkSystem 3.5" 10TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
7XB7A00067	B117	ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13906	B496	ThinkSystem 3.5" 14TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A13911	B7EZ	ThinkSystem 3.5" 16TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
4XB7A38266	BCFP	ThinkSystem 3.5" 18TB 7.2K SAS 12Gb Hot Swap 512e HDD	4
3.5-inch hot-swap SED HDDs - 12 Gb NL SAS			
7XB7A00047	AUUH	ThinkSystem 3.5" 4TB 7.2K SAS 12Gb Hot Swap 512n HDD FIPS	4

Table 24. 3.5-inch hot-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap HDDs - 6 Gb NL SATA			
7XB7A00049	AUUF	ThinkSystem 3.5" 1TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00050	AUUD	ThinkSystem 3.5" 2TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00051	AUU8	ThinkSystem 3.5" 4TB 7.2K SATA 6Gb Hot Swap 512n HDD	4
7XB7A00052	AUUA	ThinkSystem 3.5" 6TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00053	AUU9	ThinkSystem 3.5" 8TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00054	AUUB	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
7XB7A00068	B118	ThinkSystem 3.5" 12TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13907	B497	ThinkSystem 3.5" 14TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A13914	B7F0	ThinkSystem 3.5" 16TB 7.2K SATA 6Gb Hot Swap 512e HDD	4
4XB7A38130	BCFH	ThinkSystem 3.5" 18TB 7.2K SATA 6Gb Hot Swap 512e HDD	4

Table 25. 3.5-inch hot-swap 12 Gb SAS SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 12 Gb SAS - Mainstream (3-5 DWPD)			
4XB7A17066	B8HT	ThinkSystem 3.5" PM1645a 800GB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17043	B8JN	ThinkSystem 3.5" PM1645a 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17067	B8JK	ThinkSystem 3.5" PM1645a 3.2TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A17068	B8JG	ThinkSystem 3.5" PM1645a 6.4TB Mainstream SAS 12Gb Hot Swap SSD	4
4XB7A13658	B4A4	ThinkSystem 3.5" PM1645 1.6TB Mainstream SAS 12Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 12 Gb SAS - Entry / Capacity (<3 DWPD)			
4XB7A17058	B91E	ThinkSystem 3.5" PM1643a 3.84TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A17059	BEVK	ThinkSystem 3.5" PM1643a 7.68TB Entry SAS 12Gb Hot Swap SSD	4
4XB7A13649	B4A8	ThinkSystem 3.5" PM1643 3.84TB Capacity SAS 12Gb Hot Swap SSD	4

Table 26. 3.5-inch hot-swap 6 Gb SATA SSDs

Part number	Feature	Description	Maximum supported
3.5-inch hot-swap SSDs - 6 Gb SATA - Mainstream (3-5 DWPD)			
4XB7A17096	B8JL	ThinkSystem 3.5" 5300 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17097	B8JF	ThinkSystem 3.5" 5300 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17098	B8J0	ThinkSystem 3.5" 5300 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17099	B8HR	ThinkSystem 3.5" 5300 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A17100	B8HX	ThinkSystem 3.5" 5300 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13639	B49R	ThinkSystem 3.5" Intel S4610 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13640	B49S	ThinkSystem 3.5" Intel S4610 480GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13641	B49T	ThinkSystem 3.5" Intel S4610 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13642	B49U	ThinkSystem 3.5" Intel S4610 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A13643	B49V	ThinkSystem 3.5" Intel S4610 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10242	B48D	ThinkSystem 3.5" 5200 240GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10244	B48F	ThinkSystem 3.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10245	B48G	ThinkSystem 3.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD	4
4XB7A10246	B48H	ThinkSystem 3.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD	4
3.5-inch hot-swap SSDs - 6 Gb SATA - Entry (<3 DWPD)			
4XB7A38276	BCTH	ThinkSystem 3.5" Multi Vendor 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38277	BCTJ	ThinkSystem 3.5" Multi Vendor 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38278	BCTK	ThinkSystem 3.5" Multi Vendor 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38279	BCTL	ThinkSystem 3.5" Multi Vendor 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A38281	BCTM	ThinkSystem 3.5" Multi Vendor 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17081	B8JB	ThinkSystem 3.5" 5300 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17082	B8J9	ThinkSystem 3.5" 5300 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17083	B8JC	ThinkSystem 3.5" 5300 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17084	B8HZ	ThinkSystem 3.5" 5300 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17085	B8HQ	ThinkSystem 3.5" 5300 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17086	B8J3	ThinkSystem 3.5" 5300 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Part number	Feature	Description	Maximum supported
4XB7A13625	B49D	ThinkSystem 3.5" Intel S4510 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13626	B49E	ThinkSystem 3.5" Intel S4510 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13627	B49F	ThinkSystem 3.5" Intel S4510 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13628	B49G	ThinkSystem 3.5" Intel S4510 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A13629	B49H	ThinkSystem 3.5" Intel S4510 3.84TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17176	B6TM	ThinkSystem 3.5" PM883 240GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17177	B6TN	ThinkSystem 3.5" PM883 480GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17178	B6TP	ThinkSystem 3.5" PM883 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17179	B6JY	ThinkSystem 3.5" PM883 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A17180	B6JZ	ThinkSystem 3.5" PM883 3.84TB Entry SATA 6Gb Hot Swap SSD	4
7SD7A05735	B0Z5	ThinkSystem 3.5" Intel S4500 960GB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10160	B2X9	ThinkSystem 3.5" 5200 1.92TB Entry SATA 6Gb Hot Swap SSD	4
4XB7A10162	B2XB	ThinkSystem 3.5" 5200 7.68TB Entry SATA 6Gb Hot Swap SSD	4

Table 27. 3.5-inch simple-swap 6 Gb SATA HDDs

Part number	Feature	Description	Maximum supported
3.5-inch simple-swap HDDs - 6 Gb NL SATA			
7XB7A00055	AUZS	ThinkSystem 1TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00056	AUZT	ThinkSystem 2TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00057	AUZU	ThinkSystem 4TB 7.2K 6Gbps SATA 3.5" Simple Swap 512n HDD	4
7XB7A00058	AXC7	ThinkSystem 6TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00059	AXC6	ThinkSystem 8TB 7.2K 6Gbps SATA 3.5" Simple Swap 512e HDD	4
7XB7A00060	AXC8	ThinkSystem 3.5" 10TB 7.2K SATA 6Gb Simple Swap 512e HDD	4

Table 29. M.2 SATA drives

Part number	Feature	Description	Maximum supported
M.2 SSDs - 6 Gb SATA - Entry (<3 DWPD)			
7N47A00129	AUUL	ThinkSystem M.2 32GB SATA 6Gbps Non-Hot Swap SSD	2
7N47A00130	AUUV	ThinkSystem M.2 128GB SATA 6Gbps Non-Hot Swap SSD	2
7SD7A05703	B11V	ThinkSystem M.2 5100 480GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17071	B8HS	ThinkSystem M.2 5300 240GB SATA 6Gbps Non-Hot Swap SSD	2
4XB7A17073	B919	ThinkSystem M.2 5300 480GB SATA 6Gbps Non-Hot Swap SSD	2

Optical drives

The server supports the external USB optical drive listed in the following table.

Table 30. External optical drive

Part number	Feature code	Description
7XA7A05926	AVV8	ThinkSystem External USB DVD RW Optical Disk Drive

The drive is based on the Lenovo Slim DVD Burner DB65 drive and supports the following formats: DVD-RAM, DVD-RW, DVD+RW, DVD+R, DVD-R, DVD-ROM, CD-RW, CD-R, CD-ROM.

I/O expansion

The SR530 server supports one LOM card slot and up to three PCIe slots with different riser cards installed into two riser sockets on the system planar (one riser socket supports installation of one riser card).

The slot form factors are as follows:

- LOM card slot
- Slot 1: PCIe 3.0 x8; low profile
- Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length
- Slot 3: PCIe 3.0 x8 or x16; low profile

Configuration notes:

- PCIe x16 slot 3 requires the second processor to be installed.
- The COM Port Upgrade Kit is installed in place of one of the PCIe slots 1, 2, or 3.

The locations of the PCIe slots are shown in the following figure.

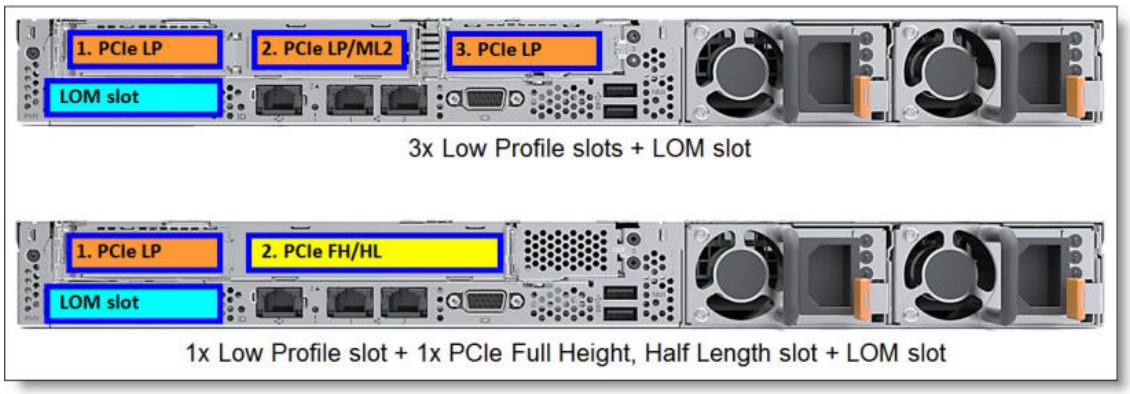


Figure 7. Slot locations

Riser 1 supplies slots 1 and 2, and Riser 2 supplies slot 3. The slots that are available for use depend on the number of riser cards that are installed and whether the second processor is installed, as shown in the following table.

Table 31. Slots available for use

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
None	None	LOM	-
None	PCIe x8	LOM, 3	-
None	PCIe x16	LOM	3
PCIe x8/x16 or PCIe x8/x8ML2	None	LOM, 1, 2	-
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x8	LOM, 1, 2, 3	-

Riser Card 1	Riser Card 2	Slots available for use	
		Processor 1	Processor 2
PCIe x8/x16 or PCIe x8/x8ML2	PCIe x16	LOM, 1, 2	3

The following table lists available PCIe riser card options.

Table 32. PCIe riser cards and miscellaneous options

Description	Part number	Feature code	Maximum quantity
x8 Riser Card 1 options (Riser card 1 supplies slots 1 and 2)			
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+LP Riser 1 Kit	7XH7A02682	AUWC	1
ThinkSystem SR530/SR570/SR630 x8/x16 PCIe LP+FH Riser 1 Kit	7XH7A05893	None*	1
ThinkSystem SR530/SR570 x8/x8ML2 PCIe LP+LP Riser 1 Kit	7XH7A05892	AV0X	1
Riser Card 2 option (Riser card 2 supplies slot 3)			
ThinkSystem SR530/SR570/SR630 x16 PCIe LP Riser 2 Kit	7XH7A02685	AUWA	1
ThinkSystem SR530/SR570 x8 PCIe LP Riser 2 Kit	7XH7A05891	AV0W	1
Serial port upgrade kit			
ThinkSystem COM Port Upgrade Kit	7Z17A02577	AUSL	1

* The LP+FH Riser 1 can be factory-installed by selecting the feature codes AUWC (LP+LP Riser 1) and AUWS (LP+FH Bracket).

The COM Port Upgrade Kit, part number 7Z17A02577, is used for mounting the external serial port on the rear of the SR530. This option includes the bracket and the cable. The COM Port option is mounted in place of one of the PCIe slots 1, 2, or 3.

Network adapters

The SR530 server has two onboard 1 GbE ports (no 10/100 Mb support) and up to two additional onboard 1/10 GbE network ports (no 10/100 Mb support) with optional LOM cards. Onboard ports and LOM cards use the Intel Ethernet Connection X722 1/10 GbE technology integrated into the Intel C622 Platform Controller Hub (PCH). The server also supports ML2 adapters that are installed in the custom ML2 slot provided by an ML2 riser card. The LOM cards support direct connectivity to the XClarity Controller via the Network Controller Sideband Interface (NSCI) for out-of-band systems management.

Note: ML2 network adapters do not support NSCI when used in the SR530 server.

The integrated Intel Ethernet Connection X722 has the following features:

- Two 1 Gb Ethernet ports (no 10/100 Mb Ethernet support)
- Two 1/10 Gb Ethernet capable ports (no 10/100 Mb Ethernet support)
- NIC Teaming (load balancing and failover)
- Data Center Bridging
- iWARP (RDMA over IP)
- VMDq and SR-IOV virtualization (10 Gb speeds only, 4 PFs, 128 VFs per device)
- IEEE 802.1q Virtual Local Area Networks (VLANs)
- NVGRE, VXLAN, IPinGRE, and MACinUDP network virtualization
- IEEE 802.1Qbg Edge Virtual Bridging
- TCP, IP, and UDP checksum offload
- Large Send Offload (LSO) and Generic Send Offload (GSO)
- Receive Side Scaling (RSS) for TCP and UDP traffic
- Jumbo frames up to 9.5 Kbytes

The following table lists the network adapters that are supported with the SR530 server.

Table 33. Network adapters

Description	Part number	Feature code	Max qty	I/O slots supported
LOM cards - 1 Gb Ethernet				
ThinkSystem 1Gb 2-port RJ45 LOM	7ZT7A00544	AUKG	1	LOM slot
LOM cards - 10 Gb Ethernet				
ThinkSystem 10Gb 2-port Base-T LOM	7ZT7A00548	AUKL	1	LOM slot
ThinkSystem 10Gb 2-port SFP+ LOM	7ZT7A00546	AUKJ	1*	LOM slot
ML2 adapters - 10 Gb Ethernet				
Broadcom NX-E ML2 10Gb 2-Port Base-T Ethernet Adapter	7ZT7A00497	AUKQ	1	2 (ML2)
Emulex VFA5.2 ML2 Dual Port 10GbE SFP+ Adapter	00AG560	AT7U	1*	2 (ML2)
Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	01CV770	AU7Z	1*	2 (ML2)
Intel X710-DA2 ML2 2x10GbE SFP+ Adapter	00JY940	ATRH	1*	2 (ML2)
PCIe Low Profile adapters - 1 Gb Ethernet				
Broadcom 5720 1GbE RJ45 2-Port PCIe Ethernet Adapter	7ZT7A00482	AUZX	3	1, 2, 3
Broadcom 5719 1GbE RJ45 4-Port PCIe Ethernet Adapter	7ZT7A00484	AUZV	3	1, 2, 3
ThinkSystem I350-F1 PCIe 1Gb 1-Port SFP Ethernet Adapter	7ZT7A00533	AUZZ	3	1, 2, 3
ThinkSystem I350-T2 PCIe 1Gb 2-Port RJ45 Ethernet Adapter	7ZT7A00534	AUZY	3	1, 2, 3
ThinkSystem I350-T4 PCIe 1Gb 4-Port RJ45 Ethernet Adapter	7ZT7A00535	AUZW	3	1, 2, 3
PCIe Low Profile adapters - 10 Gb Ethernet				
Broadcom 57416 10GBASE-T 2-Port PCIe Ethernet Adapter	7ZT7A00496	AUKP	3	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ PCIe Adapter	00AG570	AT7S	3*	1, 2, 3
Emulex VFA5.2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW	00AG580	AT7T	3*	1, 2, 3
Intel X550-T2 Dual Port 10GBase-T Adapter	00MM860	ATPX	3	1, 2, 3
Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter	7ZT7A00537	AUKX	3*	1, 2, 3
QLogic QL41134 PCIe 10Gb 4-Port Base-T Ethernet Adapter	4XC7A08225	B31G	3	1, 2, 3
PCIe Full Height adapters - 10 Gb Ethernet				
Emulex OCe14104B-NX PCIe 10Gb 4-Port SFP+ Ethernet Adapter	7ZT7A00493	AUKN	1*	2
PCIe Low Profile adapters - 25 Gb Ethernet				
Broadcom 57412 10/25GbE SFP28 1-Port PCIe Ethernet Adapter	7ZT7A00505	AUKS	3*	1, 2, 3
Broadcom 57414 10/25GbE SFP28 2-port PCIe Ethernet Adapter	4XC7A08238	B5T0	3*	1, 2, 3
PCIe Low Profile adapters - Omni-Path				
Intel OPA 100 Series Single-port PCIe 3.0 x16 HFA	00WE027	AU0B	1 / 2#*	2, 3

The maximum quantity shown is with one processor / two processors.
* The adapter comes without transceivers or cables; for ordering transceivers or cables, see the adapter product guide

Configuration notes:

- ML2 network adapters are supported in the ML2 x8 slot 2 supplied by the x8/x8ML2 Riser Card 1 (7XH7A05892).
- PCIe full-height network adapters are supported in the full-height PCIe x16 slot 2 supplied by the PCIe x8/x16 LP+FH Riser Card 1 (7XH7A05893).
- Omni-Path adapters are supported in the low profile or full-height PCIe x16 slots supplied by the riser cards 1 and 2.
- PCIe Low Profile network adapters (except Omni-Path adapters) are supported in the low profile and full-height PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

- Some adapters require supported transceivers or DAC cables to be purchased for the adapter. The maximum number of transceivers or cables that are supported per adapter equals the quantity of the adapter ports, and all adapter ports must have the same type of the transceiver or cable selected.

For more information, see the list of Product Guides in the Ethernet Adapters category:
http://lenovopress.com/servers/options/ethernet#rt=product-guide

SAS adapters for external storage

The following table lists SAS RAID controllers and HBAs for external storage attachments that are supported by the SR530 server.

Table 34. SAS RAID adapters and HBAs for external storage

Description	Part number	Feature code	Maximum quantity	I/O slots supported
12 Gbps SAS RAID adapters				
ThinkSystem RAID 930-8e 4GB Flash PCIe 12Gb Adapter	7Y37A01087	AUNQ	2	1, 2, 3
12 Gbps SAS HBAs				
ThinkSystem 430-8e SAS/SATA 12Gb HBA	7Y37A01090	AUNR	2	1, 2, 3
ThinkSystem 430-16e SAS/SATA 12Gb HBA	7Y37A01091	AUNN	2	1, 2, 3

Configuration notes:

- Low profile SAS RAID controllers and HBAs for external storage are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.
- The total quantity of the RAID 730-8i 2GB, RAID 930-8i, RAID 930-16i, and RAID 930-8e controllers in a supported combination in the server must not exceed 2 (up to 2 supercapacitors can be mounted in the server).

The following table summarizes features of supported RAID controllers and HBAs for external storage.

Table 35. Features and specifications of the RAID controllers and HBAs for external storage

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
Form factor	PCIe LP	PCIe LP	PCIe LP
SAS controller chip	SAS3516	SAS3408	SAS3416
Host interface	PCIe 3.0 x8	PCIe 3.0 x8	PCIe 3.0 x8
Port interface	12 Gb SAS	12 Gb SAS	12 Gb SAS
Number of ports	8	8	16
Connector type	SFF-8644 x4	SFF-8644 x4	SFF-8644 x4
Number of connectors	2	2	4
Drive interface	SAS, SATA	SAS, SATA	SAS, SATA
Drive type	HDD, SSD, SED	HDD, SSD, SED*	HDD, SSD, SED*
Hot-swap drive support	Yes	Yes	Yes
Number of devices	240	1024	1024
RAID levels	0/1/10/5/50/6/60	None	None
JBOD mode	Yes	Yes	Yes
Cache	4 GB	None	None
Cache protection	Flash backup (Included)	None	None
SED key management (SafeStore)	Yes	No	No
SSD I/O acceleration (FastPath)	Yes	No	No

Feature	RAID 930-8e	430-8e HBA	430-16e HBA
SSD Caching (CacheCade Pro 2.0)	No**	No	No
Consistency check	Yes	No	No
Patrol read	Yes	No	No
Online capacity expansion	Yes	No	No
Online RAID level migration	Yes	No	No
Global Hot Spare	Yes	No	No
Auto-rebuild	Yes	No	No

* HBAs do not support key management for SEDs; third-party host software is responsible for managing the keys.
** The SSD caching feature has been phased out in the new generation of advanced RAID controllers.

For more information, see the list of Product Guides in the following categories:

- RAID adapters
  http://lenovopress.com/servers/options/raid#rt=product-guide
- Host bus adapters
  http://lenovopress.com/servers/options/hba#rt=product-guide

Fibre Channel host bus adapters

The following table lists Fibre Channel HBAs supported by the SR530 server.

Table 36. Fibre Channel HBAs

Description	Part number	Feature code	Maximum quantity	I/O slots supported
16 Gb Fibre Channel - PCIe				
Emulex 16Gb Gen6 FC Single-port HBA	01CV830	ATZU	3	1, 2, 3
Emulex 16Gb Gen6 FC Dual-port HBA	01CV840	ATZV	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Single-port HBA	01CV750	ATZB	3	1, 2, 3
QLogic 16Gb Enhanced Gen5 FC Dual-port HBA	01CV760	ATZC	3	1, 2, 3
8 Gb Fibre Channel - PCIe (available only in PRC and Asia Pacific)				
Emulex LPe12002-M8-L PCIe 8Gb 2-Port SFP+ FC HBA	4XC7A08221	B0X0	3	1, 2, 3
Emulex LPe12000-M8-L PCIe 8Gb 1-Port SFP+ FC HBA	4XC7A08220	B0WZ	3	1, 2, 3

Configuration note: FC HBAs are supported in the low profile and full-high PCIe x8 and x16 slots supplied by the riser cards 1 and 2. The PCIe x16 slot 3 requires the second processor to be installed.

For more information, see the list of Product Guides in the Host bus adapters category:
http://lenovopress.com/servers/options/hba#rt=product-guide

Cooling

The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.

The following table shows additional cooling options.

Table 37. Cooling options

Description	Part number	Feature code	Maximum quantity
ThinkSystem SR530 FAN Option Kit	4F17A12354	AV0N	1

Configuration note: The SR530 FAN Option Kit (4F17A12354) includes two system fans that are required for field upgrades that add a second processor to the server. If two processors are selected in the initial server configurations, two fans for the second processor are derived by the configurator.

Power supplies and cables

The SR530 server supports up to two redundant power supplies and is capable of N+N redundancy depending on the configuration. A second power supply can be added to the models that come with one power supply. The following table lists the power supply options.

Table 38. Power supplies

Description	Part number	Feature code	Maximum quantity
ThinkSystem 550W (230V/115V) Platinum Hot-Swap Power Supply	7N67A00882	AVV6	2
ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply	7N67A00883	AVV7	2
ThinkSystem 750W (230V) Titanium Hot-Swap Power Supply	7N67A00884	AVV5	2

Configuration notes:

- Minimum of 1 and maximum of 2 power supplies per system.
- If 2 are installed, power supplies must be identical.
- Power supplies support AC (Worldwide) and HVDC (PRC only) power sources.

Important: The Standalone Solution Configuration Tool (SSCT) and Lenovo Data Center Solution Configurator (DCSC) power supply selection rules allow a subset of possible configurations due to power restrictions. Configurations that cannot be built in SSCT or DCSC due to power restrictions may still be supported. To verify support and ensure that the right power supply is chosen for optimal performance, you should always validate your server configuration using the latest version of the Lenovo Capacity Planner: http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

The SR530 server ship standard with or without a power cord (model dependent). A hot-swap power supply option ships without a power cord. The following table lists the rack power cables and line cords that can be ordered for the SR530 server.

Table 39. Power cables

Description	Part number	Feature code
Rack power cables		
1.0m, 10A/125-250V, C13 to IEC 320-C14 Rack Power Cable	00Y3043	A4VP
1.5m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7937	6201
2.0m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08369	6570
2.8m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08366	6311

Description	Part number	Feature code
2.8m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08370	6400
2.8m, 10A/100-250V, C13 to IEC 320-C20 Rack Power Cable	39Y7938	6204
4.3m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable	39Y7932	6263
4.3m, 13A/125V-10A/250V, C13 to IEC 320-C14 Rack Power Cable	4L67A08371	6583
Line cords		
Argentina 2.8m, 10A/250V, C13 to IRAM 2073 Line Cord	39Y7930	6222
Argentina 4.3m, 10A/250V, C13 to IRAM 2073 Line Cord	81Y2384	6492
Australia/New Zealand 2.8m, 10A/250V, C13 to AS/NZS 3112 Line Cord	39Y7924	6211
Australia/New Zealand 4.3m, 10A/250V, C13 to AS/NZS 3112 Line Cord	81Y2383	6574
Brazil 2.8m, 10A/250V, C13 to NBR 14136 Line Cord	69Y1988	6532
Brazil 4.3m, 10A/250V, C13 to NBR14136 Line Cord	81Y2387	6404
China 1.8m, 10A/250V, C13 to GB 2099.1 Line Cord	4L67A69954	6361
China 2.8m, 10A/250V, C13 to GB 2099.1 Line Cord	39Y7928	6210
China 4.3m, 10A/250V, C13 to GB 2099.1 Line Cord	81Y2378	6580
Denmark 2.8m, 10A/250V, C13 to DK2-5a Line Cord	39Y7918	6213
Denmark 4.3m, 10A/250V, C13 to DK2-5a Line Cord	81Y2382	6575
Europe 2.8m, 10A/250V, C13 to CEE7-VII Line Cord	39Y7917	6212
Europe 4.3m, 10A/250V, C13 to CEE7-VII Line Cord	81Y2376	6572
India 2.8m, 10A/250V, C13 to IS 6538 Line Cord	39Y7927	6269
India 4.3m, 10A/250V, C13 to IS 6538 Line Cord	81Y2386	6567
Israel 2.8m, 10A/250V, C13 to SI 32 Line Cord	39Y7920	6218
Israel 4.3m, 10A/250V, C13 to SI 32 Line Cord	81Y2381	6579
Italy 2.8m, 10A/250V, C13 to CEI 23-16 Line Cord	39Y7921	6217
Italy 4.3m, 10A/250V, C13 to CEI 23-16 Line Cord	81Y2380	6493
Japan 2.8m, 12A/125V, C13 to JIS C-8303 Line cord	46M2593	6314
Japan 2.8m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08357	5472
Japan 4.3m, 12A/125V, C13 to JIS C-8303 Line Cord	39Y7926	6335
Japan 4.3m, 12A/250V, C13 to JIS C-8303 Line Cord	4L67A08362	6495
Korea 2.8m, 12A/250V, C13 to KS C8305 Line Cord	39Y7925	6219
Korea 4.3m, 12A/250V, C13 to KS C8305 Line Cord	81Y2385	6494
South Africa 2.8m, 10A/250V, C13 to SABS 164 Line Cord	39Y7922	6214
South Africa 4.3m, 10A/250V, C13 to SABS 164 Line Cord	81Y2379	6576
Switzerland 2.8m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	39Y7919	6216
Switzerland 4.3m, 10A/250V, C13 to SEV 1011-S24507 Line Cord	81Y2390	6578
Taiwan 2.8m, 10A/125V, C13 to CNS 10917-3 Line Cord	23R7158	6386
Taiwan 2.8m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2375	6317
Taiwan 2.8m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2374	6402
Taiwan 4.3m, 10A/125V, C13 to CNS 10917-3 Line Cord	4L67A08363	AX8B
Taiwan 4.3m, 10A/250V, C13 to CNS 10917-3 Line Cord	81Y2389	6531
Taiwan 4.3m, 15A/125V, C13 to CNS 10917-3 Line Cord	81Y2388	6530
United Kingdom 2.8m, 10A/250V, C13 to BS 1363/A Line Cord	39Y7923	6215
United Kingdom 4.3m, 10A/250V, C13 to BS 1363/A Line Cord	81Y2377	6577
United States 2.8m, 10A/125V, C13 to NEMA 5-15P Line Cord	90Y3016	6313

Description	Part number	Feature code
United States 2.8m, 10A/250V, C13 to NEMA 6-15P Line Cord	46M2592	A1RF
United States 2.8m, 13A/125V, C13 to NEMA 5-15P Line Cord	00WH545	6401
United States 4.3m, 10A/125V, C13 to NEMA 5-15P Line Cord	4L67A08359	6370
United States 4.3m, 10A/250V, C13 to NEMA 6-15P Line Cord	4L67A08361	6373
United States 4.3m, 13A/125V, C13 to NEMA 5-15P Line Cord	4L67A08360	AX8A

Systems management

The SR530 supports the following systems management tools:

- Lenovo XClarity Controller
- Lenovo XClarity Provisioning Manager
- Lenovo XClarity Essentials
- Lenovo XClarity Administrator
- Lenovo XClarity Integrators
- Lenovo XClarity Energy Manager
- Lenovo Capacity Planner

Lenovo XClarity Controller

The SR530 server contains Lenovo XClarity Controller (XCC), which provides advanced service-processor control, monitoring, and alerting functions. XClarity Controller offers three functional levels: Standard, Advanced, and Enterprise.

By default, the SR530 server includes XClarity Controller Standard features, and it can be upgraded to Advanced or Enterprise functionality by using the Features on Demand (FoD) upgrades.

XClarity Controller Standard offers the following capabilities:

- Gathering and viewing system information and inventory
- Monitoring system status and health
- Alerting and notifications
- Event logging
- Configuring network connectivity
- Configuring security
- Updating system firmware
- Configuring server settings and devices
- Real-time power usage monitoring
- Remotely controlling server power (Power on, Power off, Restart)
- Managing FoD activation keys
- Redirecting serial console via IPMI
- Capturing the video display contents when an operating system hang condition is detected

XClarity Controller Advanced Upgrade adds the following functionality to the Standard features:

- Remotely viewing video with the following graphics resolutions:
  - Up to 1600x1200 with up to 23 bits per pixel; or
  - Up to 1920x1200 with up to 15 bits per pixel
- Remotely accessing the server using the keyboard and mouse from a remote client
- Remotely deploying an operating system
- Syslog alerting
- Redirecting serial console via SSH
- Displaying graphics for real-time and historical power usage data and temperature

XClarity Controller Enterprise Upgrade adds the following functionality to the Advanced features:

- Capping power usage
- Mapping the ISO and image files located on the local client as virtual drives for use by the server
- Mounting the remote ISO and image files via HTTPS, SFTP, CIFS, and NFS
- Collaborating across up to six users of the virtual console
- Controlling quality and bandwidth usage

The XClarity Controller provides remote server management through industry-standard interfaces:

- Intelligent Platform Management Interface (IPMI) Version 2.0
- Simple Network Management Protocol (SNMP) Version 3
- Common Information Model (CIM)
- Data Center Manageability Interface (DCMI) Version 1.5
- Redfish REpresentational State Transfer (REST) API
- Web browser with HTML5 support
- Command-line interface
- Virtual Operator Panel with XClarity Mobile App via the front USB port with XClarity Controller access

Virtual Operator Panel provides quick access to system status, firmware, network, health, and alerts information. With proper authentication, it also allows to configure systems management and network settings and to control system power (Power on, Power off, Restart). The Virtual Operator Panel can be accessed from the XClarity Mobile App running on the Android or iOS mobile device that is connected to the front USB port with XClarity Controller access (See Components and connectors).

Note: Depending on the system settings, the front USB port can be assigned to XClarity Controller for management functions, or to the system as a regular USB 2.0 port, or switched between two functions by using the system ID button.

IPMI via the Ethernet port (IPMI over LAN) is supported, however it is disabled by default. For CTO orders you can specify whether you want to the feature enabled or disabled in the factory, using the feature codes listed in the following table.

Table 40. IPMI-over-LAN settings

Part number	Feature code	Description
CTO only	B7XZ	Disable IPMI-over-LAN (default)
CTO only	B7Y0	Enable IPMI-over-LAN

The following table lists the XClarity Controller FoD upgrades.

Table 41. XClarity Controller FoD upgrades

Description	Part number	Feature code	Maximum quantity
ThinkSystem XClarity Controller Standard to Advanced Upgrade	4L47A09132	AVUT	1
ThinkSystem XClarity Controller Standard to Enterprise Upgrade	None*	AUPW	1
ThinkSystem XClarity Controller Advanced to Enterprise Upgrade	4L47A09133	None**	1

* Factory-installed only.
** Field upgrade only.

Configuration notes:

- For factory-installed upgrades, either Standard to Advanced Upgrade (feature AVUT) or Standard to Enterprise Upgrade (feature AUPW) can be selected, but not both.
- For field upgrades, the Advanced to Enterprise Upgrade (4L47A09133) requires the Standard to Advanced Upgrade to be activated on the server previously with either the factory-installed feature AVUT or field upgrade 4L47A09132.

Lenovo XClarity Provisioning Manager

Lenovo XClarity Provisioning Manager is a UEFI-embedded GUI application that combines the functions of configuring system setup settings, configuring RAID, and updating applications and firmware. It also enables you to install the supported operating systems and associated device drivers, run diagnostics, and collect service data.

Lenovo XClarity Provisioning Manager has the following features:

- Automatic hardware detection
- Collecting and viewing system inventory information
- Configuring UEFI system setup settings
- Updating the system firmware
- Configuring RAID by using the RAID Setup Wizard or Advanced mode
- Installing an operating system and device drivers automatically or manually
- Running diagnostics and collecting service data

Lenovo XClarity Essentials

Lenovo offers the following XClarity Essentials software tools that can help you set up, use, and maintain the server at no additional cost:

- Lenovo XClarity Essentials OneCLI
  OneCLI is a collection of server management tools that utilize a command line interface program to manage firmware, hardware, and operating systems. It provides functions to collect full system health information (including health status), configure system setting, and update system firmware and drivers.
- Lenovo XClarity Essentials UpdateXpress
  The UpdateXpress tool is a standalone GUI application for firmware and device driver updates that enables you to maintain your server firmware and device drivers up-to-date and help you avoid unnecessary server outages. The tool acquires and deploys individual updates and UpdateXpress System Packs (UXSPs) which are integration-tested bundles.
- Lenovo XClarity Essentials Bootable Media Creator
  The Bootable Media Creator (BOMC) tool is used to create bootable media for offline firmware update.

For more information and downloads, visit the Lenovo XClarity Essentials web page:
http://support.lenovo.com/us/en/documents/LNVO-center

Lenovo XClarity Administrator

Lenovo XClarity is a centralized systems management solution that helps administrators deliver infrastructure faster. This solution integrates easily with Lenovo x86 servers, RackSwitch switches, and DS Series storage, providing automated agent-less discovery, monitoring, firmware updates, configuration management, and bare metal deployment of operating systems and hypervisors across multiple servers.

Lenovo XClarity Administrator is an optional software component for the SR530 server which can be downloaded and used at no charge to discover and monitor the SR530 and manage firmware upgrades for them.

If software support is required for Lenovo XClarity Administrator, or Lenovo XClarity Administrator premium features (such as configuration management and operating system deployment) are required, or both, Lenovo XClarity Pro software subscription should be ordered. Lenovo XClarity Pro is licensed on a per managed system basis, that is, each managed Lenovo system requires a license.

The following table lists the geo-specific Lenovo XClarity software license options.

Table 42. Lenovo XClarity software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Pro, per Managed Endpoint w/1 Yr SW S&S	00MT201	00MT207	1
Lenovo XClarity Pro, per Managed Endpoint w/3 Yr SW S&S	00MT202	00MT208	1
Lenovo XClarity Pro, per Managed Endpoint w/5 Yr SW S&S	00MT203	00MT209	1

* NA = North America; AP = Asia Pacific
** EMEA = Europe, Middle East, Africa; LA = Latin America

Lenovo XClarity Administrator offers the following standard features that are available at no charge:

- Auto-discovery and monitoring of Lenovo x86 servers, RackSwitch switches, Flex System chassis, and DS Series storage systems
- Firmware updates and compliance enforcement
- External alerts and notifications via SNMP traps, syslog remote logging, and e-mail
- Secure connections to managed endpoints
- NIST 800-131A or FIPS 140-2 compliant cryptographic standards between the management solution and managed endpoints
- Integration into existing higher level management systems such as cloud automation and orchestration tools through REST APIs, providing extensive external visibility and control over hardware resources
- An intuitive, easy-to-use GUI
- Scripting with Windows PowerShell, providing command-line visibility and control over hardware resources

Lenovo XClarity Administrator offers the following premium features that require an optional Pro license:

- Pattern-based configuration management that allows to define configurations once and apply repeatedly without errors when deploying new servers or redeploying existing servers without disrupting the fabric
- Bare-metal deployment of operating systems and hypervisors to streamline infrastructure provisioning

For more information, refer to the Lenovo XClarity Administrator Product Guide:
http://lenovopress.com/tips1200

Lenovo XClarity Integrators

Lenovo offers at no charge (if software support is required, a Lenovo XClarity Pro software subscription license should be ordered) two software plug-in modules, Lenovo XClarity Integrators, to manage physical infrastructure from leading external virtualization management software tools from Microsoft and VMware:

- Lenovo XClarity Integrator for Microsoft System Center
- Lenovo XClarity Integrator for VMware vCenter

Lenovo XClarity Integrators offer the following additional features:

- Ability to discover, manage, and monitor Lenovo server hardware from VMware vCenter or Microsoft System Center
- Deployment of firmware updates and configuration patterns to Lenovo x86 rack servers and Flex System from the virtualization management tool
- Non-disruptive server maintenance in clustered environments that reduces workload downtime by dynamically migrating workloads from affected hosts during rolling server updates or reboots
- Greater service level uptime and assurance in clustered environments during unplanned hardware events by dynamically triggering workload migration from impacted hosts when impending hardware failures are predicted

For more information, refer to the Lenovo XClarity Integrators web page:
http://www3.lenovo.com/us/en/data-center/software/systems-management/xclarity-integrators

Lenovo XClarity Energy Manager

Lenovo XClarity Energy Manager provides a stand-alone, web-based agent-less power management console that provides real time data and enables you to observe, plan and manage power and cooling for Lenovo servers. Using built-in intelligence, it identifies server power consumption trends and ideal power settings and performs cooling analysis so that you can define and optimize power-saving policies.

Lenovo XClarity Energy Manager offers the following capabilities:

- Monitors room, row, rack, and device levels in the data center
- Reports vital server information, such as power, temperature and resource utilization
- Monitors inlet temperature to locate hot spots, reducing the risk of data or device damage
- Provides finely-grained controls to limit platform power in compliance with IT policy
- Generates alerts when a user-defined threshold is reached

Lenovo XClarity Energy Manager is an optional software component for the SR530 server that is licensed on a per managed node basis, that is, each managed server requires a license. The 1-node Energy Manager license is included in the XClarity Controller Enterprise upgrade.

To manage systems without XClarity Controller Enterprise licenses, a node license pack should be purchased. The following table lists the geo-specific Lenovo XClarity Energy Manager software license options.

Table 43. Lenovo XClarity Energy Manager software options

Description	Part number (NA, AP, Japan)*	Part number (EMEA, LA)**	Quantity
Lenovo XClarity Energy Manager, 1 Node w/ 1 Yr S&S	01DA225	01DA228	1

* NA = North America; AP = Asia Pacific.
** EMEA = Europe, Middle East, Africa; LA = Latin America.

For more information, refer to the Lenovo XClarity Energy Manager web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lxem

Lenovo Capacity Planner

Lenovo Capacity Planner is a power consumption evaluation tool that enhances data center planning by enabling IT administrators and pre-sales professionals to understand various power characteristics of racks, servers, and other devices. Capacity Planner can dynamically calculate the power consumption, current, British Thermal Unit (BTU), and volt-ampere (VA) rating at the rack level, improving the planning efficiency for large-scale deployments.

For more information, refer to the Capacity Planner web page:
http://datacentersupport.lenovo.com/us/en/solutions/lnvo-lcp

Security

The SR530 server offers the following security features:

- Power-on password
- Administrator's password
- Secure firmware updates
- Onboard Trusted Platform Module (TPM) version 1.2 or 2.0 (configurable UEFI system setting)
- Trusted Cryptographic Module (TCM) (optional; available in PRC only)
- Nationz Trusted Platform Module v2.0 (optional; available in PRC only)
- Lockable front bezel (optional)
- Security Key Lifecycle Manager (SKLM) encryption key management for SEDs - FoD upgrade (optional)
- Lenovo Business Vantage security software (optional; available in PRC only)

The server is NIST SP 800-147B compliant.

The following table lists the security options that are available for the SR530 server.

Table 44. Security options

Description	Part number	Feature code	Maximum quantity
Lockable front bezel			
ThinkSystem 1U Security Bezel	7Z17A02581	AUWR	1
Trusted Cryptographic Module (PRC only)			
ThinkSystem Trusted Cryptographic Module	None*	AVKE	1
Trusted Platform Module (PRC only)			
ThinkSystem Nationz Trusted Platform Module v2.0	None*	B22N	1
Security Key Lifecycle Manager - FoD (United States, Canada, Asia Pacific, and Japan)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00D9998	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00D9999	AS6C	1
Security Key Lifecycle Manager - FoD (Latin America, Europe, Middle East, and Africa)			
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S	00FP648	A5U1	1
SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S	00FP649	AS6C	1

* Factory-installed only; no field upgrade.

Lenovo Business Vantage is a security software tool suite (available only in PRC) designed to work with the TCM or Nationz TPM for enhanced security, to keep user data safe, and to erase confidential data completely from a drive.

Lenovo Business Vantage provides the following features:

- Encrypts files to ensure data safety by using the TCM or Nationz TPM.
- Erases confidential data from a hard disk.
- Prohibits unauthorized access to the USB port of devices.
- Encrypts files to ensure data security on a USB storage device.

For more information, refer to the Lenovo Business Vantage web page:
http://support.lenovo.com.cn/lenovo/wsi/es/es.html

Rack installation

The following table lists the rack installation options that are available for the SR530 server.

Table 45. Rack installation options

Description	Part number	Feature code	Maximum quantity
4-post rail kits			
ThinkSystem Tool-less Slide Rail	7M27A05702	AXCA	1
ThinkSystem Tool-less Slide Rail Kit with 1U CMA	7M27A05701	AXCB	1
ThinkSystem Screw-in Slide Rail	4M17A07274	AXFN	1
ThinkSystem Screw-in Slide Rail Kit with 1U CMA	4M17A07281	B0TE	1
ThinkSystem Tool-less Friction Rail	4M17A07273	AXFM	1
Cable management arm (CMA) upgrade			
ThinkSystem 1U CMA Upgrade Kit for Tool-less Slide Rail	7M27A05699	None^	1*
ThinkSystem 1U CMA Upgrade Kit for Screw-in Slide Rail	4M17A07276	AXFP	1**
Front VGA port			
ThinkSystem SR530/SR630 Front VGA Connector (for 3.5" models)	None***	AUWU	1
ThinkSystem SR530/SR570/SR630 Front VGA Connector Upgrade Kit (for 2.5" models)	7Z17A02579	AUWW	1

^ Field upgrade only.
* The CMA Upgrade Kit for Tool-less Slide Rail is supported with the Tool-less Slide Rail (7M27A05702) only.
** The CMA Upgrade Kit for Screw-in Slide Rail is supported with the Screw-in Slide Rail (4M17A07274) only.
*** Factory-installed only; no field upgrade.

The following table summarizes the rail kit features and specifications.

Table 46. Rail kit features and specifications summary

Feature	Tool-less Slide Rail		Screw-in Slide Rail		Tool-less Friction Rail
	Without CMA	With CMA	Without CMA	With CMA	
Part number	7M27A05702	7M27A05701	4M17A07274	4M17A07281	4M17A07273
CMA	7M27A05699	Included	4M17A07276	Included	No support
Rail length	730 mm (28.74 in.)	807 mm (31.8 in.)	836.8 mm (32.9 in.)	836.8 mm (32.9 in.)	728.1 mm (28.7 in.)
Rail type	Full-out slide (ball bearing)		Full-out slide (ball bearing)		Half-out slide (friction)
Tool-less installation	Yes		No		Yes
In-rack server maintenance	Yes		Yes		No
1U PDU support	Yes		Yes		Yes
0U PDU support	Limited*		Limited*		Limited**
Rack type	IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant		IBM and Lenovo 4-post, IEC standard-compliant
Mounting holes	Square or round		Square, round, or threaded		Square or round
Mounting flange thickness	2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)		2 mm (0.08 in.) – 3.3 mm (0.13 in.)
Distance between front and rear mounting flanges^	609.6 mm (24 in.) – 863.6 mm (34 in.)		609.6 mm (24 in.) – 812.8 mm (32 in.)		609.6 mm (24 in.) – 863.6 mm (34 in.)

* If a 0U PDU is used, the rack cabinet must be at least 1100 mm (43.31 in.) deep if no CMA is used, or at least 1200 mm (47.24 in.) deep if a CMA is used.
** If a 0U PDU used, the rack must be at least 1000 mm (39.37 in.) deep.
^ Measured when mounted on the rack, from the front surface of the front mounting flange to the rear most point of the rail.

Operating systems

The server supports the following operating systems:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 8.1
- Red Hat Enterprise Linux 8.2
- Red Hat Enterprise Linux 8.3
- SUSE Linux Enterprise Server 12 SP4
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 12 Xen SP4
- SUSE Linux Enterprise Server 12 Xen SP5
- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Server 15 SP1
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 15 Xen
- SUSE Linux Enterprise Server 15 Xen SP1
- SUSE Linux Enterprise Server 15 Xen SP2
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2

For a complete list of supported, certified and tested operating systems, plus additional details and links to relevant web sites, see the Operating System Interoperability Guide: https://lenovopress.com/osig#servers=sr530-7x07-7x08-sp-gen-2

For configure-to-order configurations, the server can be preloaded with VMware ESXi installed on M.2 cards. Ordering information is listed in the following table.

Table 47. VMware ESXi preload

Part number	Feature code	Description
CTO only	B3VW	VMware ESXi 6.5 U2 (Factory Installed)
CTO only	B6U0	VMware ESXi 6.5 U3 (factory installed)
CTO only	B3VX	VMware ESXi 6.7 (Factory Installed)
CTO only	B4XA	VMware ESXi 6.7 U1 (Factory Installed)
CTO only	B6U1	VMware ESXi 6.7 U2 (factory installed)
CTO only	B88T	VMware ESXi 6.7 U3 (factory installed)
CTO only	BBZG	VMware ESXi 7.0 (Factory Installed)
CTO only	BE5E	VMware ESXi 7.0 U1 (Factory Installed)

Physical specifications

The SR530 has the following overall physical dimensions, excluding components that extend outside the standard chassis, such as EIA flanges, front security bezel (if any), and power supply handles:

- Width: 435 mm (17.1 inches)
- Height: 43 mm (1.7 inches)

- Depth: 750 mm (29.5 inches)

The following table lists the detailed dimensions. See the figure below for the definition of each dimension.

Table 48. Detailed dimensions

Dimension	Description
482 mm	X_a = Width, to the outsides of the front EIA flanges
435 mm	X_b = Width, to the rack rail mating surfaces
435 mm	X_c = Width, to the outer most chassis body feature
43 mm	Y_a = Height, from the bottom of chassis to the top of the chassis
715 mm	Z_a = Depth, from the rack flange mating surface to the rearmost I/O port surface
716 mm	Z_b = Depth, from the rack flange mating surface to the rearmost feature of the chassis body
744 mm	Z_c = Depth, from the rack flange mating surface to the rearmost feature such as power supply handle
35 mm	Z_d = Depth, from the forwardmost feature on front of EIA flange to the rack flange mating surface
47 mm	Z_e = Depth, from the front of security bezel (if applicable) or forwardmost feature to the rack flange mating surface

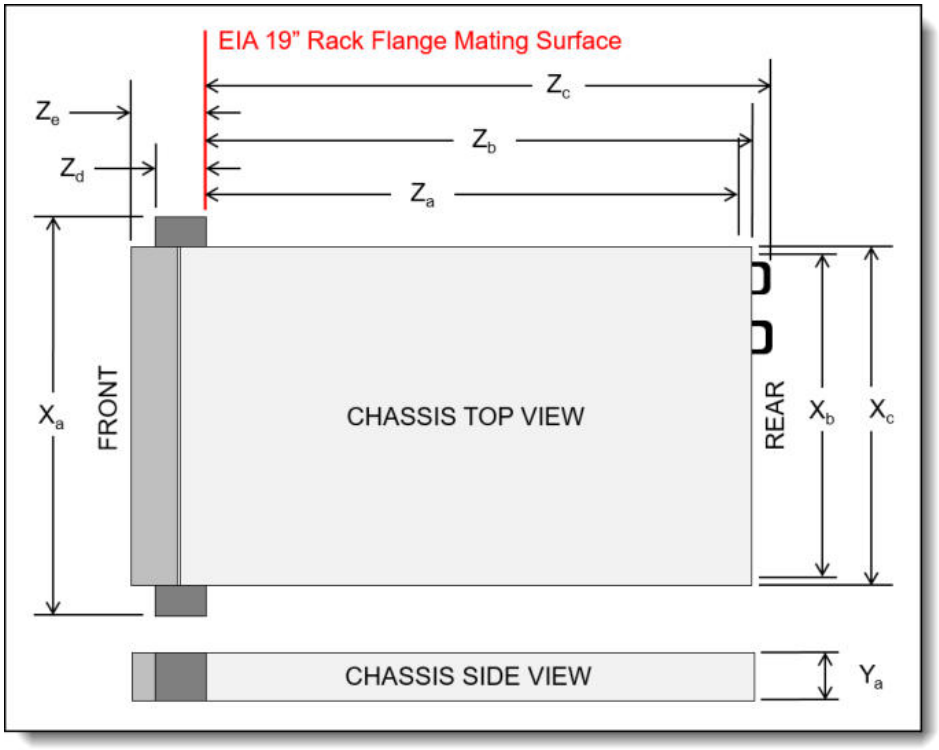


Figure 8. Server dimensions

The shipping dimensions (cardboard packaging) of the SR530 are as follows:

- Width: 587 mm (23.1 inches)
- Height: 225 mm (8.9 inches)
- Depth: 998 mm (39.3 inches)

The SR530 server has the following weight:

- Minimum configuration: 10.2 kg (22.5 lb)
- Maximum configuration: 16.0 kg (35.3 lb)

Operating environment

The SR530 server complies with ASHRAE class A2 specifications. The server performance might be impacted when the operating temperature is outside the ASHRAE A2 specifications. Depending on the hardware configuration, some server models comply with ASHRAE class A3 and class A4 specifications. To comply with ASHRAE class A3 and class A4 specifications, the server models must meet the following hardware configuration requirements at the same time:

- Two power supplies must be installed
- No system fan failure

The SR530 server is supported in the following environment:

- Air temperature:
  - Operating:
    - ASHRAE Class A4: 5 °C - 45 °C (41 °F - 113 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 125-m (410-ft) increase in altitude
    - ASHRAE Class A3: 5 °C - 40 °C (41 °F - 104 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 175-m (574-ft) increase in altitude
    - ASHRAE Class A2: 10 °C - 35 °C (50 °F - 95 °F); for altitudes above 900 m (2,953 ft), decrease the maximum ambient temperature by 1 °C for every 300-m (984-ft) increase in altitude
  - Non-operating: 5 °C - 45 °C (41 °F - 113 °F)
  - Storage: -40 °C - +60 °C (-40 °F - 140 °F)
- Maximum altitude: 3,050 m (10,000 ft)
- Humidity:
  - Operating:
    - ASHRAE Class A4: 8% - 90% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A3: 8% - 85% (non-condensing); maximum dew point: 24 °C (75 °F)
    - ASHRAE Class A2: 8% - 80% (non-condensing); maximum dew point: 21 °C (70 °F)
  - Storage: 8% - 90% (non-condensing)
- Electrical:
  - 100 - 127 (nominal) V AC; 50 Hz / 60 Hz
  - 200 - 240 (nominal) V AC; 50 Hz / 60 Hz
  - 180 - 300 V DC (HVDC; supported in PRC only)
- Acoustics:
  - Minimum configuration:
    - Operating: 5.0 bels
    - Idle: 4.5 bels
  - Maximum configuration:
    - Operating: 5.5 bels
    - Idle: 5.2 bels
- Vibration:
  - Operating: 0.21 G rms at 5 Hz to 500 Hz for 15 minutes across 3 axes
  - Non-operating: 1.04 G rms at 2 Hz to 200 Hz for 15 minutes across 6 surfaces
- Shock:
  - Operating: 15 G for 3 milliseconds in each direction (positive and negative X, Y, and Z axes)
  - Non-operating:
    - 12 kg - 22 kg: 50 G for 152 in./sec velocity change across 6 surfaces
    - 23 kg - 31 kg: 35 G for 152 in./sec velocity change across 6 surfaces

The following table lists the maximum system power load, rated inlet current, and system heat output based on the power supply and source voltage.

Table 49. Rated system power, inlet current, and system heat output

Power supply	Source voltage	Maximum power load per system (two power supplies)	Rated current per inlet	System heat output
550 W Platinum	100 - 127 V AC	722 W	6.2 A	2463 BTU/hour
	200 - 240 V AC	704 W	3 A	2402 BTU/hour
	180 - 300 V DC	702 W	2.5 A	2395 BTU/hour
750 W Platinum	100 - 127 V AC	984 W	8.4 A	3357 BTU/hour
	200 - 240 V AC	958 W	4.1 A	3269 BTU/hour
	180 - 300 V DC	958 W	3.5 A	3269 BTU/hour
750 W Titanium	200 - 240 V AC	949 W	4.1 A	3238 BTU/hour
	180 - 300 V DC	948 W	3.5 A	3235 BTU/hour

Warranty and support

The SR530 server has a one-year (7X07) or three-year (Machine Type 7X08) warranty.

The standard warranty terms are customer-replaceable unit (CRU) and onsite (for field-replaceable units FRUs only) with standard call center support during normal business hours and 9x5 Next Business Day Parts Delivered.

Lenovo's additional support services provide a sophisticated, unified support structure for your data center, with an experience consistently ranked number one in customer satisfaction worldwide. Available offerings include:

- **Premier Support**

  Premier Support provides a Lenovo-owned customer experience and delivers direct access to technicians skilled in hardware, software, and advanced troubleshooting, in addition to the following:

  - Direct technician-to-technician access through a dedicated phone line
  - 24x7x365 remote support
  - Single point of contact service
  - End to end case management
  - Third-party collaborative software support
  - Online case tools and live chat support
  - On-demand remote system analysis
- **Warranty Upgrade (Preconfigured Support)**

  Services are available to meet the on-site response time targets that match the criticality of your systems.

  - 3, 4, or 5 years of service coverage
  - 1-year or 2-year post-warranty extensions
  - **Foundation Service**: 9x5 service coverage with next business day onsite response. YourDrive YourData is an optional extra (see below).
  - **Essential Service:** 24x7 service coverage with 4-hour onsite response or 24-hour committed repair (available only in select countries). Bundled with YourDrive YourData.
  - **Advanced Service:** 24x7 service coverage with 2-hour onsite response or 6-hour committed repair (available only in select countries). Bundled with YourDrive YourData.

- **Managed Services**

  Lenovo Managed Services provides continuous 24x7 remote monitoring (plus 24x7 call center availability) and proactive management of your data center using state-of-the-art tools, systems, and practices by a team of highly skilled and experienced Lenovo services professionals.

  Quarterly reviews check error logs, verify firmware & OS device driver levels, and software as needed. We'll also maintain records of latest patches, critical updates, and firmware levels, to ensure you systems are providing business value through optimized performance.

- **Technical Account Management (TAM)**

  A Lenovo Technical Account Manager helps you optimize the operation of your data center based on a deep understanding of your business. You gain direct access to your Lenovo TAM, who serves as your single point of contact to expedite service requests, provide status updates, and furnish reports to track incidents over time. In addition, your TAM will help proactively make service recommendations and manage your service relationship with Lenovo to make certain your needs are met.

- **Enterprise Server Software Support**

  Enterprise Software Support is an additional support service providing customers with software support on Microsoft, Red Hat, SUSE, and VMware applications and systems. Around the clock availability for critical problems plus unlimited calls and incidents helps customers address challenges fast, without incremental costs. Support staff can answer troubleshooting and diagnostic questions, address product comparability and interoperability issues, isolate causes of problems, report defects to software vendors, and more.

- **YourDrive YourData**

  Lenovo's YourDrive YourData is a multi-drive retention offering that ensures your data is always under your control, regardless of the number of drives that are installed in your Lenovo server. In the unlikely event of a drive failure, you retain possession of your drive while Lenovo replaces the failed drive part. Your data stays safely on your premises, in your hands. The YourDrive YourData service can be purchased in convenient bundles and is optional with Foundation Service. It is bundled with Essential Service and Advanced Service.

- **Health Check**

  Having a trusted partner who can perform regular and detailed health checks is central to maintaining efficiency and ensuring that your systems and business are always running at their best. Health Check supports Lenovo-branded server, storage, and networking devices, as well as select Lenovo-supported products from other vendors that are sold by Lenovo or a Lenovo-Authorized Reseller.

Examples of region-specific warranty terms are second or longer business day parts delivery or parts-only base warranty.

If warranty terms and conditions include onsite labor for repair or replacement of parts, Lenovo will dispatch a service technician to the customer site to perform the replacement. Onsite labor under base warranty is limited to labor for replacement of parts that have been determined to be field-replaceable units (FRUs). Parts that are determined to be customer-replaceable units (CRUs) do not include onsite labor under base warranty.

If warranty terms include parts-only base warranty, Lenovo is responsible for delivering only replacement parts that are under base warranty (including FRUs) that will be sent to a requested location for self-service. Parts-only service does not include a service technician being dispatched onsite. Parts must be changed at customer's own cost and labor and defective parts must be returned following the instructions supplied with the spare parts.

Lenovo Service offerings are region-specific. Not all preconfigured support and upgrade options are available in every region. For information about Lenovo service upgrade offerings that are available in your region, refer to the following resources:

- Service part numbers in Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com/#/services
- Lenovo Services Availability Locator
  http://lenovolocator.com/

For service definitions, region-specific details, and service limitations, please refer to the following documents:

- Lenovo Statement of Limited Warranty for Data Center Group (DCG) Servers and System Storage
  http://pcsupport.lenovo.com/us/en/solutions/ht503310
- Lenovo Data Center Services Agreement
  http://support.lenovo.com/us/en/solutions/ht116628

Services

Lenovo Services is a dedicated partner to your success. Our goal is to reduce your capital outlays, mitigate your IT risks, and accelerate your time to productivity.

Note: Some service options may not be available in all countries. For more information, go to https://www.lenovo.com/systems/services. For information about Lenovo service upgrade offerings that are available in your region, contact your local Lenovo sales representative or business partner.

Here's a more in-depth look at what we can do for you:

- **Asset Recovery Services**

  Asset Recovery Services (ARS) helps customers recover the maximum value from their end-of-life equipment in a cost-effective and secure way. On top of simplifying the transition from old to new equipment, ARS mitigates environmental and data security risks associated with data center equipment disposal. Lenovo ARS is a cash-back solution for equipment based on its remaining market value, yielding maximum value from aging assets and lowering total cost of ownership for your customers. For more information, see the ARS page, https://lenovopress.com/lp1266-reduce-e-waste-and-grow-your-bottom-line-with-lenovo-ars.

- **Assessment Services**

  An Assessment helps solve your IT challenges through an onsite, multi-day session with a Lenovo technology expert. We perform a tools-based assessment which provides a comprehensive and thorough review of a company's environment and technology systems. In addition to the technology based functional requirements, the consultant also discusses and records the non-functional business requirements, challenges, and constraints. Assessments help organizations like yours, no matter how large or small, get a better return on your IT investment and overcome challenges in the ever-changing technology landscape.

- **Design Services**

  Professional Services consultants perform infrastructure design and implementation planning to support your strategy. The high-level architectures provided by the assessment service are turned into low level designs and wiring diagrams, which are reviewed and approved prior to implementation. The implementation plan will demonstrate an outcome-based proposal to provide business capabilities through infrastructure with a risk-mitigated project plan.

- **Basic Hardware Installation**

  Lenovo experts can seamlessly manage the physical installation of your server, storage, or networking hardware. Working at a time convenient for you (business hours or off shift), the technician will unpack and inspect the systems on your site, install options, mount in a rack cabinet, connect to power and network, check and update firmware to the latest levels, verify operation, and dispose of the packaging, allowing your team to focus on other priorities.

- **Deployment Services**

  When investing in new IT infrastructures, you need to ensure your business will see quick time to value with little to no disruption. Lenovo deployments are designed by development and engineering teams who know our Products & Solutions better than anyone else, and our technicians own the process from delivery to completion. Lenovo will conduct remote preparation and planning, configure & integrate systems, validate systems, verify and update appliance firmware, train on administrative tasks, and provide post-deployment documentation. Customer's IT teams leverage our skills to enable IT staff to transform with higher level roles and tasks.

- **Integration, Migration, and Expansion Services**

  Move existing physical & virtual workloads easily, or determine technical requirements to support increased workloads while maximizing performance. Includes tuning, validation, and documenting ongoing run processes. Leverage migration assessment planning documents to perform necessary migrations.

Regulatory compliance

The ThinkSystem SR530 server conforms to the following regulations:

- United States: FCC Part 15, Class A; UL 60950-1
- Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1
- Mexico: NOM-19
- Argentina: IEC60950-1
- European Union: CE Mark (EN55022 Class A, IEC/EN60950-1, EN55024, EN61000-3-2, EN61000-3-3)
- Germany: TUV-GS (IEC/EN 60950-1, EK1-ITB2000)
- Russia, Kazakhstan, Belarus: EAC (TR CU 004/2011, TR CU 020/2011)
- China: CCC GB4943.1, GB9254 Class A, GB17625.1
- India: BIS
- Japan: VCCI, Class A
- Taiwan: BSMI CNS13438, Class A; CNS14336-1
- Korea: KN22, Class A; KN24
- Australia/New Zealand: AS/NZS CISPR 22 Class A
- Reduction of Hazardous Substances (ROHS)
- Energy Star 3.0 (excluding configurations with Bronze 3204, Gold 5222, or Platinum 8256 processors)

Note: For more information on the Energy Star 3.0 certification, refer to the *Energy Star 3.0 Certifications for ThinkSystem Servers* publication:
http://lenovopress.com/lp1230

External drive enclosures

The server supports attachment to external drive enclosures using a RAID controller with external ports or a SAS host bus adapter. Adapters supported by the server are listed in the SAS adapters for external storage section.

Note: Information provided in this section is for ordering reference purposes only. For the operating system and adapter support details, refer to the interoperability matrix for a particular storage enclosure that can be found on the Lenovo Data Center Support web site:
http://datacentersupport.lenovo.com

Table 50. External drive enclosures

Description	Part number		
	Worldwide	Japan	PRC
Lenovo Storage D1212 LFF Disk Expansion with Dual SAS IO Modules	4587A11	4587A1J	4587A1C
Lenovo Storage D1224 SFF Disk Expansion with Dual SAS IO Modules	4587A31	4587A3J	4587A3C
Lenovo Storage D3284 4TB x 84 HD Expansion Enclosure	641311F		
Lenovo Storage D3284 6TB x 84 HD Expansion Enclosure	641312F		
Lenovo Storage D3284 8TB x 84 HD Expansion Enclosure	641313F		
Lenovo Storage D3284 10TB x 84 HD Expansion Enclosure	641314F		

For details about supported drives, adapters, and cables, see the following Lenovo Press Product Guides:

- Lenovo Storage D1212 and D1224
  http://lenovopress.com/lp0512
- Lenovo Storage D3284
  http://lenovopress.com/lp0513

External storage systems

Lenovo offers the ThinkSystem DE Series and ThinkSystem DM Series external storage systems for high-performance storage. See the DE Series and DM Series product guides for specific controller models, expansion enclosures and configuration options:

- ThinkSystem DE Series Storage
  https://lenovopress.com/storage/thinksystem/de-series#rt=product-guide
- ThinkSystem DM Series Storage
  https://lenovopress.com/storage/thinksystem/dm-series#rt=product-guide

External backup units

The following table lists the external backup options that are offered by Lenovo.

Table 51. External backup options

Part number	Description
External RDX USB drives	
4T27A10725	ThinkSystem RDX External USB 3.0 Dock
External SAS tape backup drives	
6160S6E	IBM TS2260 Tape Drive Model H6S
6160S7E	IBM TS2270 Tape Drive Model H7S
6160S8E	IBM TS2280 Tape Drive Model H8S
External SAS tape backup autoloaders	
6171S5R	IBM TS2900 Tape Autoloader w/LTO5 HH SAS
6171S6R	IBM TS2900 Tape Autoloader w/LTO6 HH SAS
6171S7R	IBM TS2900 Tape Autoloader w/LTO7 HH SAS
External tape backup libraries	
6741A1F	IBM TS4300 3U Tape Library-Base Unit
6741A3F	IBM TS4300 3U Tape Library-Expansion Unit
Full High 8 Gb Fibre Channel for TS4300	
01KP954	LTO 8 FH Fibre Channel Drive
01KP938	LTO 7 FH Fibre Channel Drive
01KP935	LTO 6 FH Fibre Channel Drive
Half High 8 Gb Fibre Channel for TS4300	
01KP952	LTO 8 HH Fibre Channel Drive
01KP936	LTO 7 HH Fibre Channel Drive
01KP933	LTO 6 HH Fibre Channel Drive
Half High 6 Gb SAS for TS4300	
01KP953	LTO 8 HH SAS Drive
01KP937	LTO 7 HH SAS Drive
01KP934	LTO 6 HH SAS Drive

For more information, see the list of Product Guides in the Backup units category:
https://lenovopress.com/servers/options/backup

Fibre Channel SAN switches

Lenovo offers the ThinkSystem DB Series of Fibre Channel SAN switches and directors for high-performance storage expansion. See the DB Series product guides for models and configuration options:

- ThinkSystem DB Series SAN Switches and Directors: https://lenovopress.com/storage/switches/rack#rt=product-guide

Rack cabinets

The following table lists the supported rack cabinets.

Table 52. Rack cabinets

Part number	Description
7D2B0001WW / 7D2N0001WW	12U 1200mm Deep Micro Datacenter Rack
7D2C0001WW / 7D2P0001WW	18U 1200mm Deep Micro Datacenter Rack
93072RX	25U Standard Rack
93072PX	25U Static S2 Standard Rack
93634PX	42U 1100mm Dynamic Rack
93634EX	42U 1100mm Dynamic Expansion Rack
93604PX	42U 1200mm Deep Dynamic Rack
93614PX	42U 1200mm Deep Static Rack
93084EX	42U Enterprise Expansion Rack
93084PX	42U Enterprise Rack
93074RX	42U Standard Rack

For specifications about these racks, see the Lenovo Rack Cabinet Reference, available from: https://lenovopress.com/lp1287-lenovo-rack-cabinet-reference

For more information, see the list of Product Guides in the Rack cabinets category: https://lenovopress.com/servers/options/racks

KVM switches and consoles

The following table lists the supported KVM consoles, keyboards, and KVM switches.

Table 53. Console keyboards

Part number	Description
Console keyboards	
7ZB7A05469	ThinkSystem Keyboard w/ Int. Pointing Device USB - Arabic 253 RoHS v2
7ZB7A05468	ThinkSystem Keyboard w/ Int. Pointing Device USB - Belg/UK 120 RoHS v2
7ZB7A05206	ThinkSystem Keyboard w/ Int. Pointing Device USB - Czech 489 RoHS v2
7ZB7A05207	ThinkSystem Keyboard w/ Int. Pointing Device USB - Danish 159 RoHS v2
7ZB7A05208	ThinkSystem Keyboard w/ Int. Pointing Device USB - Dutch 143 RoHS v2
7ZB7A05210	ThinkSystem Keyboard w/ Int. Pointing Device USB - Fr/Canada 445 RoHS v2
7ZB7A05209	ThinkSystem Keyboard w/ Int. Pointing Device USB - French 189 RoHS v2
7ZB7A05211	ThinkSystem Keyboard w/ Int. Pointing Device USB - German 129 RoHS v2
7ZB7A05212	ThinkSystem Keyboard w/ Int. Pointing Device USB - Greek 219 RoHS v2
7ZB7A05213	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hebrew 212 RoHS v2
7ZB7A05214	ThinkSystem Keyboard w/ Int. Pointing Device USB - Hungarian 208 RoHS v2

Part number	Description
7ZB7A05215	ThinkSystem Keyboard w/ Int. Pointing Device USB - Italian 141 RoHS v2
7ZB7A05216	ThinkSystem Keyboard w/ Int. Pointing Device USB - Japanese 194 RoHS v2
7ZB7A05217	ThinkSystem Keyboard w/ Int. Pointing Device USB - Korean 413 RoHS v2
7ZB7A05218	ThinkSystem Keyboard w/ Int. Pointing Device USB - LA Span 171 RoHS v2
7ZB7A05219	ThinkSystem Keyboard w/ Int. Pointing Device USB - Norwegian 155 RoHS v2
7ZB7A05220	ThinkSystem Keyboard w/ Int. Pointing Device USB - Polish 214 RoHS v2
7ZB7A05221	ThinkSystem Keyboard w/ Int. Pointing Device USB - Portuguese 163 RoHS v2
7ZB7A05222	ThinkSystem Keyboard w/ Int. Pointing Device USB - Russian 441 RoHS v2
7ZB7A05223	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovak 245 RoHS v2
7ZB7A05231	ThinkSystem Keyboard w/ Int. Pointing Device USB - Slovenian 234 RoHS v2
7ZB7A05224	ThinkSystem Keyboard w/ Int. Pointing Device USB - Spanish 172 RoHS v2
7ZB7A05225	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swed/Finn 153 RoHS v2
7ZB7A05226	ThinkSystem Keyboard w/ Int. Pointing Device USB - Swiss F/G 150 RoHS v2
7ZB7A05227	ThinkSystem Keyboard w/ Int. Pointing Device USB - Thai 191 RoHS v2
7ZB7A05467	ThinkSystem Keyboard w/ Int. Pointing Device USB - Trad Chinese/US 467 RoHS v2
7ZB7A05228	ThinkSystem Keyboard w/ Int. Pointing Device USB - Turkish 179 RoHS v2
7ZB7A05229	ThinkSystem Keyboard w/ Int. Pointing Device USB - UK Eng 166 RoHS v2
7ZB7A05470	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Eng 103P RoHS v2
7ZB7A05230	ThinkSystem Keyboard w/ Int. Pointing Device USB - US Euro 103P RoHS v2
ThinkSystem Digital and Analog KVM Console switches and cables	
1754D1T	ThinkSystem Digital 2x1x16 KVM Switch (DVI video output port)
1754A1T	ThinkSystem Analog 1x8 KVM Switch (DVI video output port)
4X97A11108	ThinkSystem VGA to DVI Conversion Cable
4X97A11109	ThinkSystem Single-USB Conversion Cable for Digital KVM
4X97A11107	ThinkSystem Dual-USB Conversion Cable for Digital KVM
4X97A11106	ThinkSystem USB Conversion Cable for Analog KVM
GCM and LCM Console switches and cables	
1754D2X	Global 4x2x32 Console Manager (GCM32)
1754D1X	Global 2x2x16 Console Manager (GCM16)
1754A2X	Local 2x16 Console Manager (LCM16)
1754A1X	Local 1x8 Console Manager (LCM8)
43V6147	Single Cable USB Conversion Option (UCO)
39M2895	USB Conversion Option (4 Pack UCO)
46M5383	Virtual Media Conversion Option Gen2 (VCO2)
46M5382	Serial Conversion Option (SCO)

For more information, see the list of Product Guides in the KVM Switches and Consoles category:
http://lenovopress.com/servers/options/kvm

Power distribution units

The following table lists the power distribution units (PDUs) that are offered by Lenovo.

Table 54. Power distribution units

Part number	Description
0U Basic PDUs	
00YJ776	0U 36 C13/6 C19 24A/200-240V 1 Phase PDU with NEMA L6-30P line cord
00YJ777	0U 36 C13/6 C19 32A/200-240V 1 Phase PDU with IEC60309 332P6 line cord
00YJ778	0U 21 C13/12 C19 32A/200-240V/346-415V 3 Phase PDU with IEC60309 532P6 line cord
00YJ779	0U 21 C13/12 C19 48A/200-240V 3 Phase PDU with IEC60309 460P9 line cord
Switched and Monitored PDUs	
00YJ780	0U 20 C13/4 C19 Switched and Monitored 32A/200-240V/1Ph PDU w/ IEC60309 332P6 line cord
00YJ781	0U 20 C13/4 C19 Switched and Monitored 24A/200-240V/1Ph PDU w/ NEMA L6-30P line cord
00YJ782	0U 18 C13/6 C19 Switched / Monitored 32A/200-240V/346-415V/3Ph PDU w/ IEC60309 532P6 cord
00YJ783	0U 12 C13/12 C19 Switched and Monitored 48A/200-240V/3Ph PDU w/ IEC60309 460P9 line cord
46M4003	1U 9 C19/3 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
46M4004	1U 12 C13 Switched and Monitored DPI PDU (without line cord)
46M4005	1U 12 C13 Switched and Monitored 60A 3 Phase PDU with IEC 309 3P+Gnd line cord
Ultra Density Enterprise PDUs (9x IEC 320 C13 + 3x IEC 320 C19 outlets)	
71762NX	Ultra Density Enterprise C19/C13 PDU Module (without line cord)
71763NU	Ultra Density Enterprise C19/C13 PDU 60A/208V/3ph with IEC 309 3P+Gnd line cord
C13 Enterprise PDUs (12x IEC 320 C13 outlets)	
39M2816	DPI C13 Enterprise PDU+ (without line cord)
39Y8941	DPI Single Phase C13 Enterprise PDU (without line cord)
C19 Enterprise PDUs (6x IEC 320 C19 outlets)	
39Y8948	DPI Single Phase C19 Enterprise PDU (without line cord)
39Y8923	DPI 60A 3 Phase C19 Enterprise PDU with IEC 309 3P+G (208 V) fixed line cord
Front-end PDUs (3x IEC 320 C19 outlets)	
39Y8938	DPI 30amp/125V Front-end PDU with NEMA L5-30P line cord
39Y8939	DPI 30amp/250V Front-end PDU with NEMA L6-30P line cord
39Y8934	DPI 32amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8940	DPI 60amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
39Y8935	DPI 63amp/250V Front-end PDU with IEC 309 2P+Gnd line cord
NEMA PDUs (6x NEMA 5-15R outlets)	
39Y8905	DPI 100-127V PDU with Fixed NEMA L5-15P line cord
Line cords for PDUs that ship without a line cord	
40K9611	DPI 32a Line Cord (IEC 309 3P+N+G)
40K9612	DPI 32a Line Cord (IEC 309 P+N+G)
40K9613	DPI 63a Cord (IEC 309 P+N+G)
40K9614	DPI 30a Line Cord (NEMA L6-30P)
40K9615	DPI 60a Cord (IEC 309 2P+G)
40K9617	DPI Australian/NZ 3112 Line Cord
40K9618	DPI Korean 8305 Line Cord

For more information, see the Lenovo Press documents in the PDU category:
https://lenovopress.com/servers/options/pdu

Uninterruptible power supply units

The following table lists the uninterruptible power supply (UPS) units that are offered by Lenovo.

Table 55. Uninterruptible power supply units

Part number	Description
55941AX	RT1.5kVA 2U Rack or Tower UPS (100-125VAC)
55941KX	RT1.5kVA 2U Rack or Tower UPS (200-240VAC)
55942AX	RT2.2kVA 2U Rack or Tower UPS (100-125VAC)
55942KX	RT2.2kVA 2U Rack or Tower UPS (200-240VAC)
55943AX	RT3kVA 2U Rack or Tower UPS (100-125VAC)
55943KX	RT3kVA 2U Rack or Tower UPS (200-240VAC)
55945KX	RT5kVA 3U Rack or Tower UPS (200-240VAC)
55946KX	RT6kVA 3U Rack or Tower UPS (200-240VAC)
55948KX	RT8kVA 6U Rack or Tower UPS (200-240VAC)
55949KX	RT11kVA 6U Rack or Tower UPS (200-240VAC)
55948PX	RT8kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55949PX	RT11kVA 6U 3:1 Phase Rack or Tower UPS (380-415VAC)
55943KT†	ThinkSystem RT3kVA 2U Standard UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55943LT†	ThinkSystem RT3kVA 2U Long Backup UPS (200-230VAC) (2x C13 10A, 2x GB 10A, 1x C19 16A outlets)
55946KT†	ThinkSystem RT6kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)
5594XKT†	ThinkSystem RT10kVA 5U UPS (200-230VAC) (2x C13 10A outlets, 1x Terminal Block output)

† Only available in China and countries in the Asia Pacific region.

For more information, see the list of Product Guides in the UPS category:
https://lenovopress.com/servers/options/ups

Lenovo Financial Services

Lenovo Financial Services reinforces Lenovo's commitment to deliver pioneering products and services that are recognized for their quality, excellence, and trustworthiness. Lenovo Financial Services offers financing solutions and services that complement your technology solution anywhere in the world.

We are dedicated to delivering a positive finance experience for customers like you who want to maximize your purchase power by obtaining the technology you need today, protect against technology obsolescence, and preserve your capital for other uses.

We work with businesses, non-profit organizations, governments and educational institutions to finance their entire technology solution. We focus on making it easy to do business with us. Our highly experienced team of finance professionals operates in a work culture that emphasizes the importance of providing outstanding customer service. Our systems, processes and flexible policies support our goal of providing customers with a positive experience.

We finance your entire solution. Unlike others, we allow you to bundle everything you need from hardware and software to service contracts, installation costs, training fees, and sales tax. If you decide weeks or months later to add to your solution, we can consolidate everything into a single invoice.

Our Premier Client services provide large accounts with special handling services to ensure these complex transactions are serviced properly. As a premier client, you have a dedicated finance specialist who manages your account through its life, from first invoice through asset return or purchase. This specialist develops an in-depth understanding of your invoice and payment requirements. For you, this dedication provides a high-quality, easy, and positive financing experience.

For your region specific offers please ask your Lenovo sales representative or your technology provider about the use of Lenovo Financial Services. For more information, see the following Lenovo website:

https://www.lenovo.com/us/en/landingpage/lenovo-financial-services/

Related publications and links

For more information, see these resources:

- ThinkSystem SR530 product page
  https://www.lenovo.com/us/en/data-center/servers/racks/ThinkSystem-SR530/p/77XX7SRSR53
- Datasheet for the ThinkSystem SR530:
  https://lenovopress.com/ds0002-lenovo-thinksystem-sr530
- 3D Interactive Tour of the ThinkSystem SR530:
  https://lenovopress.com/lp0670-3d-tour-thinksystem-sr530
- Walkthrough Video for the ThinkSystem SR530:
  https://lenovopress.com/lp0744-thinksystem-sr530-server-video-walkthrough
- User Manuals for the ThinkSystem SR530:
  https://thinksystem.lenovofiles.com/help/topic/7X07/introduction.html?cp=4_2
  - Quick Start Guide
  - Setup Guide
  - Rack Installation Guides
  - Maintenance Manual
  - Messages and Codes Reference
  - UEFI Manual
- Lenovo Data Center Support Downloads - ThinkSystem SR530:
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x07/downloads
  http://datacentersupport.lenovo.com/products/servers/thinksystem/sr530/7x08/downloads
- Lenovo Hardware Installation & Removal Videos on the ThinkSystem SR530:
  - YouTube: https://www.youtube.com/playlist?list=PLYV5R7hVcs-AQrHuDWK6L3KtHWc6maY_O
  - Youku: https://list.youku.com/albumlist/show/id_50437162
- Lenovo Data Center Solution Configurator (DCSC):
  http://dcsc.lenovo.com

Related product families

Product families related to this document are the following:

- 2-Socket Rack Servers
- ThinkSystem SR530 Server

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2021. All rights reserved.

This document, LP1045, was created or updated on March 2, 2021.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  http://lenovopress.com/LP1045
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at http://lenovopress.com/LP1045.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
Bootable Media Creator
Flex System
Lenovo Services
RackSwitch
System x®
ThinkSystem
TopSeller
TruDDR4
UpdateXpress System Packs
XClarity®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Hyper-V®, Microsoft®, PowerShell, Windows PowerShell®, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 01 - MODELO SERVIDOR DE RACK	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
Arquitetura e gabinete	N/A	N/A	N/A
- Os servidores deverão possuir arquitetura de processadores que permitam a execução de aplicativos de 32 e 64 bits.	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Intel® 64 Sim
- Compatível com a arquitetura x86/64, na versão mais atualizada do modelo ofertado;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Intel® 64 Sim
- Suporte à migração de máquinas virtuais entre diferentes versões de processadores do mesmo fabricante (extended migration/flex migration);	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications	2	Tecnologia de virtualização Intel® (VT-x) Sim Tecnologia de virtualização Intel® para E/S dirigida (VT-d) Sim
- Suporte à virtualização de servidores;	lp1045.pdf	2	Intel Virtualization Technology integrates hardware-level virtualization hooks that allow operating system vendors to better utilize the hardware for virtualization workloads.
- Deve ocupar, no máximo, 1U no rack;	lp1045.pdf	1	Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.
- O Gabinete deverá ser do mesmo fabricante do equipamento.	lp1045.pdf	1	Lenovo ThinkSystem SR530 is an ideal 2-socket 1U rack server for small businesses up to large enterprises that need industry-leading reliability, management, and security, as well as cost-optimized performance and flexibility for future growth. Designed to handle a wide range of workloads, such as IT infrastructure, collaboration, and entry cloud, it can be the foundation of your online business.
Placa Mãe e microcomponentes	N/A	N/A	N/A
- A placa mãe deve ser da mesma marca do fabricante do processador do equipamento, não sendo aceitas soluções de outros fabricantes em regime de OEM ou customizações;	lp1045.pdf	6	Chipset Intel C622.
- O Chipset deve ser do mesmo fabricante do processador ou do fabricante da placa mãe, sendo específico para servidores.	lp1045.pdf	6	Chipset Intel C622.
BIOS ou UEFI	N/A	N/A	N/A
- O BIOS ou UEFI deve ser desenvolvido pelo mesmo fabricante do equipamento ou o fabricante deve ter direito de cópia sobre esse BIOS, comprovando através de atestado fornecido pelo fabricante do equipamento;	uefi_setting_guide.pdf	1	UEFI is an interface packed with various features, including system information and settings, boot and runtime services, BMC settings, system event logs, and user security. This guide applies to the following server models:
- O BIOS ou UEFI deve possuir recurso de controle de permissão através de senhas, uma para inicializar o equipamento e outra para acesso e alterações das configurações do BIOS ou UEFI;	uefi_setting_guide.pdf uefi_setting_guide.pdf	38 49	Secure Boot Configuration User security Use this menu to set or change Power-On and Administrator passwords.

- Possibilidade de selecionar a unidade de inicialização do sistema contemplando disco rígido, unidade USB ou via rede local;	uefi_setting_guide.pdf	43 e 44	Add UEFI Full Path Boot Option Add one UEFI application or one removable file systems as boot option. Set Boot Priority Set boot priority of the devices in a device group.
- O BIOS ou UEFI deve possuir recursos de inserção de comandos remotamente através de scripts;	uefi_setting_guide.pdf	3	Perform the following steps to first launch the UEFI setup utilities. 1. (Optional)Connect the local keyboard, video, and mouse (KVM) to the server using a cable, or open the Remote Console page on the Lenovo XClarity Controller web user interface (XCC WebUI).
- O BIOS ou UEFI deve possuir número de série / Serviço do equipamento, bem como um campo editável que permita inserir identificação de ativo e que possa ser consultado por software de gerenciamento.	Think_BIOS_Configurator_Manual.pdf	3	At the top of the application screen is the File Actions section. On the left it is possible to browse to and select an .INI file that was previously generated by this program. Once selected, click Apply Settings File to make any changes detected in the .INI file. All the settings are read into the potential changes and then compared to the current settings of the machine. Only those that are different will be applied. A dialog box is displayed once the import is completed showing the settings that were successfully changed. This feature is also available via command line which is discussed in the Execution via Command Line section.
- BIOS/UEFI deve ser 100% (cem por cento) compatível com software de gerenciamento;	xcc_book.pdf	1	This document explains how to use the functions of the XClarity Controller in a ThinkSystem server. The XClarity Controller works with the XClarity Provisioning Manager and UEFI to provide systems-management capability for ThinkSystem servers.
- Implementação em memória atualizável por software;	LXPM_user_guide.pdf	42	Firmware Update Click the Firmware Update tab in the left pane to enter the Firmware Update interface. You can update the UEFI firmware, Lenovo XClarity Controller, LXPM V3, Windows drivers, and Linux drivers for your server in the Firmware Update interface. To download the update packages, go to:
- Relógio calendário (ano com quatro posições) de tempo real, não volátil protegido por bateria;	uefi_setting_guide.pdf maintenance_manual.pdf	40 e 41 26	Date and time Use this menu to set the local Date and Time of the system. Clear CMOS jumper JP3 • Pins 1 and 2: The jumper is in default setting. • Pins 2 and 3: Clear the real-time clock (RTC) registry.
- Todos os itens que forem integrados à placa principal deverão possuir recursos para desativação, preferencialmente, via BIOS.	uefi_setting_guide.pdf maintenance_manual.pdf	11 23	System setting Select System Settings and press Enter. Then the following window is displayed: Figure 10. System board components
Processador	N/A	N/A	N/A
- Deve possuir 01 processador x86, com extensão de 64 bits, com dez núcleos ou mais sendo próprio para servidores;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- O processador deverá ser de acordo com a pontuação de desempenho, conforme informado no item abaixo com a devida comprovação;	N/A	N/A	N/A

- Suporte a software de gerenciamento remoto do Servidor;	lxca_users_guide.pdf	2	Configuration management You can quickly provision and pre-provision all of your servers using a consistent configuration. Configuration settings (such as local storage, I/O adapters, boot settings, firmware, ports, and management controller and UEFI settings) are saved as a server pattern that can be applied to one or more managed servers. When the server patterns are updated, the changes are automatically deployed to the applied servers.
- Deve possuir memória cachê L3 de 13,75 MB;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- Deve possuir tecnologia Intel Turbo Boost;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	2	Tecnologia Intel® Turbo Boost 2.0
- Deve operar com QuickPath InterConnect (QPI) de, no mínimo, 9.6 GTps;	lp1045.pdf	17	Intel Xeon Gold processors 5215 10 / 20 2.5 / 3.4 GHz 13.75 MB 2666 MHz 1 TB 10.4 GT/s 85 W
- Deve possuir tecnologia de otimização para virtualização;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	2	Tecnologia de virtualização Intel® (VT-x) Sim Tecnologia de virtualização Intel® para E/S dirigida (VT-d) Sim Intel® VT-x com Tabelas de páginas estendidas (EPT) Sim
- Possuir tecnologia Hyper Threading para até 10 Cores e 20 threads total;	Processador Intel® Xeon® Gold 5215 (cache de 13,75 M, 2,50 GHz) Product Specifications.pdf	1	Número de núcleos 10 Nº de threads 20
- Possuir barramento de sistema (bus) com desempenho igual ou superior ao utilizado no respectivo teste (benchmark) publicado pela organização SPEC;	cpu2017-20190513-13808.pdf	1	Hardware
- Todos os servidores X86 fornecidos pela CONTRATADA, deverão prover sistema de detecção de falha dos componentes vitais ao sistema (CPU, memória, discos, ventiladores e fontes).	lp1045.pdf	3	Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
Desempenho	N/A	N/A	N/A
- O modelo de equipamento ofertado deve possuir índice de desempenho SPEC 2017 INTEGER BASELINE de, no mínimo, 40 pontos auditado pelo Standard Performance Evaluation Corporation, por CPU. Não serão aceitos modelos de equipamentos não auditados pelo Standard Performance Evaluation Corporation;	cpu2017-20190513-13808.pdf	1	SPECrate2017_int_base = 119
- Os resultados devem estar publicados no site www.spec.org para comprovação.	cpu2017-20190513-13808.pdf	1	SPECrate2017_int_base = 119
Memória	N/A	N/A	N/A
- O processador deve suportar memória RAM do tipo RDIMM DDR4 (Registered DIMM DDR4) com ECC (Error Checkin and Correction) ou tecnologia equivalente e que opere em freqüência igual ou superior a 2666MHz;	lp1045.pdf	6	Memory protection Error correction code (ECC), SDDC (for x4-based memory DIMMs), ADDDC (for x4-based memory DIMMs, requires Intel Xeon Gold or Platinum processors), memory mirroring, memory rank sparing, patrol scrubbing, and demand scrubbing.
- O servidor deve possuir, no mínimo, 32GB de memória RAM em módulos de memória tipo RDIMM DDR4 de pelo menos, 16GB cada, com tecnologia de distribuição de informação detectada pelo recurso ECC, para que, em um caso de falha de memória, as informações possam ser reconstruídas;	Conforme Proposta Comercial		

- Deve possuir possibilidade de expansão de memória para, pelo menos, 384GB (registered DDR4 DIMMs) e possuir no mínimo 12 slots de memória.	lp1045.pdf	6	Memory Up to 12 DIMM sockets (6 DIMMs per processor; six memory channels per processor with one DIMM per channel) with support for the following TruDDR4 RDIMM types and capacities: 8 GB, 16 GB, 32 GB, and 64 GB 2933 MHz. 16 GB and 32 GB 2666 MHz.
Expansão	N/A	N/A	N/A
- O sistema deve suportar, pelo menos, três slots tipo PCI Express versão 3.0 ou superior de 8 vias (x8) ou mais rápido;	lp1045.pdf	6	I/O expansion slots Up to three slots depending on the riser cards installed. The slots are as follows: Slot 1: PCIe 3.0 x8; low profile Slot 2: PCIe 3.0 x16 or ML2 x8; low profile or full-height, half-length Slot 3: PCIe 3.0 x8 or x16; low profile PCIe x16 slot 3 requires the second processor to be installed.
- Deverá ter, pelo menos, 1 slot específico para uma placa 1/10Gbits dual-port. não sendo esse um dos dois slots citados no item acima, podendo ser um slot on-board.	lp1045.pdf	6	Network interfaces Onboard LOM slot for up to two additional 1/10 Gb Ethernet ports: 2x 10 GbE RJ-45 ports (no 10/100 Mb support) 1x RJ-45 10/100/1000 Mb Ethernet systems management port.
Porta de E/S	N/A	N/A	N/A
- Todos os conectores das portas de entrada/saída de sinal devem ser identificados pelos respectivos nomes ou símbolos;	lp1045.pdf	4	Figure 2. Front view of the SR530: 4x 3.5-inch drive bays Figure 3. Front view of the SR530: 8x 2.5-inch drive bays
- O equipamento deve possuir, no mínimo, 03 portas USB versão 3.0, sendo pelo menos 01 (uma) delas situadas na parte frontal do gabinete e 02 (duas) na parte traseira;	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
- O equipamento deve possuir, no mínimo, 01 (uma) porta para monitor de vídeo padrão VGA na parte traseira do equipamento, e possibilidade de incluir mais 01 (uma) porta padrão VGA na parte frontal.	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port.
Interface de Rede Gigabit RJ-45	N/A		
- O equipamento deve possuir, no mínimo, 2 (duas) interfaces de rede com conector tipo RJ 45;	lp0654.pdf	1	The Intel Ethernet Connection X722 is a network controller embedded into the Intel C624 "Lewisburg" PCH chipset of Lenovo ThinkSystem servers. The controller connects to available 10 GbE and 1 Gigabit Ethernet LAN-on-motherboard (LOM) adapter cards and onboard connectors to provide a comprehensive 1 GbE / 10 GbE networking solution for ThinkSystem customers.
- As interfaces devem ser capazes de operar nos padrões 10/100/1000;	lp0654.pdf	8 10	Adapter connectors: 10 GbE 10GBASE-T adapters: RJ45 connectors 10 GbE standards: IEEE 802.3ab 1000BASE-T copper twisted pair Gigabit Ethernet IEEE 802.3an 10GBASE-T copper twisted pair 10 Gb Ethernet
- IEEE 802.1Qbg Edge Virtual Bridging;	lp0654.pdf	8	Virtual Bridging Support: VEPA/802.1Qbg
- TCP, IP, and UDP checksum offload;	lp0654.pdf	9	TCP/UDP/IP/SCTP Checksum Offload

- Large Send Offload (LSO) and Generic Send Offload (GSO)	lp0654.pdf	6	VXLAN, NVGRE and GENEVE Hardware Offloads: These stateless offloads preserve application performance for overlay networks. With these offloads, it is possible to distribute network traffic across CPU cores. At the same time, the controller offloads LSO, GSO, and checksum from the host software, which reduces CPU overhead.
- Permitir implementação de load balance e failover;	lp0654.pdf	10	IEEE 802.3ad Link Aggregation Control Protocol
- Admite-se interface de rede embutida na placa principal, desde que mantidas as características descritas nos subitens anteriores.	lp1045.pdf	6	The SR530 server has two onboard 1 GbE ports (no 10/100 Mb support) and up to two additional onboard 1/10 GbE network ports (no 10/100 Mb support) with optional LOM cards. Onboard ports and LOM cards use the Intel Ethernet Connection X722 1/10 GbE technology integrated into the Intel C622 Platform Controller Hub (PCH).
Fonte de Alimentação e Sistema de Ventilação	N/A	N/A	N/A
- O equipamento deve suportar fontes de alimentação redundantes e hot, cada uma com potência suficiente para manter o funcionamento do equipamento em sua configuração máxima;	lp1045.pdf	6	Power supply Up to two redundant hot-swap 550 W or 750 W (100 - 240 V) High Efficiency Platinum or 750 W (200 - 240 V) High Efficiency Titanium AC power supplies. HVDC support (PRC only).
- No mínimo, 01 (uma) fonte de alimentação por equipamento;	Conforme Proposta Comercial	N/A	N/A
- A fonte deve possuir LED indicador de status e suportar uma faixa de tensão de entrada de 100 a 127 VAC e 200 a 240 VAC em 60 Hz, com chaveamento automático de voltagem;	maintenance_manual.pdf	21	The following illustration shows the LEDs on the rear view of server models with three PCIe slots. The LEDs on the rear view of server models with two PCIe slots are the same.
- Recurso de troca sem interrupção para as fontes;	lp1045.pdf	35	Power supplies and cables The SR530 server supports up to two redundant power supplies and is capable of N+N redundancy depending on the configuration. A second power supply can be added to the models that come with one power supply. The following table lists the power supply options.
- A fonte deve possuir, no mínimo 750 W de potência e certificação 80+ Platinum comprovada mediante publicação no site www.plugloadsolutions.com/80pluspowersupplies.aspx;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Deve ser fornecido cabo de alimentação para a fonte de alimentação de forma a possibilitar sua instalação;	Conforme Proposta Comercial		
- O equipamento deve possuir ventilação adequada para a refrigeração de seu sistema interno na sua configuração máxima e dentro dos limites de temperatura adequados para operação;	lp1045.pdf	35	Cooling The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.
- Os ventiladores devem ser redundantes.	lp1045.pdf	35	Cooling The SR530 server supports up to six non-hot-swap system fans that provide N+1 cooling redundancy. SR530 server models with one processor include four system fans, and server models with two processors include six system fans.
Software de Gernciamento	N/A	N/A	N/A

- Deverá ser fornecido software de gerenciamento desenvolvido pelo fabricante do equipamento;	xcc_book.pdf	1	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers. It is the follow-on to the Integrated Management Module II (IMM2) service processor that consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities into a single chip on the server system board. It provides features such as the following: • Choice of a dedicated or shared Ethernet connection for systems management • Support for HTML5 • Support for access via XClarity Mobile • XClarity Provisioning Manager • Remote configuration using XClarity Essentials or XClarity Controller CLI. • Capability for applications and tools to access the XClarity Controller either locally or remotely • Enhanced remote-presence capabilities. • REST API (Redfish schema) support for additional web-related services and software applications.
- O equipamento ofertado deverá possuir placa de gerenciamento remoto in band que possibilite seu gerenciamento através de porta RJ-45, não sendo essa nenhuma das interfaces de rede mencionadas no item interface de Rede;	lp1045.pdf	6	Ports Front: 1x USB 2.0 port with XClarity Controller access and 1x USB 3.0 port; optional 1x VGA port. Rear: 2x USB 3.0 ports and 1x VGA port; optional 1x DB-9 serial port. Systems management XClarity Controller (XCC) Standard, Advanced, or Enterprise (Pilot 4 chip), proactive platform alerts, XClarity Provisioning Manager, XClarity Essentials, XClarity Administrator, XClarity Integrators for VMware vCenter and Microsoft System Center, XClarity Energy Manager, Capacity Planner.

- Solução de gerenciamento de sistemas físicos e virtuais em ambiente heterogêneo, com suporte a vários sistemas operacionais e tecnologias de virtualização;	lxca_users_guide.pdf	1 2 4	Hardware management XClarity Administrator provides agent-free hardware management. It can automatically discover manageable devices, including server, network, and storage hardware. Inventory data is collected for managed devices for an at-a-glance view of the managed hardware inventory and status. Operating-system deployment You can use XClarity Administrator to manage a repository of operating-system images and to deploy operating-system images to up to 28 servers managed servers concurrently. Integration with other managed software XClarity Administrator modules integrate XClarity Administrator with third-party management software to provide discovery, monitoring, configuration, and management functions to reduce the cost and complexity of routine system administration for supported devices. For more information about XClarity Administrator, see the following documents: • Lenovo XClarity Integrator for Microsoft System Center • Lenovo XClarity Integrator for VMware vCenter • Lenovo XClarity Integrator for Nutanix Prism
- O Módulo / Placa de gerenciamento deve ser do mesmo fabricante do equipamento, mantendo total compatibilidade com o mesmo e integração total com o software de gerenciamento solicitado. Tal solução deve possuir as seguintes características;	xcc_book.pdf	1	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers.
- Fazer uso de criptografia para acesso a console WEB e console CLI, de forma a dificultar a interceptação de dados;	xcc_book.pdf	6	Use the information in this topic to view the list of supported browsers, cipher suites and operating systems for your server. For increased security, only high strength ciphers are now supported when using HTTPS. When using HTTPS, the combination of your client operating system and browser must support one of the following cipher suites:
- Possuir interface de linha de comando e Web. Para interface Web, por meio de browser padrão poder realizar as tarefas de monitoração e controle, sem nenhum software adicional e independente do sistema operacional;	xcc_book.pdf	6 89	Use the information in this topic to view the list of supported browsers, cipher suites and operating systems for your server. Use the XClarity Controller command line interface (CLI) to access the XClarity Controller without having to use the web interface. It provides a subset of the management functions that are provided by the web interface.

- Permitir visualizar e interagir com aplicativos em um sistema remoto, exibindo a imagem da tela do sistema, utilizando ferramentas de controle remoto padrão de mercado, incluindo o VNC (Virtual Network Computing), RDP (Remote Desktop) e controle remoto baseado na Web para RSA	xcc_book.pdf	61	Remote Console Functionality Use the information in this topic to understand how to remotely view and interact with the server console. You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console. You can assign a disk image (ISO or IMG file) as a virtual drive on the server. The remote console functionality is available with the XClarity Controller Advanced and XClarity Controller Enterprise features and is only available through the web interface. You must log in to the XClarity Controller with a user ID that has Supervisor access or Remote Console Access privileges to use the remote console features.
- O chip/ placa/ módulo deve ser único em cada servidor e fornecer diagnósticos, presença virtual e controle remoto para gerenciar, monitorar e resolver problemas;	xcc_book.pdf	1 61	The Lenovo XClarity Controller (XCC) is the next generation management controller that replaces the baseboard management controller (BMC) for Lenovo ThinkSystem servers. You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console.
- Segurança de acesso e utilização do protocolo TCP/IP;	xcc_book.pdf	36	SSL overview This topic is an overview of the SSL security protocol. SSL is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that prevents eavesdropping, tampering, and message forgery. You can configure the XClarity Controller to use SSL support for different types of connections, such as secure web server (HTTPS), secure LDAP connection (LDAPS), CIM over HTTPS, and SSH server, and to manage the certificates that are required for SSL.
- Ser totalmente compatível com os padrões de gerenciamento IPMI (Intelligent Platform Management Interface) 2.0;	xcc_book.pdf	2	Industry Standard Management Interfaces • IPMI 2.0 Interface • Redfish • CIM-XML • DCMI 1.5 • SNMPv3 • SNMPv1 (Traps Only) requires minimum v2.10 or v2.12 XCC Firmware updates depending on server type. See XCC Firmware update Change file for details.
- Deve permitir controle remoto tipo virtual KVM, mesmo quando o sistema operacional estiver inoperante;	xcc_book.pdf	61 61 63	You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console. The remote console is able to display only the video that is generated by the video controller on the system board. Remote console capture screen Use the information in this topic to understand how to use the remote console screen capture feature. The screen capture feature in the remote console window captures the video display contents of the server. To capture and save a screen image, complete the following steps:

- Deve informar o status do equipamento, indicando os componentes com falha e notificando o administrador via e-mail ou trap SNMP;	xcc_book.pdf	52	To add and modify email and syslog notifications or SNMP TRAP recipients, use the information in this topic.
- Suportar o envio de mensagens de Pré-Falha para no mínimo processadores, fontes, memória, ventiladores e discos;	lp1045.pdf	3	Allows preventive actions in advance of possible failure, thereby increasing server uptime and application availability with Proactive Platform Alerts (including PFA and SMART alerts) for processors, voltage regulators, memory, internal storage (SAS/SATA HDDs and SSDs, M.2 storage), fans, power supplies, RAID controllers, and server ambient and sub-component temperatures.
- Deve permitir remotamente o acesso as mensagens do equipamento, por serial ou LAN;	xcc_book.pdf	33	Enabling or Disabling IPMI Network Access Use the information in this topic to control IPMI network access to the XClarity Controller. Click Network under BMC Configuration to view or modify XClarity Controller IPMI settings. Complete the following fields to view or modify IPMI settings: IPMI over LAN Access Click the switch to enable or disable IPMI network access to the XClarity Controller. Important: • If you are not using any tools or applications that access the XClarity Controller through the network using the IPMI protocol, it is highly recommended that you disable IPMI network access for improved security. • IPMI over LAN access to the XClarity Controller is disabled by default.

- Suporte a SSL e SSH de no mínimo 128bits;	xcc_book.pdf	3 6	Network Protocols • DHCP • DNS • DDNS • HTTP/HTTPS • SNMPv3 • SNMPv1 (Traps only) • SSL • SSH • SMTP • LDAP client • NTP • SLP • SSDP • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-SHA256
- Permitir transferir arquivos de um local para outro e sincronizar arquivos, diretórios ou unidades, utilizando uma alternativa segura para o FTP;	xcc_book.pdf	65 68	Media mount methods – SFTP – SSH File Transfer Protocol – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the checkbox. – Enter the credentials that are need to for the XClarity Controller to access the file on the remote system.

- Deve possuir tecnologia de mídia virtual, possibilitando que imagens ISSO sejam montadas remotamente ou através de compartilhamentos CIFS, NFS ou HTTPFS, permitindo inclusive a inicialização (boot) através dessas unidades;	xcc_book.pdf	65 e 66	Media mount methods – CIFS - Common Internet File System: – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the check box. – Enter the credentials that are needed for the XClarity Controller to access the file on the remote system. Note: The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space. – Mount options are optional and defined by the CIFS protocol. – If the remote server belongs to a collection of servers, where the security is centrally handled, enter the domain name to which the remote server belongs. – NFS - Network File System: – Enter the URL that locates the file on the remote system. – If you want the file to be presented to the server as read-only virtual media, tick the checkbox. – Mount options are optional and defined by the NFS protocol. Both NFSv3 and NFSv4 are supported. For example, to use NFSv3, you need to specify option 'nfsvers=3'. If the NFS server uses AUTH_ SYS security flavor to authenticate NFS operations, you need to specify option 'sec=sys'. – HTTPFS – HTTP Fuse-based File System: – Enter the URL that locates the file on the remote system – If you want the file to be presented to the server as read-only virtual media, tick the check box.
- Deve permitir o desligamento e reinicialização do servidor através da console de gerenciamento, mesmo em condições de indisponibilidade do sistema operacional, além de permitir atualização e configuração remota do BIOS e fornecer indicação de abertura de gabinete e número de série do equipamento;	xcc_book.pdf xcc_book.pdf LXPM_user_guide.pdf LXPM_user_guide.pdf	62 197 10 44	Remote power control This topic explains how to send server power and restart commands from the remote console window. You can send server power and restart commands from the remote console window without returning to the main web page. To control the server power with the remote console, click Power and select one of the following commands: Chassis Intrusion Detection You can enable this function to protect your server by detecting any physical movement of the top cover. System Summary Click the System Summary tab in the left pane to view the following system information in the right p Click the UEFI Setup tab in the left pane to enter the UEFI Setup interface. In the UEFI Setup interface, you can view and change the UEFI settings of your server.

- Possuir gestão automática de chamados ao suporte;	xcc_book.pdf	43	Lenovo is committed to security. When enabled, Call Home automatically contacts Lenovo to open a service ticket and sends in service data collected from a managed device whenever that device reports a hardware failure. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later, your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel.
- Permitir a descoberta, navegação e visualização de sistemas na rede de dados, permitindo o inventário detalhado e relacionamento com os demais recursos da rede.	lxca_users_guide.pdf	1	Lenovo XClarity Administrator is a centralized, resource-management solution that simplifies infrastructure management, speeds responses, and enhances the availability of Lenovo® server systems and solutions. It runs as a virtual appliance that automates discovery, inventory, tracking, monitoring, and provisioning for server, network, and storage hardware in a secure environment.
Documentação Técnica	N/A		
- Certificação de compatibilidade com o sistema Vmware ESXi 6.7 U2 publicada no site https://www.vmware.com/resources;	VMware Compatibility Guide - System Search.pdf	1	Model ThinkSystem SR530 CPU Series Intel Xeon Gold 6200/5200 (Cascade-LakeSP/Refresh) Series
- Certificação de compatibilidade com o sistema operacional RedHat Enterprise Linux 8.x publicada no site https://access.redhat.com/ecosystem/hardware/;	ThinkSystem SR530 (Xeon SP Gen 2) - Red Hat Certified Hardware - Red Hat Customer Portal.pdf	1	Products Level
- Certificado da serie ISO-9001 do fabricante do equipamento;	Lenovo ISO 9001.pdf	1	CERTIFICATE
- Certificado de conformidade contra incidentes elétricos e combustão dos materiais elétricos, (Norma IEC 60950) comprovador através de certificado ou relatório de avaliação de conformidade emitido por um órgão credenciado pelo INMETRO ou Certificado internacional, (Safety of Information Technology Equipment Including Eletrical Business Equipment);	lp1045.pdf	51	Regulatory compliance The ThinkSystem SR530 server conforms to the following regulations: United States: FCC Part 15, Class A; UL 60950-1 Canada: ICES-003/NMB-03, Class A; CAN/CSA-C22.2 60950-1 Mexico: NOM-19 Argentina: IEC60950-1 European Union: CE Mark (EN55022 Class A, IEC/EN60950-1, EN55024, EN61000-3-2, EN61000-3-3)
- Certificado quanto à emissão de radiação radiada e conduzida. Expedido por órgãos competentes comprovando que o equipamento detém da norma CISPR 22 / EN55022;	lp1045.pdf	51	Australia/New Zealand: AS/NZS CISPR 22 Class A
- A documentação solicitada juntamente com a proposta de preços, será apresentada por parte da licitante detentora do menor lance, Caso não remeta a documentação a licitante terá desclassificada a sua proposta de preços;	N/A	N/A	N/A
- Todos os periféricos, placas, controladoras, módulos de memória, disco rígido, deverão ser do mesmo fabricante, ou homologados pelo mesmo.	Conforme Proposta Comercial		
Garantia	N/A		
- O prazo de garantia padrão deverá ser, no mínimo, de 03 (três) anos acrescidos de 02 (dois) anos de garantia estendida, totalizado 05 (cinco) anos de garantia, contado do recebimento provisório. Caso o licitante não seja o próprio fabricante, deverá ser apresentada junto a proposta comercial a relação atualizada de assistência técnica autorizada do fabricante para todo o território nacional;	Conforme Proposta Comercial	N/A	N/A
- Todas as características descritas devem ser comprovadas através de catálogos, manuais, etc;	N/A	N/A	N/A

- Os produtos fornecidos estarão cobertos por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento;	N/A	N/A	N/A
- Declaração da licitante informando a rede autorizada de assistência técnica no Estado do Amazonas. Durante o período de garantia a empresa vencedora devera, sem ônus adicional, fornecer as atualizações (“patches”) corretivas do software e firmware do equipamento fornecido; A empresa vencedora prestará garantia ao sistema fornecido nas seguintes condições: fornecerá informações detalhadas sobre o suporte técnico gratuito (inclusive a ligação telefônica por meio de DDG) em português durante o período de garantia, incluindo atualização de software. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada gratuita (DDG) em horário comercial, de segunda a sexta-feira (8x5). A contratada deverá possuir central de atendimento técnico, com abertura de chamados via DDG 0800 ou portal web ou e-mail (informar os dados de contato na proposta) realizando a gestão dos processos de suporte e atendimento ‘’on-site”. O equipamento deverá possuir 5 anos de garantia “on-site” com atendimento durante horário comercial (8x5) e dias úteis com presença de técnico “on-site”; Os componentes, peças e materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento;	N/A	N/A	N/A
- Condições de Entrega: O transporte dos equipamentos até o local especificado, será realizado pela empresa vencedora (inclusive os procedimentos de seguro, embalagem e transporte até o local especificado);	N/A	N/A	N/A
- A verificação quanto ao estado dos equipamentos após o transporte será de exclusiva responsabilidade da empresa vencedora, sendo que, quaisquer danos observados no transporte, a qualquer tempo, serão reparados pela empresa vencedora;	N/A	N/A	N/A
- Condições Gerais de Fornecimento: Todos os itens de Hardware deverão ser do mesmo fabricante, mesmo que em regime OEM, neste último caso apresentar comprovação desta condição; O sistema deverá ser fornecido com todos os cabos necessários para a interconexão dos equipamentos adquiridos, além de todos os acessórios de montagem e operação; Apresentar atestado de capacidade técnica compatível com os equipamentos solicitados em quantidade similar com fornecimento e instalação; Os serviços de manutenção e suporte deverão ser prestados pelo próprio fabricante do equipamento ou através da proponente;	Conforme Proposta Comercial	N/A	N/A
- PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a “repetição” deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação;	Conforme Proposta Comercial	N/A	N/A
- Deverá informar o site onde se encontra o catálogo para confirmação das características do equipamento.	N/A	N/A	N/A

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 02 - UNIDADE DE DISCO DE 8TB SAS DE 12GB/S	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir formato de 3,5” Hot Swap SATA (HDDs);	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Ter velocidade mínima de 7.200 rpm;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Ter no mínimo interface SAS de 12 Gb/s;	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4
- Possuir no mínimo 8TB de capacidade bruta.	lp1045.pdf	27	7XB7A00045 B0YR ThinkSystem 3.5" 8TB 7.2K SAS 12Gb Hot Swap 512e HDD 4

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 03 - UNIDADE DE DISCO DE 12TB SAS DE 12GB/S	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir formato de 3,5” Hot Swap SATA (HDDs);	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Ter velocidade mínima de 7.200 rpm;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Ter no mínimo interface SAS de 12 Gb/s;	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD
- Possuir no mínimo 12TB de capacidade bruta.	lp1045.pdf	27	7XB7A00067 B117 ThinkSystem 3.5" 12TB 7.2K SAS 12Gb Hot Swap 512e HDD

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 04 - FONTE DE ALIMENTAÇÃO (110/220) DE 750W	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Possuir LED indicador de status e suportar uma faixa de tensão de entrada de 100 a 127 VAC e 200 a 240 VAC em 60 Hz, com chaveamento automático de voltagem;	lp1045.pdf maintenance_manual.pdf	35 21	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply The following illustration shows the LEDs on the rear view of server models with three PCIe slots. The LEDs on the rear view of server models with two PCIe slots are the same.
- Ter recurso de troca sem interrupção;	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply
- Possuir, no mínimo 750 W de potência e certificação 80+ Platinum comprovada mediante publicação no site www.plugloadsolutions.com/80pluspowersupplies.aspx.	lp1045.pdf	35	ThinkSystem 750W (230/115V) Platinum Hot-Swap Power Supply

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 05 - UNIDADE DE MEMÓRIA DE 16GB DDR4 DE 2666MHZ	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Ser compatível com o equipamento descrito no item 1;	lp1045.pdf	19	ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM
- Possuir o mesmo nível de suporte e garantia;	Conforme Proposta Comercial	N/A	N/A
- Ser, no mínimo, memória RAM do tipo RDIMM DDR4 (Registered DIMM DDR4) com ECC (Error Checkin and Correction) ou tecnologia equivalente e que opere em frequência igual ou superior a 2666MHz.	lp1045.pdf	19	ThinkSystem 16GB TruDDR4 2666 MHz (2Rx8 1.2V) RDIMM

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 06 - RACK DE TORRE FECHADO	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Largura: 600 mm;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT
- Altura: 42US;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT
- Profundidade: 1070 mm;	Rack Servidor 42U 2mm.pdf	2	RACK SERVIDOR DESMONTÁVEL 19" X 42U 800X1100 mm PT
- Deve atender as especificações ANSI/EIA RS-310-E;	Rack Servidor 42U 2mm.pdf	1	Atende especificações ANSI/EIA RS-310-D, I EC 297-2, DIN 41494 partes 1 e 7;
- O equipamento deve ser totalmente desmontável para facilitar a montagem e o transporte (deverá ser entregue montado);	Rack Servidor 42U 2mm.pdf	1	Rack totalmente desmontável;
- A estrutura deve ser em aço SAE 1010/1020 # 2 mm;	Rack Servidor 42U 2mm.pdf	1	Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável;
- Deve possuir porta frontal curva em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°;	Rack Servidor 42U 2mm.pdf	1	Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável;
- Deve possuir porta traseira bipartida em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°;	Rack Servidor 42U 2mm.pdf	1	Porta traseira bipartida perfurada com índice de ventilação de 71%, em aço SAE 1010/1020 1,2 mm, reversíveis em relação ao lado de abertura da porta e intercambiáveis, possibilitando a instalação em ambas a faces do rack (traseira ou frontal), fechadura escamoteável;
- Ambas as portas devem possuir fechaduras escamoteáveis com sistema automático de destrave; - Deve ser fornecido com tampas laterais em aço SAE 1010/1020 # 1,2 mm, removíveis através de fechos rápidos, com opção para colocação de fechadura;	Rack Servidor 42U 2mm.pdf	1	• Porta frontal com perfil curvo perfurada, com índice de ventilação de 71%, reversível, com moldura, em aço SAE 1010/1020 1,2 mm, com ângulo de abertura de 220°, fechadura escamoteável; • Porta traseira bipartida perfurada com índice de ventilação de 71%, em aço SAE 1010/1020 1,2 mm, reversíveis em relação ao lado de abertura da porta e intercambiáveis, possibilitando a instalação em ambas a faces do rack (traseira ou frontal), fechadura escamoteável;
- O teto deve estar preparado para instalação de kit de ventiladores, tipo bandeja;	Rack Servidor 42U 2mm.pdf	1	Laterais em aço 1,2 mm, removíveis, com fecho rápido (Opcional fechadura do tipo cilíndrico);
- Deve possuir planos de montagem frontal e traseiro, galvanizados, anti-estáticos e numerados de 1 a 44 US;	Rack Servidor 42U 2mm.pdf	2	Teto em aço SAE 1010/1020 # 1,2 mm, com perfuração tipo colmeia, preparado para instalação de unidade de ventilação;
- Deve possuir2 guias de cabos verticais em aço SAE 1010/1020 # 1,0 mm, com anéis internos em termoplástico de alto impacto, nas dimensões de 44U x 95 mm x 70 mm (A x L x P), sendo fixadas na parte frontal do Rack;	Rack Servidor 42U 2mm.pdf	2	Planos em aço SAE 1010/1020 # 2 mm, galvanizados e anti-estáticos;
- O teto e a base do Rack deve ter abertura para entrada e saída de cabos, e tampas removíveis;	CatlogoIPMetal.pdf	10	GUIA VERTICAL 44U X 90 X 70 MM
- A estrutura do Rack deve possuir terminais de aterramento;	Rack Servidor 42U 2mm.pdf	1	Entrada e saída de cabos pelo teto ou pela base com tampa modular fechada com parafusos, para que quando não utilizada, não haja ingresso de objetos indesejados no interior do rack;
- Deve ser fornecido com pés niveladores e rodízios, sendo 2 com travas e 2 sem travas;	Rack Servidor 42U 2mm.pdf	1	Fornecido com terminais de aterramento;
- Deve suportar uma carga estática até 800 kg;	Rack Servidor 42U 2mm.pdf	1	• Base em aço SAE 1010/1020 # 1,2 mm, preparada para a instalação de rodízios e pés niveladores simultâneos;
- O Rack deve possuir pintura micro epóxi na cor preta;	Rack Servidor 42U 2mm.pdf	1	Suporte de carga estática para até 800 kg;
- Deverá vir acompanhado:	Rack Servidor 42U 2mm.pdf	1	Pintura pó em micro epóxi na cor preta RAL 9004;
- Duas Réguas de tomadas 19” de 12 posições 20ª;	Conforme Proposta Comercial	N/A	N/A
- Uma Bandeja Fixa, Instalada e Fixada nos Trilhos Frontais e Traseiros do	Conforme Proposta Comercial	N/A	N/A
- Rack;	Conforme Proposta Comercial	N/A	N/A

- Um kit de Ventilação contendo 2 Ventiladores Exaustores com 1U de tamanho	Conforme Proposta Comercial	N/A	N/A
- 127/220v, instalado e Fixando no Rack na Parte Superior;	Conforme Proposta Comercial	N/A	N/A
- Três Patch Pannel 1U, com 24 portas com conectores fêmea RJ45 CAT 5e;	Conforme Proposta Comercial	N/A	N/A
- Três guia de cabos;	Conforme Proposta Comercial	N/A	N/A
- Garantia mínima de 12 meses.	Conforme Proposta Comercial	N/A	N/A
	Conforme Proposta Comercial	N/A	N/A

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 07 - RACK TELECOM DE PAREDE	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Rack de parede 19” x 12U;	Rack Parede 12U 600mm.pdf	1	Altura de 12U – 634 mm;
- 600mm de largura e profundidade de 600mm (mínimo)	Rack Parede 12U 600mm.pdf	1	
- Atender especificações ANSI/EIA RS-310-D, IEC 297-2;	Rack Parede 12U 600mm.pdf	1	Atende especificações ANSI/EIA RS 310-D, IEC 297-2, DIN 41494 partes 1 e 7;
- Porta frontal reversível em vidro temperado, com fechadura tipo cilindro;	Rack Parede 12U 600mm.pdf	1	Porta frontal reversível, com moldura em aço 0,9 mm de espessura, com visor de vidro temperado 4 mm, com ângulo de abertura de 180°, fechadura tipo cilindro com fechadura simples;
- Confeccionado em aço SAE 1020;	Rack Parede 12U 600mm.pdf	1	Fabricado em aço SAE 1020;
- Estrutura em aço 1.5 mm;	Rack Parede 12U 600mm.pdf	1	Estrutura em aço 1,5 mm de espessura, com terminais de aterramento;
- Capacidade de carga estática de 60kg;	Rack Parede 12U 600mm.pdf	1	Capacidade de carga estática até 60 kg;
- Laterais com fecho rápido com a opção de utilização de chaves nas laterais;	Rack Parede 12U 600mm.pdf	1	Laterais removíveis, com fecho rápido;
- Entrada e saída de cabos pelo teto ou pela base do rack com acabamento de proteção;	Rack Parede 12U 600mm.pdf	1	Entrada e saída de cabos pelo teto, com furações oblongadas;
- Teto com preparação para instalação de ventiladores;	Rack Parede 12U 600mm.pdf	1	Teto preparado para instalação de ventiladores;
- Terminal de aterramento;	Rack Parede 12U 600mm.pdf	1	Estrutura em aço 1,5 mm de espessura, com terminais de aterramento;
- Deverá vir acompanhado:	N/A	N/A	N/A
- Régua de tomadas 19” de 6 posições 20A;	Conforme Proposta Comercial	N/A	N/A
- Um Patch Pannel 1U, com 24 portas com conectores fêmea RJ45 CAT 5e;	Conforme Proposta Comercial	N/A	N/A
- Um guia de cabos;	Conforme Proposta Comercial	N/A	N/A
- Dezesseis conjuntos de Porca-Gaiola para fixação de Acessórios e Ativos.	Conforme Proposta Comercial	N/A	N/A
- Garantia mínima de 12 meses.	Conforme Proposta Comercial	N/A	N/A

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 08 - PONTO DE ACESSO WI-FI COM PoE	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- Equipamento de ponto de acesso para WLAN, de uso interno (indoor), atendendo aos padrões IEEE 802.11b, IEEE 802.11g, 802.11n, 802.11ac com configuração via software.	UniFi_AC_APs_DS.pdf	10	Wi-Fi Standards 802.11 a/b/g/n/r/k/v/ac
- Deve possuir pelo menos dois rádios, permitindo simultaneamente, usuários configurados nos padrões IEEE 802.11b/g/n, na faixa de frequência de 2.4GHz e 802.11n/ac, na faixa de frequência de 5GHz.	UniFi_AP-AC-Pro_QSG.pdf	26	2G Data Rate Control Select this option to determine what bit rates your 2 4 GHz network will allow Disabling lower bit rates can improve performance for higherdensity networks but will make some older devices incompatible with your network and limit the range of your wireless network 5G Data Rate Control Select this option to determine what bit rates your network will allow Disabling lower bit rates can improve performance for higherdensity networks but will make some older devices incompatible with your network and limit the range of your wireless network
- Deve implementar funcionamento em modo de gerenciamento centralizado pela SOLUÇÃO CENTRALIZADA, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF e outras funcionalidades deSolução Centralizadaritas nesta especificação.	UniFi_AP-Pro_UG.pdf	8	The UniFi Controller software that comes with your UniFi AP-Pro has a browser-based interface for easy configuration and management.
- O ponto de acesso poderá estar diretamente ou remotamente conectado à Solução Centralizada da WLAN, inclusive via roteamento da camada de rede OSI.	UniFi_Controller_V5_UG.pdf	1	Network Topology Requirements • A DHCP-enabled network (so any device can obtain an IP address) • One of the following: • UniFi Cloud Key • A management station running the UniFi Controller software, located either on-site and connected to the same Layer-2 network, or off-site* in a cloud or NOC • For the public address system capability of the UAP-AC-EDU: A compatible Android™ or iOS device located on the same Layer-2 network as the UniFi Controller and UniFi APs
- Possibilitar alimentação elétrica local entre 100V e 230V, em corrente alternada e frequência de 60hz.	PoE_Adapters_DS.pdf	8	U-POE-af 100-240VAC @ 50/60Hz

- Permitir a alimentação elétrica via Power over Ethernet (padrões IEEE 802.3af ou 802.3at) através de uma única interface de rede.	UniFi_AC_APs_DS.pdf	10	Power Method Passive Power over Ethernet (48V), 802.3af/802.3at Supported (Supported Voltage Range: 44 to 57VDC)
- Deve ser fornecido com o adaptador que permita a alimentação via Power over Ethernet (PoE).	UniFi_AP-AC-Pro_QSG.pdf	2	Package Contents
- Implementar as seguintes taxas de transmissão e com fallback automático, valores mínimos:	UniFi_AC_APs_DS.pdf	10	Supported Data Rates (Mbps)
- 802.11b - 1, 2, 5.5, 11 Mbps	UniFi_AC_APs_DS.pdf	10	802.11b 1, 2, 5.5, 11 Mbps
- 802.11g - 6, 9, 12, 18, 24, 36, 48, 54 Mbps	UniFi_AC_APs_DS.pdf	10	802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 802.11n - 6.5 Mbps a 450 Mbps (MCS0 - MCS23, HT 20/40)	UniFi_AC_APs_DS.pdf	10	802.11n 6.5 Mbps to 450 Mbps (MCS0 - MCS23, HT 20/40)
- 802.11ac - 6.5 Mbps a 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)	UniFi_AC_APs_DS.pdf	10	802.11ac 6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)
- Implementar o protocolo de enlace CSMA/CA para acesso ao meio de transmissão.	UniFi_AC_APs_DS.pdf	10	Standard Data Rates 802.11ac 6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80) 802.11n 6.5 Mbps to 450 Mbps (MCS0 - MCS23, HT 20/40) 802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b 1, 2, 5.5, 11 Mbps
- Possuir capacidade de selecionar automaticamente o canal de transmissão.	UniFi - RF Scan Suggested Channels Feature – Ubiquiti Support and Help Center.pdf	1 e 2	The WiFi spectrum must be scanned, manually analyzed, and a channel plan created. Suggested Channels does this automatically: after an RF scan has been triggered, the best channel found will be selected and automatically set, based on how busy the channel is, the RSSI of the channel, and whether or not the same SSID is already transmitting on that channel.
- Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.	UniFi_Controller_V5_UG.pdf	135	Transmit Power By default the transmit power is set to Auto You can also manually select the following:
- Possuir suporte a pelo menos 4 SSIDs.	UniFi_AC_APs_DS.pdf	10	BSSID Up to 8 per Radio
- Implementar diferentes tipos de combinações de criptografia/autenticação por SSID.	UniFi_Controller_V5_UG.pdf	23	Create Wireless Network Click to add a wireless network Go to the Create or Edit a Wireless Network section WPA-Personal WPA or Wi-Fi Protected Access was developed as an encryption method stronger than WEP WPA-Personal requires a passphrase to connect to the wireless network
- Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras.	UniFi_AC_APs_DS.pdf	10	WMM Voice, Video, Best Effort, and Background
- Não deve haver licença restringindo o número de usuários por ponto de acesso.	UniFi_AC_APs_DS.pdf	10	Concurrent Clients 250+

- Suportar mínimo 200 clientes conectados por ponto de acesso no modo concorrente.	UniFi_AC_APs_DS.pdf	10	Concurrent Clients 250+
- Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11b/g/n/ac com ganho de pelo menos 3 dBi, com padrão de irradiação omnidirecional multi-banda dipolar, integral e dual mínimo 3X3 MIMO com diversidade espacial.	UniFi_AC_APs_DS.pdf	10	Antennas (3) Dual-Band Antennas, 2.4 GHz: 3 dBi, 5 GHz: 3 dBi
- Possuir potência máxima de transmissão de, no mínimo, 22 dBm para IEEE 802.11b/g/n/ac.	UniFi_AC_APs_DS.pdf	10	Maximum TX Power 2.4 GHz 22 dBm 5 GHz 22 dBm
- Implementar a pilha de protocolos TCP/IP.	UniFi_Controller_V5_UG.pdf	1 15	Network Topology Requirements • A DHCP-enabled network (so any device can obtain na IP address) Launch Using Cloud If cloud access is available, then you can use it to access the UniFi Controller Click the appropriate option: Launch using Cloud, Launch using hostname of your Controller, or Launch using IP of your Controller For cloud access, these are the requirements: • Ports 443 (TCP), 3478 (UDP), and 443 (UDP) must be open
- Implementar VLANs conforme padrão IEEE 802.1q.	UniFi_AC_APs_DS.pdf	10	VLAN 802.1Q
- Possuir, no mínimo, duas interfaces IEEE 802.3 10/100/1000 BaseT Ethernet, auto-sensing, autoMDI/MDX, com conectores RJ-45, para conexão à rede local fixa.	UniFi_AC_APs_DS.pdf	10	Networking Interface (2) 10/100/1000 Ethernet Ports
- Implementar o protocolo NTP ou SNTP.	UniFi - Explaining the config.properties File – Ubiquiti Support and Help Center.pdf	4	To change the default NTP server being used, config.ntp_server=0.ubnt.pool.ntp.org
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.	UniFi_AP-AC-Pro_QSG.pdf	5	Hardware Overview LED
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.	UniFi - UniFi Overview – Ubiquiti Support and Help Center.pdf	5	SNMP v1/2c/3
- Possuir suporte a MIB II, conforme RFC 1213.	UniFi - UniFi Overview – Ubiquiti Support and Help Center.pdf	5	SNMP v1/2c/3
- Implementar cliente DHCP, para configuração automática de rede.	UniFi_Controller_V5_UG.pdf	7	Network Topology Requirements • A DHCP-enabled network (for the wired Access Point to obtain an IP address as well as for the wireless Access Points after the deployment)
- Possuir LED's indicativos do estado de operação e atividade dos rádios.	UniFi_AP-AC-Pro_QSG.pdf	5	Hardware Overview LED
- Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação.	UniFi_AC_APs_DS.pdf	10	Mounting Wall/Ceiling (Kits Included)
- Implementar associação dinâmica de regras de acesso e de QoS por usuário, com base nos parâmetros da etapa de autenticação.	UniFi_AC_APs_DS.pdf	10	Advanced QoS Per-User Rate Limiting

- Possibilitar roaming layer 2 (modelo OSI) com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VOIP, streaming de vídeo, videoconferência.	UniFi - Fast Roaming – Ubiquiti Support and Help Center.pdf	1	As wireless devices improve in power and portability, exceptional on-the-go performance is expected from devices such as tablets, cell phones, and mobile VoIP.
- Implementar criptografia do tráfego local.	UniFi_AC_APs_DS.pdf	10	Wireless Security WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
- Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.	UniFi_Controller_V5_UG.pdf	23	WPA-Personal WPA or Wi-Fi Protected Access was developed as an encryption method stronger than WEP WPA-Personal requires a passphrase to connect to the wireless network
- Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento.	Conforme Proposta Comercial	N/A	N/A
- A solução ofertada deve possuir homologação junto à ANATEL conforme a resolução nº 242, de 30 de novembro de 2000. A exigência de certificação de Produtos de Telecomunicação classificáveis nas Categorias I, II e III do art. 4o da Resolução Anatel 242/2000 é pré-requisito obrigatório para fins de comercialização e utilização no país, para atendimento ao disposto no parágrafo único do art. 20 da Resolução 242 da Anatel. Todas as certificações necessárias devem estar disponíveis publicamente nos sítio eletrônico da agência reguladora conforme endereço eletrônico http://sistemas.anatel.gov.br/sgch/	5ae31c1bbfc33.pdf	1	Modelo - Nome Comercial (s): UAP-AC-PRO (*) - (UAP-AC-PRO (*))

ITENS PARA COMPROVAÇÃO	DOCUMENTAÇÃO	PÁGINA DO DOCUMENTO	TRECHO
ITEM 09 - BATERIA DE NOBREAK - REPOSIÇÃO	N/A	N/A	N/A
Especificações mínimas:	N/A	N/A	N/A
- VRLA (Chumbo Ácida Selada Regulada por Válvula	1555958987folder-UNIPOWER_2019_web.pdf	2	A linha excede todos os requisitos da ANATEL, atestando o desempenho excepcional das baterias UNIPOWER® VRLA certificado pelo CPqD.
- Vida útil: 02 anos.	1555958987folder-UNIPOWER_2019_web.pdf	2	As baterias UNIPOWER® têm capacidade extra para suportar condições extremas de descarga em aplicações cíclicas ou em flutuação, sendo consideradas baterias de alta integridade, com vida útil projetada para mais de 10 anos, Certificado ANATEL 570.
- Tensão Nominal: 12V.	1555958987folder-UNIPOWER_2019_web.pdf	2	UP1270 E
- Capacidade C20: 7AH.	1555958987folder-UNIPOWER_2019_web.pdf	2	UP1270 E
- Terminal: tipo Faston 187 - Posição D.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Tipo Terminal Faston 187
- Temperatura: +15ºC a 50ºC.	ManualTecnicoBateriaUnipower.pdf	6	Armazenagem A bateria quando armazenada completamente descarregada por um longo período sofre o processo de “sulfatação”. Quanto mais avançado o grau de “sulfatação” da bateria menor é a capacidade de armazenar energia da bateria.Atabela abaixo mostra o tempo máximo de armazenagem em diferentes temperaturas ambientes.
- Dimensões aproximadas do produto: 15,1 x 6,5 x 10,0cm.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Comprimento Largura Altura
- Peso aproximado do produto: 1,860Kg.	Bateria Estacionária VRLA 12V 7Ah Mod.UP1270E UNIPOWER.pdf	2	Peso (kg)
- Garantia do fornecedor: 12 meses.	Conforme Proposta Comercial	N/A	N/A
- Tecnologia AGM com eletrôlito absorvido.	1555958987folder-UNIPOWER_2019_web.pdf	1	Eletrólito Absorvido em Manta de Fibra de Vidro (AGM) Baixa resistência interna e maior eficiência em altas correntes de descargas. Por que escolher as baterias VRLA UNIPOWER®? UNIPOWER®, marca comercial da UNICOBA Baterias, está presente no mercado desde 1978 e conquistou a liderança absoluta em baterias seladas VRLA com produtos de alta qualidade, tecnologia de ponta e portfólio incomparáve
- Livre de Manutenção.	Conforme Proposta Comercial	N/A	N/A
- Vaso em resina ABS especial com elevada resistência mecânica.	1555958987folder-UNIPOWER_2019_web.pdf	1	CAIXA EM ABS Mais robustez, maior proteção para os componentes internos
- Atende o guia EUROBAT.	Conforme Proposta Comercial	N/A	N/A
- São seguras para o transporte aéreo (IATA-A67).	Conforme Proposta Comercial	N/A	N/A

CATÁLOGO



IP METAL®

IP METAL®

Composta por uma equipe de profissionais capacitados e estrutura fabril de última geração, a IP METAL chega ao mercado preparada para superar as expectativas.

Aliado a um design inovador e um acabamento diferenciado, a IP METAL apresenta ao mercado produtos com características modernas para o seu projeto. Seu portfólio conta com uma linha completa de Gabinetes de Parede, Gabinetes de Cabeamento, Gabinetes para Servidores, Gabinetes Abertos de Alta Densidade (HD) e acessórios.

Sua linha de produtos espelha o seu comprometimento com o constante desenvolvimento e aprimoramento, típicos da infraestrutura de TI. Além disso, todos os produtos foram planejados com estrutura desmontável, pensando na facilidade e redução de custo em armazenamento e frete. Considerando a crescente dos problemas ambientais, a IP METAL exerce um papel fundamental ao investir continuamente em práticas sustentáveis em seu processo de produção visando o respeito ambiental.

Esta é a IP METAL, uma indústria que além de disponibilizar produtos de qualidade superior, compromete-se com questões relacionadas ao bem-estar social.



RACK 19” PARA CABEAMENTO ESTRUTURADO DESMONTÁVEL

Os Racks para cabeamento estruturado IP METAL, além de desmontáveis, foram desenvolvidos para acomodação de uma grande quantidade de cabos, com opção de aberturas para passagem de cabos para o teto e base do rack.



CARACTERÍSTICAS:

- Totalmente desmontável
- Atende especificações ANSI/EIA RS-310-D, IEC 297-2, DIN41494 partes 1 e 7
- Grau de proteção IP20
- Estrutura em aço com 1,50 mm
- Fornecido com terminais de aterramento
- Porta frontal reversível em vidro temperado, com ângulo de abertura de 220° e fechadura tipo cilindro
- Porta traseira reversível em aço, com ângulo de abertura de 220° e fechadura tipo cilindro
- Laterais em aço, com fecho rápido
- Planos (frontal e traseiro) com numeração de Us
- Entrada e saída de cabos pelo teto ou pela base
- Teto com preparação para instalação de ventiladores
- Acompanha um conjunto com quatro pés niveladores
- Pintura pó em micro epóxi na cor preta RAL 9004

** Acompanha um par de guias de cabo verticais para os modelos de 800 mm de largura (Ver tabela)

OPCIONAIS:

- Fechadura tipo cilindro para tampas laterais;
- Kit rodizio de fácil instalação

Fabricação	Altura	Largura	Profundidade	Carga	Cor
2002060600	20U (1076 mm)	600 mm	600 mm	800 kg	Preto
2002060800	20U (1076 mm)	600 mm	800 mm	800 kg	Preto
2002460600	24U (1254 mm)	600 mm	600 mm	800 kg	Preto
2002460800	24U (1254 mm)	600 mm	800 mm	800 kg	Preto
2002860600	28U (1432 mm)	600 mm	600 mm	800 kg	Preto
2002860800	28U (1432 mm)	600 mm	800 mm	800 kg	Preto
2003260600	32U (1610 mm)	600 mm	600 mm	800 kg	Preto
2003260800	32U (1610 mm)	600 mm	800 mm	800 kg	Preto
2003660600	36U (1788 mm)	600 mm	600 mm	800 kg	Preto
2003660800	36U (1788 mm)	600 mm	800 mm	800 kg	Preto
2004060600	40U (1966 mm)	600 mm	600 mm	800 kg	Preto
2004060800	40U (1966 mm)	600 mm	800 mm	800 kg	Preto
2004460600	44U (2144 mm)	600 mm	600 mm	800 kg	Preto
2004460800	44U (2144 mm)	600 mm	800 mm	800 kg	Preto
2004480800	44U (2144 mm)	800 mm	800 mm	800 kg	Preto