Lenovo XClarity Integrator for VMware vCenter Installation and User Guide

Version 8.4.0

Note

Before using this information and the product it supports, read the information in .

Contents

Figures

Tables

About this publication

This book provides instructions for installing and using Lenovo XClarity Integrator for VMware vCenter, *Version 8.4.0*.

These instructions include information about how to use the features to acquire system information, update firmware, monitor power usage, configure system settings, and create migration rules for the virtual machine in the VMware vCenter management environment.

Conventions and terminology

Paragraphs that start with a bold **Note**, **Important**, or **Attention** are notices with specific meanings that highlight key information.

Note: These notices provide important tips, guidance, or advice.

Important: These notices provide information or advice that might help you avoid inconvenient or difficult situations.

Attention: These notices indicate possible damage to programs, devices, or data. An attention notice appears before the instruction or situation in which damage can occur.

The following table describes some of the terms, acronyms, and abbreviations used in this document.

Table 1. Frequently used terms and acronyms

Term/Acronym	Definition
BMC	baseboard management controller
LXCA	Lenovo XClarity Administrator
LXCI	Lenovo XClarity Integrator
PFA	predictive failure alert
UXSP	UpdateXpress System Packs

Web resources

The following Web sites provide resources for understanding, using, and troubleshooting System x, Flex System, BladeCenter servers, and systems-management tools.

Lenovo XClarity Integrator for VMware vCenter site

Locate the latest downloads for the Lenovo XClarity Integrator for VMware vCenter:
- Lenovo XClarity Integrator for VMware Web site

System Management with Lenovo XClarity Solutions

This Web site provides an overview of the Lenovo XClarity solutions that integrate System x and Flex System hardware to provide system management capability:
- System Management with Lenovo XClarity Solution Web site

Lenovo technical support portal

This Web site can assist users in locating support for hardware and software:

- Lenovo Support Portal Web site

ServerProven Web sites

The following Web sites provide an overview of hardware compatibility for BladeCenter, Flex System, System x, and xSeries ® hardware:
- Lenovo ServerProven: Compatibility for BladeCenter products
- Lenovo ServerProven: Compatibility for Flex System Chassis
- Lenovo ServerProven: Compatibility for System x hardware, applications, and middleware

VMware Web site

This Web site can assist users in locating VMware products:
- VMware Web site

Chapter 1. Lenovo XClarity Integrator for VMware vCenter

Lenovo XClarity Integrator for VMware vCenter is an extension to LXCI for VMware vCenter and provides system administrators with enhanced management capabilities for System x servers, BladeCenter servers and Flex System servers. Lenovo XClarity Integrator for VMware vCenter expands the management capabilities of VMware vCenter by integrating Lenovo hardware management functionality.

Lenovo XClarity Integrator for VMware vCenter provides the following features.

Dashboard
> The Dashboard provides:
> - Overview of a selected host and cluster status, including a system information summary and system health messages.
> - Summary information, including overall resource usage, host health messages, and connection status.
> - BMC information for each host and allows users to launch the BMC console directly.

Firmware Updates
> The Firmware Updates function acquires and applies Lenovo UpdateXpress System Packs (UXSPs) and individual updates to an ESXi system. The Rolling System Update function provides nondisruptive system updates with zero downtime, automates the update process of the hosts in a cluster environment without any workload interruption, and supports updating multiple hosts concurrently to save time.

Power Metric
> Power Metric monitors and provides a summary of power usage, thermal history, and fan speed, in addition to a trend chart for the managed host. Users can also set the power capping for a power-capping capable host to limit the server power usage.

Advanced Settings Utility
> ASU manages the current system settings on the host, including the BMC, Unified Extensible Firmware Interface (UEFI), and boot order settings.

Predictive failure management
> Predictive failure management monitors the server hardware status and receives predictive failure alerts. Users can set a management policy for a server based on a predictive failure alert to either automatically evacuate virtual machines in response to predictive failure alerts to protect users' workloads or notify users. Predictive failure management is manually enabled or disabled on a host.

Rolling System Update function
> The Rolling System Update (RSU) function updates the firmware in a single batch while the system continues running without interruption to application services on a server host. The RSU function provides an approach of non-disruptive firmware updates. It enables full management of firmware by leveraging dynamic virtual machine movement and automatic host restart within a defined VMware cluster without any workload interruption.

Rolling System Reboot
> The Rolling System Reboot (RSR) function provides an automatic rolling restart mechanism by leveraging dynamic virtual machine movement and automatic host restart within a defined VMware cluster without any workload interruption.

Hardware topology view for ThinkAgile VX appliance servers
> The hardware topology function provides an embedded graphical view for ThinkAgile VX appliance servers. It displays server layout, detailed hardware inventory, and health information, and provides guided wizard to manage the vSAN disks.

Lenovo XClarity Administrator Integration

Lenovo XClarity Integrator integrates with Lenovo XClarity Administrator to provide a convenient method of automating Lenovo server discovery, visualizing inventory map view of managed servers, configuring servers with configuration patterns, and orchestrating rolling firmware policy deployment.

vSphere Lifecycle Manager (vLCM) integration

Lenovo XClarity Integrator integrates with vSphere Lifecycle Manager (vLCM), which is introduced in vSphere 7.0, to provide a convenient method of orchestrating firmware updates through a defined cluster-wide image.

Chapter 2. Planning and installing LXCI for VMware vCenter

Use this procedure to plan for and install Lenovo XClarity Integrator for VMware vCenter.

System requirements

This section describes system requirements for Lenovo XClarity Integrator for VMware vCenter.

Supported versions of VMware vCenter Server

Lenovo XClarity Integrator for VMware vCenter is an extension to VMware vCenter Server.

Starting from version 6.0.0, Lenovo XClarity Integrator supports only VMware vCenter 6.5 (U2) and later versions, and can only be accessed through the vSphere HTML client. The vSphere Flex client is no longer supported.

Depending on the VMware vCenter version and the vSphere client being used, select the right Lenovo XClarity Integrator version according to the following matrix:

Table 2. VMware vCenter version support matrix

VMware vCenter version	Lenovo XClarity Integrator version		
	5.5.0 (Support Flex client only)	7.7.0 (Support HTML client only)	8.4.0
8.0 (U1, U2)	X	X	√
8.0 GA	X	X	√
7.0 (U3)	X	√	√
7.0 (U1, U2)	X	√	X
7.0 GA	X	√	X
6.7 (U1, U2, U3)	√	√	X
6.5 (U2, U3)	√	√	X
6.5 (U1)	√	X	X
6.5	√	X	X
6.0 and earlier versions	√	X	X

Notes:
- If the version of the target VMware vCenter is earlier than 6.5 (U2) or if users are intended to use LXCI with the vSphere Flex client, do not upgrade LXCI to version 6.0.0.
- If the version of the target VMware vCenter is earlier than 7.0 (U1), do not upgrade LXCI to version 8.0.0.

Supported versions of Lenovo XClarity Administrator

Table 3. Lenovo XClarity Administrator version support matrix

LXCA	LXCI version								
	7.4.0	7.5.0	7.6.0	7.7.0	8.0.0	8.1.0	8.2.0	8.3.0	8.4.0
4.0	X	X	X	X	X	√	√	√	√
3.6	X	X	√	√	√	√	√	√	√
3.5	X	√	√	√	√	√	√	√	√
3.4	√	√	√	√	√	X	X	X	X

Supported ESXi version

Lenovo XClarity Integrator for VMware vCenter supports both Lenovo VMware vSphere Hypervisor (ESXi) custom image and VMware ESXi standard image. The following versions are supported.
- 8.0
- 7.0
- 6.7
- 6.5
- 6.0

Users can download Lenovo customized ESXi images from the VMWare product download Web site: https://my.vmware.com/web/vmware/downloads. Locate VMware vSphere and click the **Download Product** link. Then click the **Custom ISOs** tab to locate the Lenovo custom image for ESXi.

Supported server models

This topic provides information about supported server models for Lenovo XClarity Integrator for VMware vCenter.

The XClarity Integrator plug-in has no server model limitations. However, the hardware that the plug-in manages is limited to the Lenovo server models listed in the following table.

Table 4. Supported Lenovo servers

Series	Server models	
ThinkSystem	- SD530 (7X20, 7X21, 7X22) - SD630 V2 (7D1K) - SE350 (7Z46, 7D1X) - SN550 (7X16) - SN550 V2 (7Z69) - SN850 (7X15) - SR150 (7Y54) (China only) - SR158 (7Y55) - SR250 (7Y51, 7Y52) (worldwide except India) - SR250 (7Y72, 7Y73) (India only) - SR250 V2 (7D7Q, 7D7R, 7D7S) - SR258 (7Y53) - SR530 (7X07, 7X08) - SR550 (7X03, 7X04) - SR570 (7Y02, 7X03) - SR590 (7X98, 7X99) - SR630 (7X01, 7X02) - SR630 V2 (7Z70, 7Z71) - SR630 V3 (7D72, 7D73, 7D74) - SR635 (7Y98, 7Y99) - SR635 V3 (7D9G, 7D9H) - SR645 (7D2X, 7D2Y) - SR645 V3 (7D9C, 7D9D)	- SR650 (7X05, 7X06) - SR650 V2 (7Z72, 7Z73) - SR650 V3 (7D75, 7D76, 7D77) - SR655 (7Y00, 7Z01) - SR655 V3 (7D9E, 7D9F) - SR665 (7D2V, 7D2W) - SR665 V3 (7D9A, 7D9B) - SR670 V2 (7Z22, 7Z23) - SR675 V3 (7D9Q, 7D9R) - SR850 (7X18, 7X19) - SR850 V2 (7D31,7D32,7D33) - SR850 V3 (7D96, 7D97, 7D98) - SR850P (7D2F, 7D2G, 7D2H) - SR860 (7X69, 7X70) - SR860 V2 (7Z59, 7Z60, 7D42) - SR860 V3 (7D93, 7D94, 7D95) - SR950 (7X11, 7X12, 7X13) - ST250 (7Y45, 7Y46) - ST250 V2 (7D8F, 7D8G, 7D8H) - ST258(7Y47) - ST550 (7X09, 7X10) - ST558 (7Y15, 7Y16) (China only) - ST650 V2 (7Z74, 7Z75, 7Z76) - ST650 V3 (7D7A, 7D7B)	
ThinkServer	- SR588 V2 (7D53) - SR590 V2 (7D53)	- SR660 V2 (7D6L) - SR668 V2 (7D6L)	
ThinkEdge	- SE350 V2 (7DA9) - SE360 V2 (7DAM)	- SE450 (7D8T) - SE455 V3 (7DBY)	
Solutions	- ThinkAgile HX Series Appliance (7D20, 7D2T, 7D1Z, 7X82, 7X83, 7X84, 7Y95, 7Z08, 7Z29, 7Z44, 8689, 8693, 8695, 5462) - ThinkAgile HX Series Certified Node (7D20, 7D29, 7Y88, 7Y89, 7Y90, 7Y96, 7Z03, 7Z04, 7Z05, 7Z09, 7Z45) - ThinkAgile VX Integrated System (7D43, 7D6X, 7D6W, 7D82, 7D9K, 7D9L, 7D9V, 7D9W)	- ThinkAgile VX Series Appliance (7Y11, 7Y12, 7Y13, 7Y14, 7Y91, 7Y92, 7Y93, 7Y94, 7Z13, 7Z58, 7Z62, 7Z63) - ThinkAgile VX Series Certified Node (7D6W, 7D6X, 7D9L, 7D9K, 7D9V, 7D9W, 7Y92, 7Y93, 7Y94, 7Z12, 7Z58, 7Z63, 7DDK)	
System x	- nx360 M5 (5465) - nx360 M5 DWC (5467, 5468, 5469) - x240 Compute Node (7162, 2588) - x240 M5 Compute Node (2591, 9532) - x280, x480, x880 X6 Compute Node (7196, 4258) - x440 Compute Node (7167, 2590) - x3250 M6 (3633)	- x3500 M5 (5464) - x3550 M4 (7914) - x3550 M5 (5463) - x3630 M4 (7158) - x3650 M4 (7915) - x3650 M5 (5462, 8871) - x3750 M4 (8753) - x3850 X6/x3950 X6 (6241)	

Table 4. Supported Lenovo servers (continued)

Series	Server models	
Legacy ThinkServer	• RD350 • RD450 • RD550 • RD650	• RS160 • SD350 (5493) • TD350 • TS460

Notes:
- Only the following servers are supported by vSphere Lifecycle Manager:
  - Lenovo ThinkAgile VX Series Appliance
  - Lenovo ThinkAgile VX Series Certified Node
  - Lenovo ThinkAgile VX Integrated System
  - Lenovo ThinkSystem SD630 V2, SE350, SR630, SR630 V2, SR630 V3, SR645, SR645 V3, SR650, SR650 V2, SR650 V3, SR665, SR665 V3, SR850P, and SR950.
- Only the following servers are supported for Hardware Topology:
  - Lenovo ThinkAgile VX Series Appliance:
    - 7D82: ThinkAgile VX2375/VX3375/VX7375-N Appliance
    - 7Y93: ThinkAgile VX2320/VX3320/VX7320-N Appliance
    - 7Y94: ThinkAgile VX3520-G/VX5520/VX7520 Appliance
    - 7Z62: ThinkAgile VX2330/VX3330/VX7330-N Appliance
    - 7Z63: ThinkAgile VX3530-G/VX5530/VX7530 Appliance
  - ThinkAgile VX Integrated System:
    - 7D43: ThinkAgile VX3575-G/VX5575/VX7575 Integrated System
    - 7D6X: Lenovo ThinkAgile VX630 V3 IS
    - 7D6W: Lenovo ThinkAgile VX650 V3/VX650 V3-DPU IS
    - 7D9K: Lenovo ThinkAgile VX645 V3 IS
    - 7D9L: Lenovo ThinkAgile VX665 V3 IS
    - 7D9V: Lenovo ThinkAgile VX635 V3 IS
    - 7D9W: Lenovo ThinkAgile VX655 V3 IS
- The ThinkServer servers support only inventory, monitoring, and rolling restart, and some inventory information will be displayed as "NA".
- For ThinkServer SR588 V2/SR590 V2 (7D53), BMC version should be 5.30 or later.
- For ThinkServer SR660 V2/SR668 V2 (7D6L), BMC version should be 5.33 or later.

Table 5. Supported IBM servers

Series	Server models	
System x	• dx360 M2 (7321, 7323) • dx360 M3 (6391) • dx360 M4 (7912, 7913, 7918, 7919) • HS22 (7870, 7809, 1911, 1936) • HS22V (7871, 1949) • HS23 (7875, 1882, 1929) • HS23E (8038, 8039) • HX5 (7872, 7873, 1909, 1910) • nx360 M4 (5455) • Smart Analytics System (7949) • x220 Compute Node (7906, 2585) • x222 Compute Node (7916) • x240 Compute Node (8956, 8737, 8738, 7863) • x280 X6 Compute Node/x480 X6 Compute Node/x880 Compute Node X6 (4259, 7903) • x440 Compute Node (7917) • x3100 M4 (2582, 2586) • x3100 M5 (5457) • x3200 M2 (4367, 4368) • x3200 M3 (7327, 7328) • x3250 M2 (7657, 4190, 4191, 4194) • x3250 M3 (4251,4252,4261) • x3250 M4 (2583)	• x3250 M5 (5458) • x3300 M4 (7382) • x3400 M2 (7836, 7837) • x3400 M3 (7378, 7379) • x3500 M2 (7839) • x3500 M3 (7380) • x3500 M4 (7383) • x3530 M4 (7160) • x3550 M2 (7946, 4198) • x3550 M3 (7944, 4254) • x3550 M4 (7914) • x3620 M3 (7376) • x3630 M3 (7377) • x3630 M4 (7158, 7518, 7519) • x3650 M2 (7947, 4199) • x3650 M3 (7944, 7945, 4254, 4255, 5454) • x3650 M4 (7915) • x3650 M4 HD (5460) • x3650 M4 BD (5466) • x3750 M4 (8722, 8733) • x3755 M4 (7164) • x3690 X5 (7148, 7149, 7147, 7192) • x3850 X5/x3950 X5 (7145, 7146, 7143, 7191) • x3850 X6/x3950 X6 (3837, 3839)

Notes:
- Firmware updates are not supported on IBM servers.
- Lenovo customized ESXi 6.5 or later is not supported on IBM servers.
- System x3250 M4 (2583) supports only partial functions in the Dashboard and Lenovo Dynamic System Analysis. Update, power, and system configuration functions are not supported.

Hardware requirements

The following table lists minimum and recommended hardware requirements for Lenovo XClarity Integrator for VMware vCenter.

Table 6. Hardware requirements

Component	Minimum	Recommended
Memory	4 GB RAM	8 GB RAM
Disk space	64GB of free hard disk space	128 GB of free hard disk space
Processor	1 processor	2 processors

Note: The Lenovo XClarity Integrator for VMware vCenter virtual appliance is pre-configured with recommended hardware configuration by default.

Network requirements

This section provides the network requirements, including the port, firewall, and proxy requirements.

Port availability

Several ports must be available, depending on how the firewalls are implemented in environment. If the required ports are blocked or used by another process, some Lenovo XClarity Integrator functions might not work.

To determine which ports must be opened based in environment, review the following sections. The tables in these sections include information about how each port is used in XClarity Integrator, the vCenter, the managed device that is affected, the protocol (TCP or UDP), and the direction of traffic flow.

Inbound traffic identifies flows from the managed device or external systems to XClarity Integrator, so ports need to open on the XClarity Integrator appliance. *Outbound* traffic flows from XClarity Integrator to the managed device or external systems.

- "Access to the XClarity Integrator servers" on page 8
- "Access between XClarity Integrator and managed devices" on page 8

Access to the XClarity Integrator servers

If the XClarity Integrator server and all managed devices are behind a firewall, and users are intended to access those devices from a browser that is outside of the firewall, users should ensure that the XClarity Integrator ports are open.

The XClarity Integrator server listens on and responds through the ports that are listed in the following table.

Note: XClarity Integrator is a RESTful application that communicates securely over TCP on port 443.

Table 7. Internet connection requirements

Communication	XClarity Integrator appliance	vCenter	XClarity Administrator [1]	Lenovo services [2]
Outbound (ports open on external systems)	DNS – TCP/UDP on port **53**	HTTPS – TCP on port **443**	HTTPS – TCP on port **443**	HTTPS – TCP on port **443**
Inbound (ports open on XClarity Integrator appliance)	HTTPS – TCP on port **443**	HTTPS – TCP on port **443**	N/A	N/A

1. To register XClarity Administrator to XClarity Integrator, refer to https://sysmgt.lenovofiles.com/help/topic/ com.lenovo.lxca.doc/plan_openports.html.
2. To access to the specific Lenovo service web sites, refer to "Firewall" on page 9.

Access between XClarity Integrator and managed devices

If managed devices (such as compute nodes or rack servers) are behind a firewall and if users are intended to manage those devices from a XClarity Integrator server that is outside of that firewall, users should ensure that all ports involved with communications between XClarity Integrator and the baseboard management controller in each managed device are open.

Note: ICMP protocol also should be permitted between XClarity Integrator and server BMC. Lenovo XClarity Integrator uses ICMP (ping) to check BMC connectivity during firmware updates.

Table 8. Servers and compute nodes

Communication	ThinkSystem and ThinkAgile	System x
Outbound (ports open on external systems)	• SLP – UDP on port **427** • HTTPS – TCP on port **443** • CIM HTTPS – TCP on port **5989** [2] • Firmware updates - TCP on port **6990**[4] • SLP – UDP on port **427**	• HTTPS – TCP on port **443** • IPMI – TCP on port **623** [1] • CIM HTTP – TCP on port **5988**[3] • CIM HTTPS – TCP on port **5989** [3] • Firmware updates - TCP on port **6990** [4]
Inbound (ports open on XClarity Integrator appliance)	• HTTPS – TCP on port **443** • Firmware updates - TCP on port **6990** [4]	• HTTPS – TCP on port **443** • Firmware updates - TCP on port **6990** [4]

1. XClarity Integrator uses this port for server configuration and firmware update.
2. By default, this port is disabled on some new servers. In this case, it is not required to open this port and XClarity Integrator uses REST Over HTTPS for management. It is only required to open this port for the servers managed by XClarity Integrator using CIM.
3. By default, management is performed over secure ports. The non-secure ports are optional.
4. This port is used for connecting to the BMU OS to transfer files and run the update commands.

Firewall

Downloading management server updates and firmware updates requires Internet access. Configure the firewall (if any) in network to enable LXCI management server to perform these operations. If the management server fails to access to the Internet, configure LXCI to use a proxy server.

Ensure that the following FQDN and ports are available on the firewall and allowed in the proxy.

Table 9. Internet connection requirements

DNS name	Ports	Protocols
datacentersupport.lenovo.com	443	https
download.lenovo.com	443	https
filedownload.lenovo.com	443	https
support.lenovo.com	443	https
supportapi.lenovo.com	443	https

Proxy

To set the proxy in vCenter and to use vLCM function to update the firmware, users should allow the connection from vCenter to Lenovo XClarity Integrator (protocol HTTPS, port 443) in the proxy configuration of users' company.

The proxy server should meet the following requirements:
• The proxy server is set up to use basic authentication.
• The proxy server is set up as a non-terminating proxy.
• The proxy server is set up as a forwarding proxy.
• The load balancers are configured to keep sessions with only one proxy server.

Installing Lenovo XClarity Integrator for VMware vCenter

This section describes how to install the Lenovo XClarity Integrator for VMware vCenter virtual appliance.

Note: The Lenovo XClarity Integrator for VMware vCenter virtual appliance can only be installed in VMware ESXi-based environment.

Before you begin

Before installing, ensure that:
- The ESXi host has enough free disk space and memory for the Lenovo XClarity Integrator for VMware vCenter virtual appliance.
- The network is set up to use DHCP or a static IP address.

Procedure

Complete the following steps to install the Lenovo XClarity Integrator for VMware vCenter virtual appliance on an ESXi host from the vSphere Client.

Step 1. Log in to the vSphere Client.

Step 2. Right click the target ESXi host and select **Deploy OVF Template**. The Deploy OVF Template wizard is displayed.

Step 3. On the **Select an OVF template** page, select **URL** or **Local file** as the source location. For the local file, click **Choose Files**, input the OVF file location, and click **Next**.

Step 4. On the **Select a name and folder** page, input a unique name and a target location for the virtual machine and click **Next**.

Step 5. On the **Select a computer resource** page, select the destination computer resource and click **Next**.

Step 6. On the **Review details** page, confirm the details and click **Next**.

Step 7. On the **Select storage** page, select storage for the configuration and disk files and click **Next**.

Step 8. On the **Select networks** page, select the network for the target virtual server and click **Next**.

   Note: Skip the settings displayed in the **IP Allocation Settings** section. The IP allocation settings will be configured in the next step.

Step 9. On the **Customize template** page, configure the network configurations and click **Next**.

Step 10. On the **Ready to Complete** page, check the details and click **Finish**.

Step 11. Turn on the virtual machine. When the virtual machine is turned on, URL for accessing the Lenovo XClarity Integrator appliance administration page is displayed on the VM console.

   For example, the following diagram prompts the URL for managing the appliance:
```
-----------------------------------------
Lenovo XClarity Integrator - Version x.x.x build xxx
-----------------------------------------

Manage the appliance from: https://192.0.2.10/admin

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:ffff:ffff:ffff:ffff:ffff:ffff/64 Scope:Global
          inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link
```

Step 12. Go to the Lenovo XClarity Integrator appliance administration page. For example: `https:// 192.0.2.10/admin`

Step 13. Do the following after a wizard is displayed:

   a. Read and accept the license agreement, and click **Next**.

   b. On the **Network Setting** page, configure the network settings by following the steps in "Configuring network access" on page 54, and click **Next**.

   c. On the **Account Configuration** page, set an administrator account for logging in to the Lenovo XClarity Integrator appliance administration page, and click **Submit**.

Step 14. On the **Lenovo XClarity Integrator appliance administration** login page, input the administrator account created in the wizard, and click **Login**. The **vCenter Connection** page is displayed.

Step 15. On the **vCenter Connection** page, click **Register** to register Lenovo XClarity Integrator to the vCenter servers. For more information, refer to "Configuring vCenter connections" on page 51.

Enabling/disabling vSphere Lifecycle Manager

LXCI acts as the hardware support manager for vSphere Lifecycle Manager (vLCM),and enables vLCM to manage Lenovo ESXi servers with a cluster-wide image consisting of base ESXi, Lenovo drivers addon, and a firmware addon.

Before you begin

Ensure that the target server is supported. For more information about the supported machine types, refer to Table 4 "Supported Lenovo servers" on page 5.

Procedure

Users can enable or disable LXCI as the hardware support manager for vLCM.

On the **vCenter Connection** page, click **Disable** or **Enable** on the **vSphere Lifecycle Manager** column to change the vLCM status for the required server.

For more information about managing firmware updates through vLCM, refer to "Working with the vSphere Lifecycle Manager function" on page 37.

What to do next

Log in and configure Lenovo XClarity Integrator for VMware vCenter (see Chapter 3 "Configuring Lenovo XClarity Integrator" on page 15).

Implementing the high availability for Lenovo XClarity Integrator

To implement the high availability for Lenovo XClarity Integrator, use the vSphere High Availability (HA) function in the ESXi environment. Lenovo XClarity Integrator will be restarted on the alternate host when failing to run on the ESXi host.

Before you begin

Ensure that the vSphere HA Cluster is available. For more information about creating the vSphere HA Cluster, see Creating a vSphere HA Cluster.

Procedure

Complete the following steps to implement the high availability for Lenovo XClarity Integrator:

Step 1. Deploy Lenovo XClarity Integrator in a vSphere HA cluster.

Step 2. Select **Restart VMs**, and configure the host failure responses based on the steps in Respond to Host Failure.

Step 3. Enable VM monitoring based on the steps in Enable VM Monitoring.

Upgrading Lenovo XClarity Integrator for VMware vCenter

Users can upgrade Lenovo XClarity Integrator for VMware vCenter when it is already installed in VMware ESXi-based environments.

Upgrading LXCI for VMware vCenter in VMware ESXi-based environments

This section describes how to update Lenovo XClarity Integrator virtual appliance when it is already installed in an ESXi-based environment.

Before you begin

To perform update, get the update package first. Typically, the update package contains four files:
- **.chg file**. Change history file
- **.tgz file**. Update payload
- **.txt file**. Readme file of the specific update package
- **.xml file**. Metadata about the update

Note: To use Lenovo XClarity Integrator v5.0.2 or v5.1.0, apply the fix patch `lnvgy_sw_lxci_upload_fixpatch_1.0.0_anyos_noarch` before applying the update package. Perform steps 2 - 7 in the following procedure to apply the fix patch. Two messages are displayed with information about plug-in registration; ignore this message. Users can download the patch from the Lenovo XClarity Integrator for VMware Web site.

Procedure

Step 1.   (Optional) De-register Lenovo XClarity Integrator from VMware vCenter.

Step 2.   From the Lenovo XClarity Integrator Web interface, click **Version and upgrade** on the left panel of the page.

Step 3.   Click **Import**. The Import dialog is displayed.

Step 4.   Click **Browse**, select the target files, and click **Open**. The selected files are listed in the Import dialog.

   Note: Ensure that the TXT, CHG, XML, and TGZ files are selected.

Step 5.   Click **Import** to import the selected files.

   Notes:
   - The import process might take several minutes or hours depending on the size of the update package and underlying network. Ensure that the network is connected and wait until the progress bar finishes and the dialog closes.
   - If an `Invalid session` error is displayed, the session expired. Log out of the Lenovo XClarity Integrator Web interface, log in again, and then try the import operation again. Consider placing the update package in a faster network.

Step 6.   After the update package is imported, choose the update package in the table and click **Perform Update**. A prompt dialog is displayed. Read the information carefully

   Notes:
   - Lenovo XClarity Integrator might be restarted to complete the update process. If it is restarted, this configuration connection and all other active jobs are stopped.
   - Users can monitor the update progress from the virtual appliance console in vSphere client or vCenter Web client.

Step 7.   When the appliance console is opened, click **OK** and the update request will be sent to the server. The update progress message is shown on the console. If `update finished` is displayed and no errors are shown on console, the update is successful.

```
-------------------------------------------------------------
Manage the appliance from:  https://10.240.197.36/admin

eth0     Link encap:Ethernet  HWaddr 00:0c:29:4a:d4:5e
         inet addr:10.240.197.36  Bcast:10.240.199.25  Mask:255.255.255.0
         inet6 addr: 2002:96b:c2bb:830:20c:29ff:fe34:d34e/64 Scope:Global
```

```
                    inet6 addr: fe80:20c:39ff:fe3a:d9/64 Scope:Link

          lxci login: starting to extract update package
          extract update package finished
          ===============================Fri Feb 10 17:32:33 CST 2017========================
          start to update...
          Preparing... ##################################################
          uus           warning: /etc/lightpd.conf saved as /etc/lightpd.conf.rpmsave
          ################################################
          Stopping uusserverd
          Starting uusserverd
          Database record of identificationCode:lnvgy_sw_lxci_upatch1.0.0_anyos_noarch
          changed to applied successfully
          update finished...
```

Step 8.   (Optional) Register Lenovo XClarity Integrator to VMware vCenter.

Uninstalling Lenovo XClarity Integrator for VMware vCenter

This section describes how to uninstall Lenovo XClarity Integrator for VMware vCenter.

Procedure

Complete these steps to uninstall Lenovo XClarity Integrator for VMware vCenter.
1. Log in to the **Lenovo XClarity Integrator appliance administration** page.
2. Create a backup of the appliance.
3. Deregister the plug-in from the vCenter. For more information, see "Configuring vCenter connections" on page 51.
4. Turn off the appliance from the vSphere Client and delete it from the inventory.
5. Stop the vSphere Client service.
6. From the vCenter server, remove the `com.lenovo.lxci-*.*` directory under `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`.

   Note: Depending on the vCenter server version, the `/etc/vmware` path might vary.
7. Start the vSphere Client service.

Chapter 3. Configuring Lenovo XClarity Integrator

The topics in this section provide information about configuring the Lenovo XClarity Integrator on the target server.

Discovering and managing the BMC

Users can use Lenovo XClarity Integrator to discover the BMC and associate the BMC to the ESXi host, so as to enable out-of-band (OOB) management for the target servers in the vSphere environment.

Lenovo XClarity Integrator supports two ways to discover and manage the BMC:
• Discover and manage the BMC directly

   Notes: This is not applicable to the following servers:
   – ThinkServer servers
   – ThinkSystem SR635
   – ThinkSystem SR655
• Discover and manage the BMC through Lenovo XClarity Administrator

Note: For the ThinkSystem servers, the CIM service is disabled by default. Depending on the firmware level, LXCI might enable the CIM service to manage the server.

Discovering and managing the BMC directly

Users can discover and manage the BMC directly by providing the BMC address and credential.

Procedure

Step 1.   From the vSphere Client Web page, click the **Menu** drop-down list, and select **Lenovo XClarity Integrator**. The Lenovo XClarity Integrator administration page is displayed.

Step 2.   Click the **Discover servers** section. The server discover page is displayed.
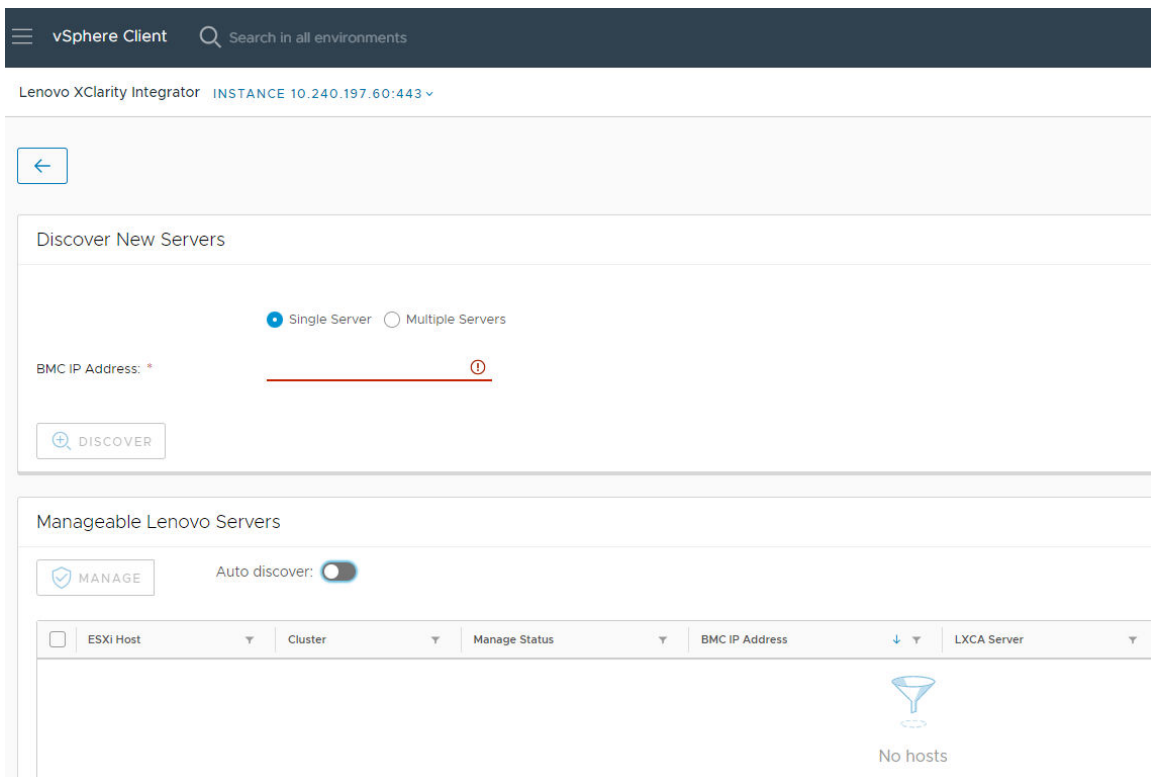
Figure 1. Discovering and managing the BMC

Note: All vCenter-managed ESXi hosts that can be managed but have not been managed by Lenovo XClarity Integrator are listed in the **Manageable Lenovo Servers** section. For the host whose BMC has not been discovered by Lenovo XClarity Integrator, the management status of this host is displayed as "Not Ready" in the **Manage Status** column.

Step 3. In the **Discover New Servers** section, input a single BMC IP address or an IP address range for multiple servers, and click **Discover**.

Notes:
- It is recommended that an IP address range contains less than 60 IP addresses.
- If one BMC is discovered and can be associated with one ESXi host, the BMC IP address will be displayed in the **BMC IP Address** column in the **Manageable Lenovo Servers** table, and the management status of the ESXi host will be changed to **Ready** in the **Manage Status** column.

Step 4. In the Manageable Lenovo Servers area, do one or more of the following:
- To manage the servers, select one or more target servers in the **Ready** status, and click **MANAGE**, input the BMC user name and password on the pop-up window, and click **OK**.

  If the server is managed successfully, a success message is displayed. The management status of the server is changed to **Managing** in the **Manage Status** column and the server is displayed in the **Managed Servers** section.
- To enable or disable the auto discover function, click the toggle icon, and click **YES** to start the process immediately or click **NO** to start the process within 24 hours after the LXCI is enabled.

  Note: SSDP protocol should be enabled before running the auto discover service. The auto discover function, if enabled, will be run once a day.

Discovering and managing the BMC through LXCA

If Lenovo XClarity Administrator is available, and ESXi servers have already been managed by Lenovo XClarity Administrator, users do not need to discover or manage the servers in Lenovo XClarity Integrator. Users can just register the Lenovo XClarity Administrator to Lenovo XClarity Integrator, and Lenovo XClarity Integrator will discover and manage BMC automatically through Lenovo XClarity Administrator. See "Configuring Lenovo XClarity Administrator" on page 17 on how to register Lenovo XClarity Administrator.

Note: When registering LXCA to LXCI, ensure that the LXCA account has the privilege to manage all the target servers managed with LXCI. These servers should be managed by **Managed Authentication** instead of **Local Authenitication** in LXCA. For more information, refer to https://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html.

Configuring Lenovo XClarity Administrator

Lenovo XClarity Integrator provides an integrated method for managing the target servers together with Lenovo XClarity Administrator. After Lenovo XClarity Administrator is registered in Lenovo XClarity Integrator, Lenovo XClarity Integrator can discover and manage servers automatically, and users can manage servers in vSphere Client by using Lenovo XClarity Administrator functions, such as chassis map, configuration pattern, and firmware policy deployment.

Before you begin

Before registering Lenovo XClarity Administrator to Lenovo XClarity Integrator, ensure the following:
- Lenovo XClarity Administrator is working in the current environment.
- The *Lenovo XClarity Integrator Administration* privileges is prepared.

Procedure

Step 1.   On the vSphere Client Web page, click the **Menu** drop-down list box on the top, and select **Lenovo XClarity Integrator**. The Lenovo XClarity Integrator administration page is displayed.

Step 2.   In the **Service Status** section, click **ADD LENOVO XCLARITY ADMINISTRATOR**. The Registration Wizard page is displayed.
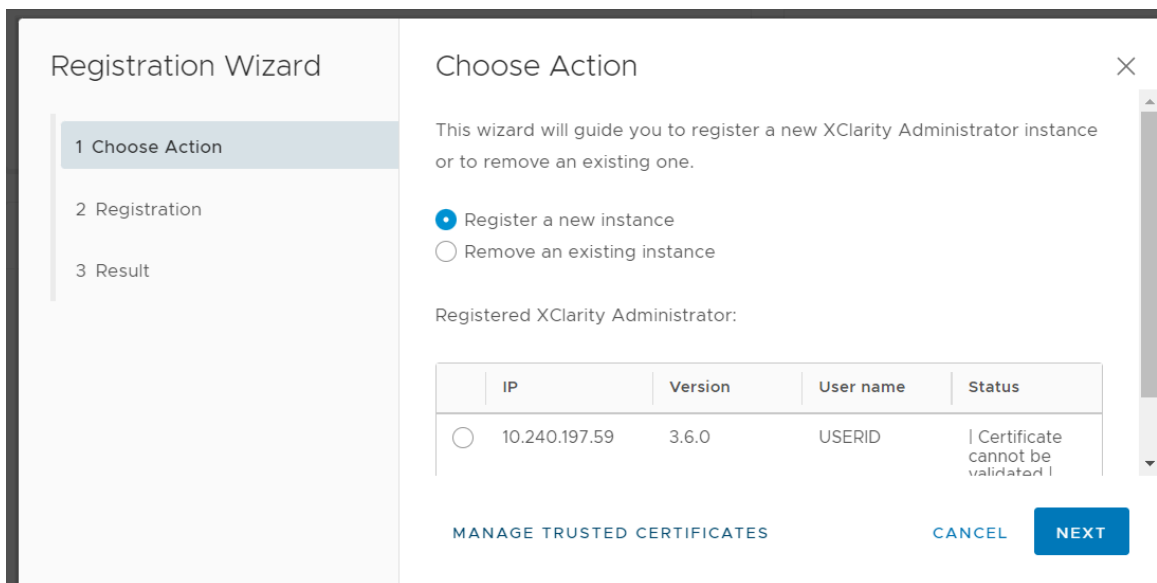

Figure 2. Registration Wizard page

Step 3.   Do one of the following:

- To register a new instance:
  1. On the Choose Action page, select **Register a new instance** and click **NEXT**.
  2. On the Registration page, do one of the following:
     - Select **Use an existing account**, input host name or IP address, user name, and password, and click **NEXT**.

       Notes: Ensure that:
       - This account has the "lxc-supervisor" role group or the combined role groups "lxc-operator, lxc-fw-admin, lxc-hw-admin, and lxc-os-admin".
       - If Resource Access Control is enabled on XClarity Administrator, this account can access the servers .
     - Select **Create a new account by connecting with this administrative account**, input host name or IP address, user name, and password, and click **NEXT**.

       Notes:
       - Ensure that the new account has role groups "lxc-operator, lxc-fw-admin, lxc-hw-admin, and lxc-os-admin".
       - If Resource Access Control is enabled on XClarity Administrator, ensure that this account can access the servers.
       - If LDAP is used in XClarity Administrator or the local account is disabled, do not choose this option.
  3. (Optional) On the View Certificate page, click **NEXT** to accept the certificate.
  4. On the Result page, click **FINISH**.
- To remove an existing instance:
  1. On the Choose Action page, select **Remove an existing instance**, select the target instance from the table, and click **NEXT**.
  2. On the Unregister page, click **NEXT**.
  3. On the Result page, click **FINISH**.
- To manage the trusted certificates:
  1. On the Choose Action page, select **MANAGE TRUSTED CERTIFICATES** to go to the VMware vCenter page.
  2. Follow the steps in "Managing Trusted Certificates" on page 63.

Configuring access control

Lenovo XClarity Integrator supports role-based access.

The following four privileges are defined to control access for different functions:

Privilege	Authorized functions
Inventory	• View the host inventory, events, and utilization information • Launch the BMC interface
Firmware update	Update the firmware
Configuration	Configure system settings and launch the KVM
Administration	Access the LXCI administration page: • Edit the LXCI/vCenter connection • Add the LXCA connection • Discover and manage a server • Disable management over a server

By default, the vCenter administrator role has all privileges defined by Lenovo XClarity Integrator. The vCenter administrator can grant these privileges to other vCenter users if needed.

Importing the Lenovo XClarity Integrator certificate in Web browser

If the certificate that Lenovo XClarity Integrator uses is not signed by a trusted third party, the display page will be blocked when using some functions such as firmware update, chassis map, and system settings. In this case, users should download Lenovo XClarity Integrator root certificate and import it into Web browser list of trusted certificates or add it into security exceptions depending on the working browser.

Procedure
- For Internet Explorer and Chrome:
     1. Log in to the Lenovo XClarity Integrator appliance administration page.
     2. Click **Security Settings**, and then click **Certificate Authority**.
     3. Click **Download Certification Authority Root Certificate** to download the certificate.
     4. Double-click the `downloadded.ca.cer` file.
     5. In the **General** tab, click **Install Certificate**.
     6. Choose **Local Machine** and click **Next**.
     7. From the **Certificate Store** page, select **Place all certificates in the following store**, and click **Browse**.
     8. Select **Trusted Root Certificate Authorities**, and click **OK**.
     9. Click **Finish**.
    10. For the Internet Explorer, close the browser and open it again to make the changes to take effect.
- For Firefox:
     1. In an open browser, click **Firefox ➜ Options ➜ Privacy&Security ➜ Certificates ➜ View Certificates ➜ Servers ➜ Add Exception**.
     2. In the **Location** field, enter the fully qualified domain name or the IP address of the host installed with Lenovo XClarity Integrator.
     3. Click **Get Certificate**.
     4. Click **Confirm Security Exception**, and then refresh the browser.

Chapter 4. Viewing a summary of environment

This section is an introduction of the Lenovo XClarity Integrator dashboard. The Lenovo XClarity Integrator dashboard provides an overview of managed servers, manageable servers, service status, and product information

Procedure

To enter the Lenovo XClarity Integrator dashboard, complete the following steps:
1. From the vSphere Client Web page, click the **Menu** drop-down list box on the top.
2. Select **Lenovo XClarity Integrator**. The Lenovo XClarity Integrator administration page is displayed.

Select one of the following sections on the dashboard:
- **Discover Servers**. Refer to "Discover Servers section" on page 21.
- **Managed Servers**. Refer to "Managed Servers section" on page 21.
- **Service Status**. Refer to "Service Status section" on page 22.
- **Product Information**. Refer to "Product Information section" on page 22.

Discover Servers section

This section enables users to view the amount of manageable Lenovo servers. Users can click **Manageable Lenovo Servers** or **Discover New Servers** to enter the detailed operation pane to perform operations, such as discovering and managing servers.

The **Manageable Lenovo Servers** section provides a table listing the following details of the manageable servers.
- ESXi host
- Cluster
- Manage Status
- BMC IP Address
- LXCA Server
- Model
- Serial Number
- Product Name
- vCenter

Managed Servers section

This section enables users to view the amount of managed Lenovo servers and the amount of virtual machines on these servers grouped by server status. Users can click the amount information to enter the **Managed Servers** operation pane.

The **Managed Servers** operation pane provides a table listing the following details of the manageable servers.
- ESXi host
- Cluster
- Status
- Power
- BMC IP Address
- LXCA Server
- Model
- Serial Number
- vCenter

Do one of the followings:
- To refresh the inventory information of a managed server, click the **REFRESH INVENTORY** button.
- To update the BMC user name and password of a managed server as required, click the **EDIT CREDENTIALS** button.
- To disable management over a managed server, click the **UNMANAGE** button.

    Note: All Lenovo XClarity Integrator functions for this server will be disabled and this server will be displayed in the **Manageable Lenovo Servers** section.

Service Status section

This section displays the status of services that Lenovo XClarity Integrator provides.

Three types of services are available on this section:
- XClarity Integrator Service

    It shows the IP address and status of the Lenovo XClarity Integrator back-end services. Users can click **EDIT** to edit the IP address, user name, and password for connecting to the Lenovo XClarity Integrator services.
- vCenter Server

    It shows the vCenter servers on which XClarity Integrator have been registered. Users can click **EDIT** to enter the Lenovo XClarity Integrator for VMware vCenter administrator Web page. For more information, see "Configuring vCenter connections" on page 51.
- XClarity Administrator

    It shows the XClarity administrators that have been registered in XClarity Integrator. Users can click **EDIT** or **LAUNCH** to edit or launch the XClarity administrators.

Product Information section

This section enables users to view the product information of Lenovo XClarity Integrator.

Users can click the following links to further learn about our products or send feedback to help us do better.
- View Lenovo License Agreement
- View Third Party License
- View Third Party License
- Online Documentation
- Product Web site
- Visit Forum
- Submit idea

Chapter 5. Managing servers

Lenovo XClarity Integrator provides platform management for System x, BladeCenter, and Flex servers. The topics in this section describe how to use Lenovo XClarity Integrator for managing servers.

Verify that these prerequisites have been completed:
- The number of Lenovo servers managed by vCenters registered to the same LXCI instance should not exceed 1,000. Otherwise, users should deploy multiple LXCI instances for these Lenovo servers.
- VMware vCenter Server has an out-of-band (OOB) network connection with the BMC of the managed ESXi servers.
- Users can locate the BMC and have requested access for the BMCs on the **Cluster Overview** page.
- The following servers must be managed by Lenovo XClarity Administrator, and Lenovo XClarity Administrator must be registered in Lenovo XClarity Integrator (see).
  – ThinkServer servers
  – ThinkSystem SR635
  – ThinkSystem SR655

Procedure

Step 1. Select a host from the vCenter host inventory tree.

Step 2. Click the **Monitor** tab.
On the left navigation pane, select one of the following functions under **Lenovo XClarity**:
- System Overview
- Events
- Inventory
- Utilization
- Chassis Map
- Hardware Topology

Step 3. Click the **Configure** tab.
On the left navigation pane, select one of the following functions under **Lenovo XClarity**:
- Firmware Updates
- Power Policy
- Configuration

Step 4. Right-click the host from the vCenter host inventory tree. On the displayed **Actions** drop-down list box, move the cursor onto **Lenovo XClarity**.
Select one of the following functions:
- Launch Remote Console
- Launch BMC Interface

Viewing system information

The System Overview page provides a snapshot view of the current system. Users can view the basic system information such as the machine type, operating system, version, BMC firmware version, and UEFI firmware version. Users can also view the System Hardware Event Summary and collect full diagnostic data.
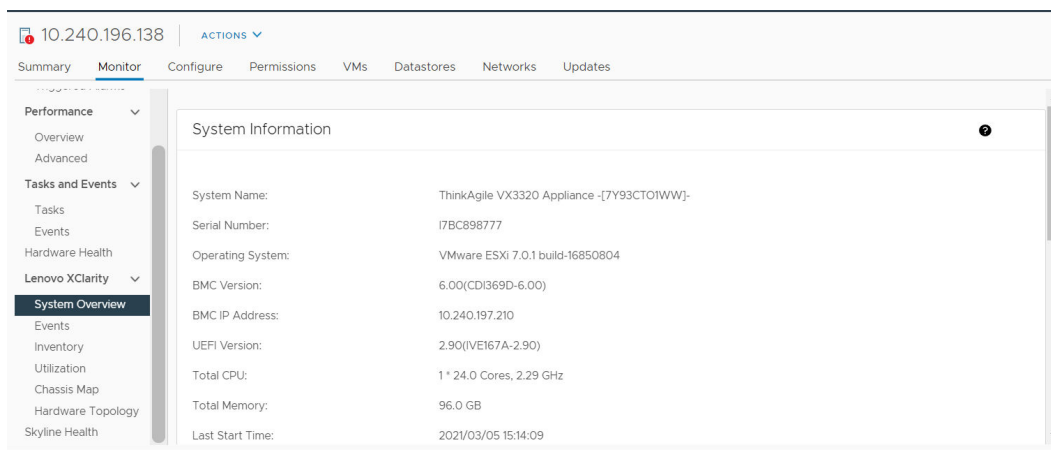
Figure 3. System Overview page

Launching the System Diagnostic Collection function

Procedure

Complete the following steps to collect the full system diagnostic data.

Step 1.   Click **Collect** in the bottom section of the System Overview page.

> **Note:** This collection process takes up to five minutes. When it completes, the last collection time
> is displayed on the **System Overview** page.

Step 2.   Click **Download log** to download the latest system diagnostic data.

Viewing server events

Users can view the hardware event details of the current server.

The following icons indicate the severity of each event.

- : Critical
- : Warning
- : Informational

This page supports the following operations:
- Filtering events by clicking **Type**
- Refreshing events by clicking **Refresh**
- Sorting the system events by clicking the table headings

Viewing the server inventory

The **Inventory** page provides a snapshot view of the current server inventory. Users can view the system
board, microprocessor, memory, fan, sensor, NIC, PCI adapter, and firmware information on this page.

Use **Quick Link** on the right of the page to access the target section. In a specific section, click the + sign to
view the details.
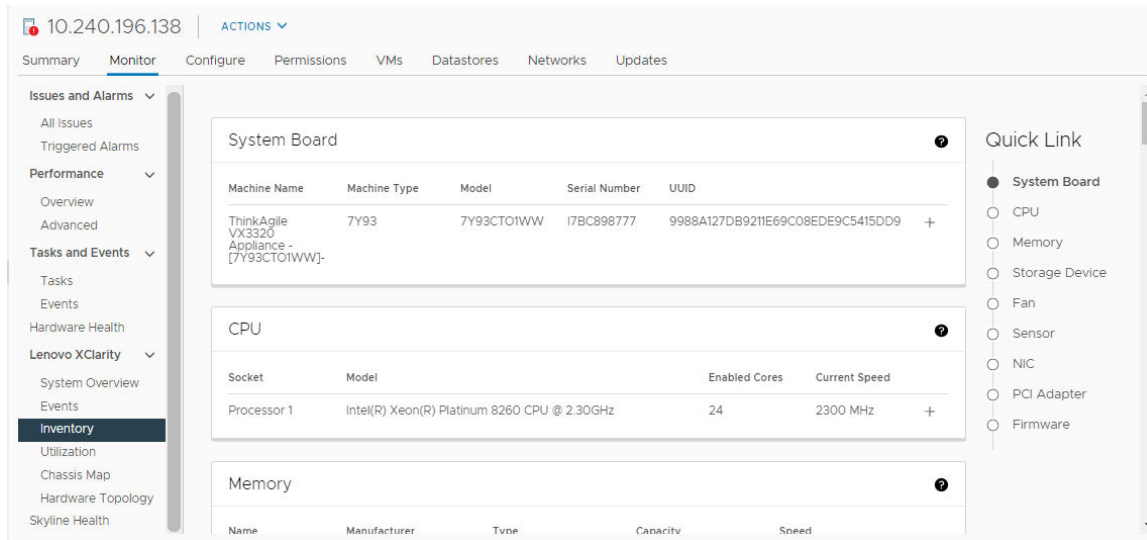
Figure 4. Inventory page

Viewing the server utilization

The **Utilization** page shows latest and history utilization information for ambient temperature, system power input, and fan speed.

To better display the information, this page provides two views for the information: graphic view and table view.

Figure 5. Utilization page

Item	Latest information	History information
Ambient Temperature	Thermometer graph	Line graph/List (Previous 6, 12 or 24 hours)
Power Utilization	Doughnut graph	Line graph/List (Previous 1, 6, 12 or 24 hours)
Fan Speed	List	N/A

Note: **Fan Speed** is only available in **Table View**.

Working with the hardware topology

The hardware topology function provides an embedded graphical view for ThinkAgile VX appliance servers. This interface supports to view server layout, detailed hardware inventory, and health information and manage the vSAN disks.

Host hardware topology

Host hardware topology provides overall information about hosts and enables users to perform the operations on the topology.

Note: Ensure that the host is supported by vCenter. For the hosts not supported by vCenter, users can check and install the hardware definition packages from LXCI or from browser by following the prompts on page.

To access the **Hardware Topology** page, do the following:
1. Select a host from the vCenter host inventory tree and click the **Monitor** tab on the right pane.
2. Click **Hardware Topology** under **Lenovo XClarity**. The Hardware Topology page is displayed.
3. Do one of the following:
   - To view the general host information, refer to "Viewing general host information" on page 26.
   - To view vSAN disk information, refer to "Viewing vSAN disk information" on page 27.
   - To view power supply information, refer to "Viewing health status of power supply units (PSU)" on page 28.
   - To remove a vSAN disk, refer to "Removing a vSAN disk" on page 28.
   - To replace a vSAN dis, refer to "Replacing a vSAN disk" on page 29.

Viewing general host information
The Hardware Topology page supports to view the general information about the host.

General information

On the upper pane of the **Hardware Topology** page, users can view the general information about the host:

- **Machine Name**
- **Machine Type**
- **Front Panel LED**
  - : Power state
  - : Location LED state
  - : Fault LED state.
- **Hardware Health**
  - Normal
  - Warning
  - Critical

Note: To view more information, users can click the expand icon ∨ in the **Hardware Health** column.

Actions

On the right of this pane, users can also click **VIEW ACTIONS** and **HOST ACTIONS**:
- Under **VIEW ACTIONS**:
  - **View Detail Inventory**: Click it to access the **Inventory** page.
  - **View Reference Photo**: Click it to access the product reference page. This page displays the actual front and rear views of this machine and directs users to access the product guide on Lenovo Press.
  - **Refresh Hardware Topology**: Click it to update the hardware topology information.

- Under **HOST ACTIONS**:
  - **Host LED**: Click **Host LED: ON**, **Host LED: OFF**, or **Host LED: BLINK** to change the status of the LED.
  - **Launch BMC Interface**: Click it to access the Lenovo XClarity Controller Web site.
  - **Launch Remote Console**: Click it to access the remote console page of the Lenovo XClarity Controller Web site.

Viewing vSAN disk information

The Hardware Topology page provides a virtual view for the disks installed in actual server slots.

Figure 6. Hardware topology
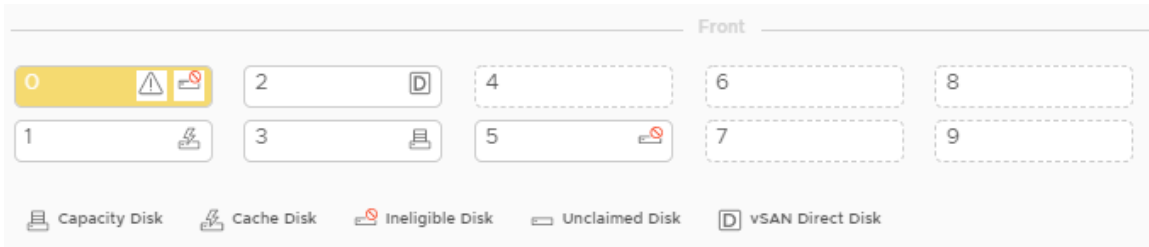
Note: For the server that has rear backplanes, both the **Front** and **Rear** topologies would be displayed.

The hardware topology illustrates:
- Disk location: The slot without any disk installed is displayed with dotted lines.
- Disk status: Different colors indicate different disk status:
  - White: Normal state
  - Yellow: Warning state
  - Red: Critical state
- Disk type: The disk type icons of capacity disk, cache disk, ineligible disk, unclaimed disk, and vSAN direct disk are displayed on the right of each slot.

Users can click one of the disks on the topology:
- If the selected disk belongs to a vSAN group, other disks in the same vSAN group will be highlighted with a solid black line.
- Under **VIEW ACTIONS**:
  - **Show Icons Legend**: This option displays the icons used to represent the disk type of the disks in a topology view, including Cache Disk, Capacity Disk, Ineligible Disk, Unclaimed Disk, vSAN Direct Disk, and Empty Bay. To hide the icon legends, click **Show Icon Legends** again.
  - **Show Disk Groups**: This option adds a new column **Disk Group** in the disk details table and show disk group on the disks in the topology view. To hide disk groups, click **Show Disk Groups** again.
- The selected disk will be highlighted in the below table that lists the detailed physical and logical disk information, including **Bay**, **Drive Type**, **Controller**, **Status**, **Capacity**, and **Media**.
- If users click the Disk Group link in the topology view, all the associated disks of the disk group will be highlighted in the disk table.

Note: Users can click the controller name to view more details.

Figure 7. Controller details
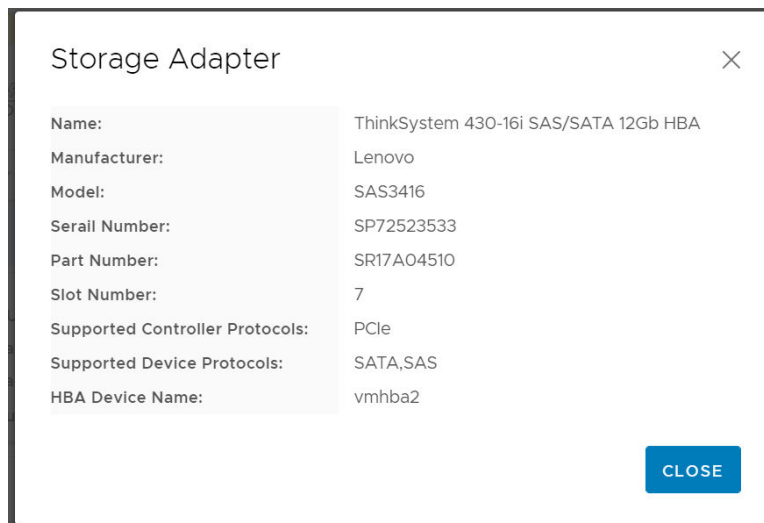
Viewing health status of power supply units (PSU)

The Hardware Topology page provides a virtual view for the health status of power supply units (PSU) installed in the server.
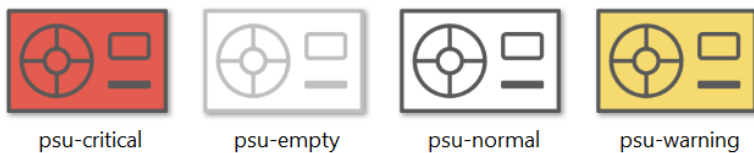
Figure 8. Health status of PSU

Different colors indicate different health status of PSU, including:
- Red: Critical state
- White with light grey line: Empty state
- White with dark grey line: Normal state
- Yellow: Warning state

Removing a vSAN disk

The disk removal option enables users to remove a vSAN disk from the disk group and physically remove it from the disk bay.

Notes:
- Before removing the cache disk, remember to back up the data; otherwise, the working virtual machines might be disrupted.
- If deduplication and compression is enabled on vSAN host, and the cache disk or the last capacity disk is removed from the disk group, the entire disk group will be removed. When necessary, users should re-create the disk group manually.
- After the physical disk is removed from the bay, the disk will be indicated with the dotted lines and its status will be empty.

Procedure

Step 1.   On the hardware topology page, select the target disk from the topology view.

Step 2.   On the right pane, click **DISK ACTIONS ➔ Remove Disk**. The Remove Disk Wizard is displayed.

Step 3.   On the Validation page, the selected disk is highlighted and the related information is displayed.

Step 4. Click **NEXT**. The Migrate Data page is displayed.

Step 5. On the Migrate Data page, from the **vSAN Data Migration** drop-down list, select one of the following desired mode to migrate the disk data:

Table 10. vSAN Data Migration options

	Supported features		
Options	**Pre-check**	**Data migration to other vSAN disks in the same cluster**	**Disk/disk group removal**
No data migration	√		√
Ensure accessibility	√	√	√
Full data migration	√	√	√

Step 6. Click **DO IT NOW** to remove the disk from the disk group.

Step 7. Click **NEXT** after the process is completed. Users will be redirected to the Remove Disk page.

Step 8. On the Remove Disk page, click **Disk LED** or **Host LED** to turn on/off the LEDs on a disk or the host, which enable the remote user to identify the correct disk or host.

Step 9. Click **FINISH** to complete the disk removal process.

Replacing a vSAN disk

Replacing disk option enables users to physically replace the selected disk from the disk group with a new one.

Note: The entire disk group will be rebuilt if the cache disk or the last capacity disk is replaced. Before replacing the cache disk, remember to back up the data; otherwise, the working virtual machines might be disputed.

Procedure

Step 1. On the hardware topology page, select the target disk from the topology view.

Step 2. On the right pane, click **DISK ACTIONS ➙ Replace Disk**. The Replace Disk Wizard is displayed.

Step 3. On the Validation page, the selected disk is highlighted and the related information is displayed.

Step 4. Click **NEXT**. The Migrate Data page is displayed.

Step 5. On the Migrate Data page, from the **vSAN Data Migration** drop-down list, select one of the following desired mode to migrate the disk data:

Table 11. vSAN Data Migration options

	Supported features		
Options	**Pre-check**	**Data migration to other vSAN disks in the same cluster**	**Disk/disk group removal**
No data migration	√		√
Ensure accessibility	√	√	√
Full data migration	√	√	√

Step 6. Click **DO IT NOW** to remove the disk from the disk group.

Step 7. Click **NEXT** after the process is completed. Users will be redirected to the Remove Disk page.

Step 8.   On the Replace Disk page, click **DETECT NEW DISK** after inserting the new disk in the same bay. The page will display the new disk information.

Step 9.   Turn on **Auto Claim New Disk** to add the new disk to the disk group automatically.

Step 10. Click **FINISH** to complete the disk replacement process.

Cluster hardware topology

The cluster hardware topology supports to view the topology of all the hosts of a cluster at one location.

To access the **Hardware Topology** page, do the following:
1. Select a cluster from the vCenter host inventory tree and click the **Monitor** tab on the right pane.
2. Click **Hardware Topology** under **Lenovo XClarity**. The hardware topology view page is displayed. Users can view general information about the cluster.

General information

On the **Hardware Topology** page, users can view the overall hardware health information about the hosts in table.
- **Total**: Displays the number of hosts, disks, or disk groups.
- **Normal** ■ : Displays the number of hosts, disks, or disk groups in normal state.
- **Warning** ⚠ : Displays the number of hosts, disks, or disk groups in warning state.
- **Critical** ⊗ : Displays the number of hosts, disks, or disk groups in critical state.

Actions

The following operations are supported:
- To search a host, input the host name or the IP address in the search box on the top right corner and press **Enter**.
- To view the information of hosts under a cluster, click any number in the **Total/Normal/Warning/Critical** column to expand the topology of each host.
- To view the details of each host, click **HOST DETAILS** on the right of each host topology. Users will be redirected to the respective Host Topology page.
- To view detail inventory, reference photo, or refresh hardware topology, click **VIEW ACTIONS**. For more information, refer to: "Actions" on page 26.
- To change LED status, launch BMC interface, or launch remote contole, click **HOST ACTIONS**. For more information, refer to: "Actions" on page 26.

Launching the BMC Web interface

Users can launch the baseboard management controller (BMC) Web interface for a specific server in Lenovo XClarity Integrator.

Procedure

Complete the following steps to launch the BMC interface for a server.

Step 1.   Right-click a host from the vCenter host inventory tree.
The **Actions** drop-down list box is displayed.

Step 2.   Choose **Lenovo XClarity ➞ Launch BMC Interface**.A confirmation dialog box is displayed.

Step 3.   Click **OK**. The BMC Web interface for the server is displayed.

Step 4.   Use the BMC credential to log in to the BMC interface.

Launching the remote console

Users can launch a remote-control session for a managed server and perform operations on this server like at a local console, such as powering on or off the server and logically mounting a local or remote drive.

Procedure

Complete the following steps to launch the remote console for a managed server.

Step 1. Right-click a host from the vCenter host inventory tree.
The **Actions** drop-down list box is displayed.

Step 2. Choose **Lenovo XClarity ➙ Launch Remote Console**.A confirmation dialog box is displayed.

Step 3. Click **OK** and accept any security warnings displayed on the Web browser. The remote-control session for the server is launched.

Working with the Firmware Updates function

The Firmware Updates function supports to obtain and deploy UpdateXpress System Pack (UXSP) or individual firmware updates to the current working ESXi server.

Updating a single ESXi server is similar with updating servers by using the Rolling System Update function. The only difference is that when an update task is being created, the current ESXi is shown and can be selected. For more information about how to update preferences and manage update tasks, see "Working with the Rolling System Update function" on page 40.

Working with the Power Policy function

The Power Policy function supports to allocate less power and cooling to a system if the firmware supports and enables the Power Capping setting. This function helps to lower datacenter infrastructure costs and potentially allows more servers to be put into an existing infrastructure.

The Power Capping value is the value set for a rack or Blade server that will be capped by the firmware. The Power Capping value is persistent across power cycles for both rack and blade servers. If a Power Capping value is set, the system power consumption will not exceed the defined value.

If the Power Capping is supported and enabled for a server, the minimum and maximum Power Capping values of the server can be retrieved by Lenovo XClarity Integrator and displayed as a power consumption range for the server. In the following example, the minimum value is 0 and the maximum value is 750.
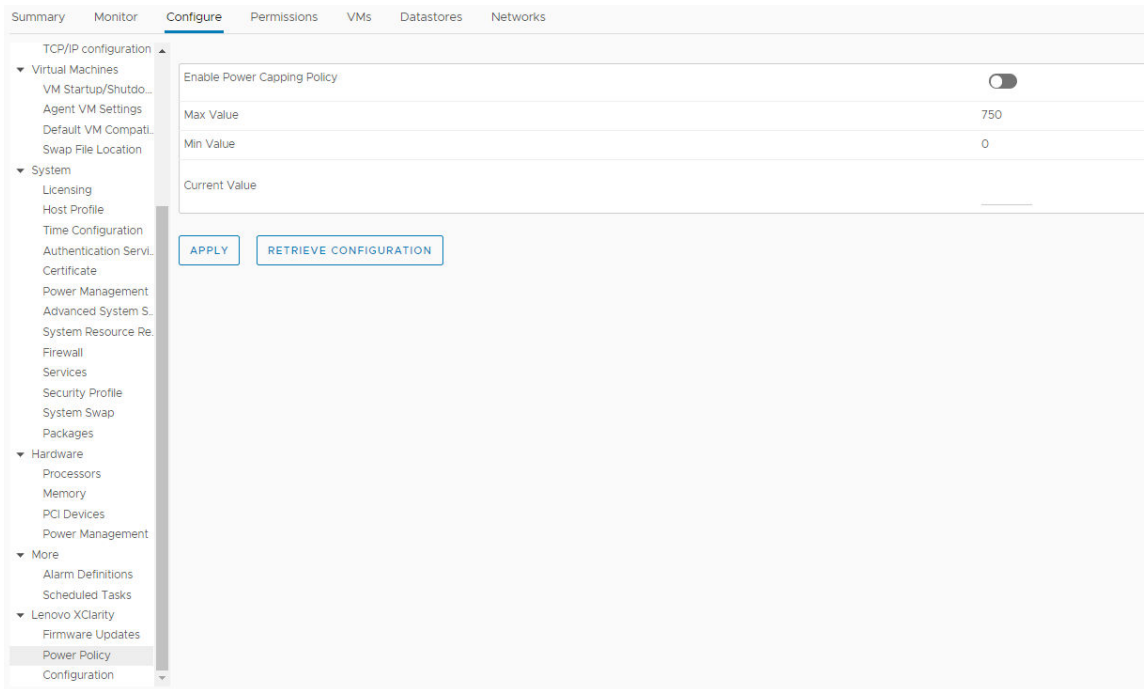
Figure 9. Power Policy configuration page

Working with the System Settings function

The System settings function supports to manage the system settings of a host. If the server is managed by Lenovo XClarity Administrator, and Lenovo XClarity Administrator is registered in this Lenovo XClarity Integrator, users can deploy a configuration pattern to the host; otherwise, users can only view the boot options and system settings for the host.

Deploying a configuration pattern on a server

After Lenovo XClarity Administrator has been registered in Lenovo XClarity Integrator, users can deploy or deactivate a configuration pattern on each supported server that is managed by a Lenovo XClarity Administrator. A server pattern represents a pre-OS server configuration, including local storage configuration, I/O adapter configuration, boot settings, and other BMC and UEFI firmware settings. A server pattern is used as an overall pattern to quickly configure multiple servers simultaneously.

About this task

If Lenovo XClarity Administrator does not have any predefined patterns, users can create server patterns by clicking the link to open Lenovo XClarity Administrator. This task is performed on the **Configuration Pattern** page.
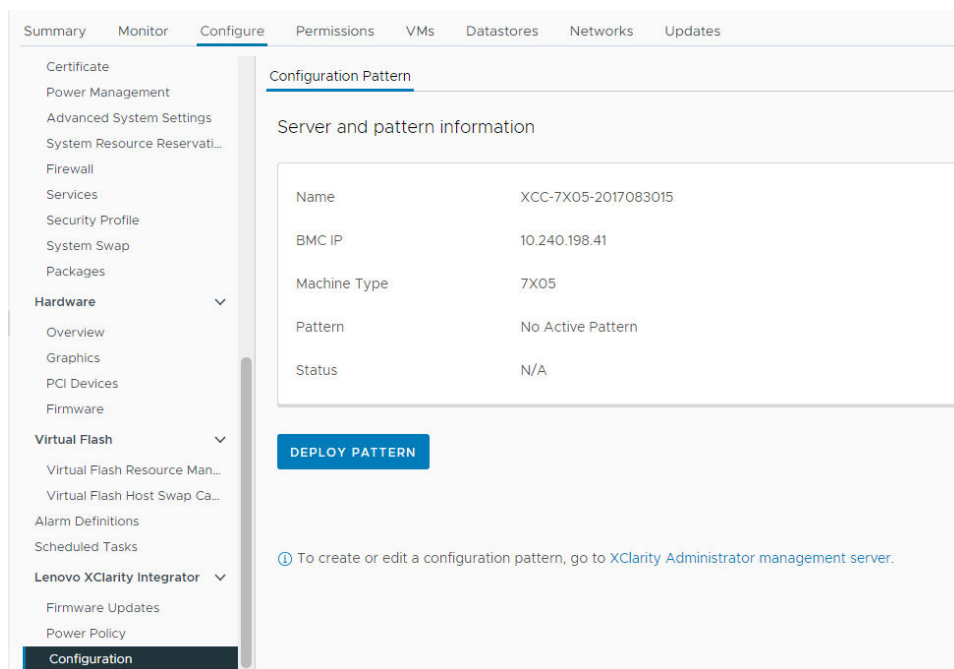
Figure 10. Configuration Pattern page

Procedure

Step 1.   Select the target host and click **Configure ➜ Lenovo XClarity Integrator ➜ Configuration**.

Step 2.   On the **Configuration Pattern** page, select the configuration pattern.
- **DEPLOY PATTERN**. Deploys the selected pattern to the target servers.
- **DEACTIVATE PATTERN**. Deactivates the pattern from the target servers.

Step 3.   On the **Deploy Pattern** page, select the target pattern from the drop-down list, and click **NEXT**.

Step 4.   On the **Confirm Action** page, select the activation time, and click **DONE**.

> **Notes:**
> - **Immediate Activation**. Deploy the pattern and restart the server to make the changes take effect immediately.
> - **Delayed Activation**. Deploy the pattern but do not restart the server. Changes will be effective at the next restart.
> - Depending on the server configuration, the deployment process might take about 30 minutes.

Working with the Boot Options function

On the **Boot Options** pane, the optional devices and the current boot order are displayed from left to right. To change the order, move a boot order option up or down, or click the corresponding arrow buttons between two columns.

A date stamp with the last update date and time is displayed on the right of the **RETRIEVE CONFIGURATION** button. Click **RETRIEVE CONFIGURATION** to get the latest boot option setting values. Click **SAVE** to save the new boot option settings if any changes are made.
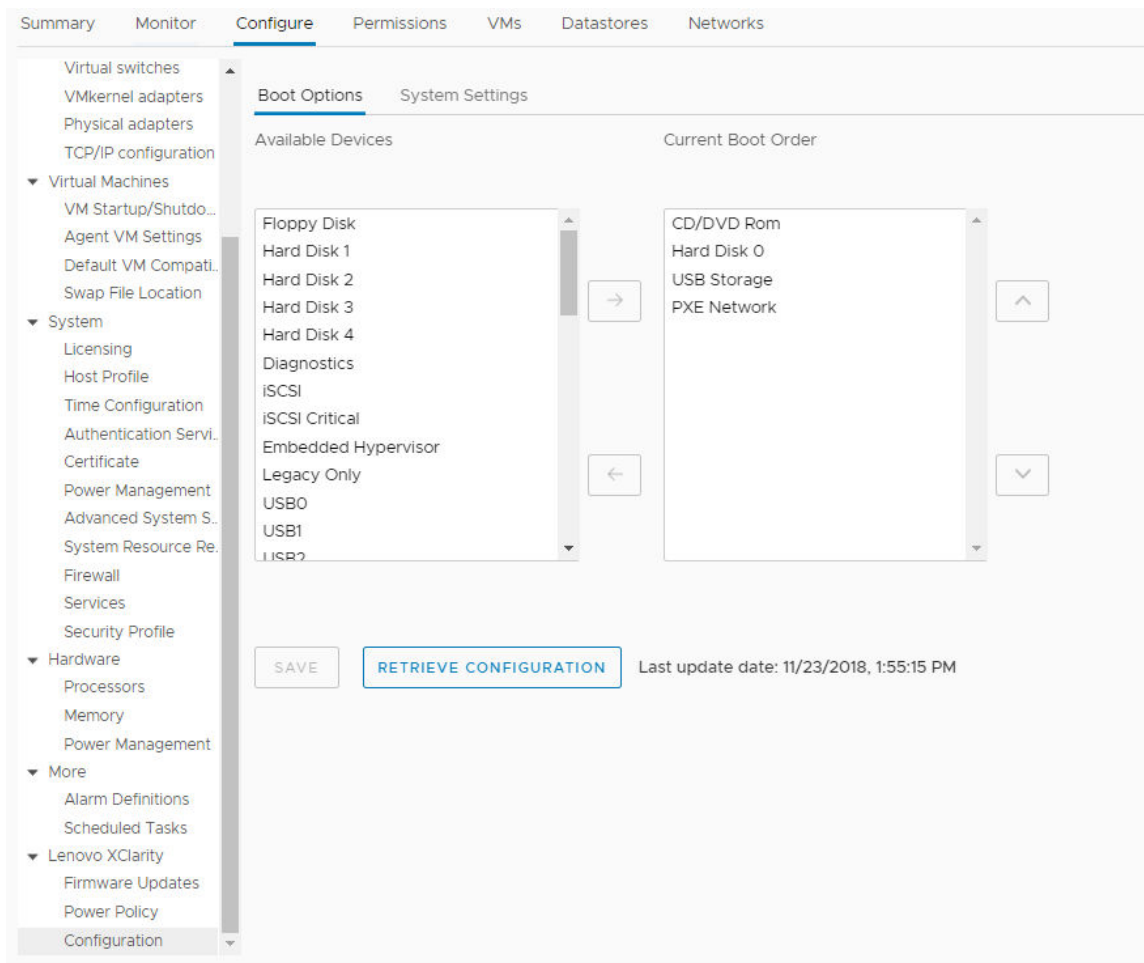
Figure 11. Boot Options pane

Viewing and exporting system settings

Users can view and export the system settings of the ThinkSystem server, Lenovo System x, BladeCenter, or Flex server using the following procedure.

Procedure

Complete the following steps to view and export the system settings:

Step 1.   On the **Configure** pane, click **Configuration** under **Lenovo XClarity**, and then click the **System Settings** tab on the right pane.
On the **System Settings** pane, system settings are listed under the **EXPORT TO CSV** and **RETRIEVE CONFIGURATION** buttons. A date stamp with the last update date and time is displayed on the right of the **RETRIEVE CONFIGURATION** button.
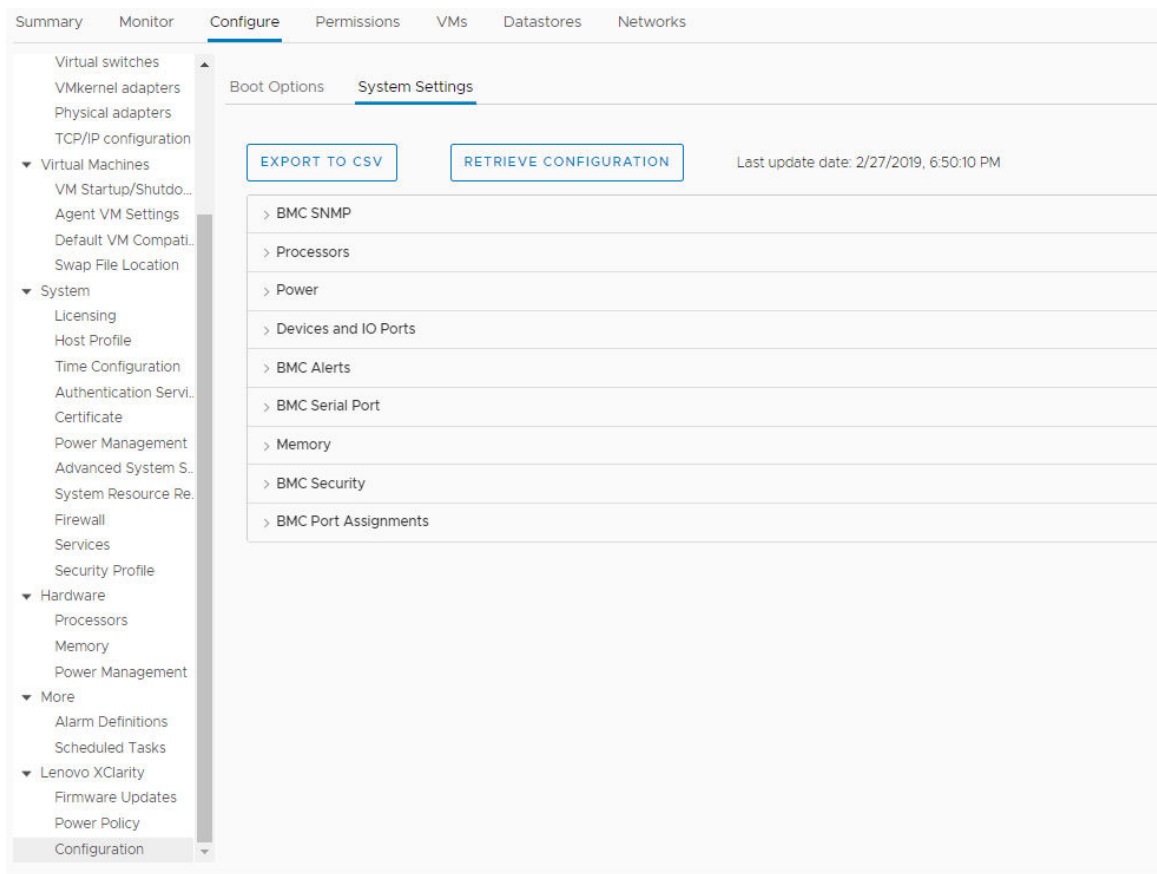
Figure 12. System Settings pane

Step 2. Do one of the followings:
- To get the latest setting values, click **RETRIEVE CONFIGURATION**.
- To export system settings to a CSV file, click **EXPORT TO CSV**.

Chapter 6. Managing clusters

The topics in this section describe how to use Lenovo XClarity Integrator for managing clusters.

Procedure

Complete the following steps to view the Lenovo XClarity Integrator cluster management functions.

Step 1.   Select a cluster from the vCenter inventory tree.

Step 2.   Click the **Configure** tab.
On the left navigation pane, select one of the following functions under **Lenovo XClarity**:
- **Rolling Update**
- **Rolling Reboot**

Working with the vSphere Lifecycle Manager function

When users manage the cluster by using a single image, it is recommended to use the vSphere Lifecycle Manager function.

Before you begin

Ensure that LXCI is enabled as the hardware support manager for vLCM. For more information about enabling vLCM, refer to "Enabling/disabling vSphere Lifecycle Manager" on page 11.

Importing base ESXi and Lenovo addons

Users can import ESXi versions and Lenovo addons to vLCM.

Procedure

Step 1.   Select **Lifecycle Manager** from the **Menu** drop-down list. The **Lifecycle Manager** page is displayed.

Step 2.   On the **Lifecycle Manager** page, select one of the following from the **ACTIONS** drop-down list:
- Select **Sync Updates** to automatically download the standard ESXi and Lenovo customization addons from the online vSphere Lifecycle Manager depot.
- Select **Import Updates** to import Lenovo custom ESXi image into the depot manually. Users can download Lenovo custom ESXi image from https://vmware.lenovo.com/content/custom_iso.

Note: In the **Image Depot** area, users can also select the ESXi version/vendor addons/component to view the detailed information on the right pane.

Managing firmware packages

Users can manage firmware packages on vSphere Client.

Procedure

Step 1.   Select **Lenovo XClarity Integrator** from the **Menu** drop-down list and click **Manage Firmware Packages** on the left pane.

Step 2.   On the right pane, do one or more of the following:
- To stage the firmware or skip to stage the firmware in vLCM operations, enable or disable **Stage Firmware**.

Note: This function is only supported in the ThinkSystem V3 and ThinkAgile V3 servers.

- To manually import the firmware packages, click **IMPORT**. The Import Firmware Package window is displayed.
  1. On the **Remote repository** page, input URL, user name, and password, and click **NEXT**.
  2. On the **Firmware package** page, select the firmware package, and click **FINISH**.
- To download the required firmware package, select the target firmware package from the list, and click **DOWNLOAD**.
- To copy the firmware package for customization, select the target firmware package and click **COPY**.
- To customize the firmware package, select the copied firmware package and click **EDIT**. The Edit Firmware Packages window is displayed.

  Notes:
  – Only the copied firmware packages can be edited.
  – The replaced firmware package might not be validated by Lenovo, which might cause update failure. Therefore, it is not recommended to edit the firmware package.
  1. Select the target firmware package and click **REPLACE**. The Replace Firmware window is displayed.
  2. On the **Remote repository** page, input URL, user name, and password, and click **NEXT**.

     Note: The URL should be the URL of the shared folder containing the CHG/TXT/UXZ/XML firmware files to be imported.
  3. On the **Firmware** page, select the firmware package to be imported, and click **FINISH**. The **Edit Firmware Packages** page is displayed.
  4. On the **Edit Firmware Packages** page, do one or more of the following:
     – To complete the replacement process, click **APPLY ➜ CONFIRM**.
     – To remove the firmware, select the firmware package and click **REMOVE ➜ APPLY ➜ CONFIRM**.
- To delete the firmware package, select the target firmware package and click **DELETE**.
- To import the firmware package list, click **IMPORT LIST**, click the URL to download the file from Lenovo website, click **Choose File** to import the file, and click **IMPORT**.

  Note: Use this option when LXCI is disconnected from Internet.
- To refresh the firmware package list, click **REFRESH LIST**.

  Note: Use this option when LXCI access to Internet.

Managing the cluster through an image

Users can manage the cluster through an image.

Procedure

Step 1. Select **Hosts and Clusters** from the **Menu** drop-down list.

Step 2. Select the required cluster on the left pane, and click **Updates ➜ Image** on the vLCM page.

Creating a cluster image

Users can create a cluster image for the server.

Procedure

Step 1. In the **Image** area, click **EDIT** and do one or more of the following:
- In the **ESXi Version** field, select an ESXi version from the drop-down list.
- In the **Vendor Addon** field, click **SELECT** to select Lenovo addons for ESXi.

- In the **Firmware and Drivers Addon** field, click ✎ to select **Lenovo XClarity Integrator** from the **Select the hardware support manager** drop-down list, and then select a firmware and driver addon in the **Select a firmware and driver addon** table.

  Note: When setting the proxy in vCenter, users should either disable the proxy or allow the connection from vCenter to Lenovo XClarity Integrator (protocol HTTPS, port 443) in the proxy configuration. Otherwise, the firmware and driver addon list will not be displayed.
- In the **Components** field, click **Show details** to add components.

Step 2. Do one of the following after editing the image:
- Click **SAVE** to save the changes.
- Click **VALIDATE** to check the compliance of Lenovo addons for ESXi and firmware addons.
- Click **CANCEL** to discard the changes.

Checking hardware compatibility

Before firmware remediation, check hardware compatibility for a vSAN cluster. This function compares the firmware and drivers displayed in the image against the listed Lenovo hardware and supported drivers in the vSAN Hardware Compatibility List (HCL).

Procedure

Step 1. In the **Image** area, click ⋯ and select **Check hardware compatibility** to compare the firmware and drivers in the cluster image with vSAN Hardware Compatibility List (HCL).

Step 2. Click **See details** to view the comparison results in the **Compatibility check results** area and resolve the potential hardware compatibility issues.

Checking cluster compliance

Users can check the compliance between the existing servers under a cluster and the configured image.

Procedure

Step 1. In the **Image Compliance** area, click **CHECK COMPLIANCE** to check the compliance of ESXi versions, firmware, and drivers between the existing servers under a cluster and the configured image.

Step 2. Check the compliance results on the **Software compliance** table and the **Firmware compliance** table.

Remediating non-compliant servers

User can remediate the ESXi versions, Lenovo addons for ESXi, firmware, and drivers of non-compliant servers under a cluster.

Procedure

Step 1. Click **RUN PRE-CHECK** to check the status of the existing servers.

Step 2. View the results on the Pre-check completed window and resolve the issues.

Step 3. To remediate the ESXi versions, Lenovo addons for ESXi, firmware, and drivers of one or all non-compliant servers under a cluster, do one of the following:
- To perform the remediation for all servers, click **REMEDIATE ALL**
- To perform the remediation for one server, select the target server and click **Actions ➜ Remediate** on the server page.

Staging firmware

User can stage the firmware for non-compliant servers under a cluster.

Note: This function is only supported in the ThinkSystem V3 and ThinkAgile V3 servers whose ESXi version is v8.0 or later.

Procedure

Step 1. Enable **Stage Firmware** on the Manage Firmware Packages page. See "Managing firmware packages" on page 37.

Step 2. Click **STAGE ALL** or **ACTIONS ➔ Stage** to stage the firmware.

Step 3. (Optional) Remediating non-compliant servers. See "Remediating non-compliant servers" on page 39.

Working with the Rolling System Update function

Rolling System Update (RSU) provides a nondisruptive approach to firmware updates. RSU fully manages firmware by orchestrating "rolling" updates, leveraging dynamic virtual machine movement within a defined VMware cluster, completing the whole update process, including ESXi host restart automatically, without any interruption to application services running on the host.

Users can update the firmware by using the Rolling System Update function if the vSphere Lifecycle Manager cannot be used in some scenarios. For example, the cluster is not managed by a single image, or users are intended to upgrade some firmware not in the firmware packages for vLCM.

For more information about updating firmware through vLCM, refer to "Working with the vSphere Lifecycle Manager function" on page 37.

Before you begin

- The following servers are not supported:
  - ThinkServer servers
  - ThinkAgile HX series server
- Ensure that VMware vCenter DRS is enabled and running in fully automated mode.
- Ensure that port 6990 is enabled.

Configuring the Rolling System Update preferences

Users can configure the update repository and download settings for firmware updates on the Preferences pane.

Specify the update repository location

Users can configure the update repository where the Rolling System Update function checks for firmware updates when creating a task of type **Update without Policy**.

Procedure

Step 1. On the left navigation pane, click **Rolling Update** under **Lenovo XClarity Integrator**. Then, click **Preferences** on the right pane.

Step 2. On the Preferences pane, select one of the following ways to specify the firmware repository location.
   - By default, an internal directory on the Lenovo XClarity Integrator appliance server is used as the firmware repository and **Download metadata from Lenovo website** is enabled.
   - To use an external folder as the firmware repository, click **EDIT** on the right in the **Repository folder** section.
       1. In the **Repository Settings** page, select **Use Remote Repository**.
       2. Input the URL of the repository in the format of \\<IP_address>\<repository_path>, and enter the user name and password if required.

3. Click **OK** to save the changes

   Notes:
   – For repository setup on a host using IPv6 addresses, specify the network address using the fully qualified domain name (FQDN).
   – The write permission of the shared folder must be granted.
   – LXCI supports the following types of external folders on the network:
     – Shared folder on a Windows server
     – Shared folder on a Linux Samba file server (with the NTLM security mode)

Step 3. Click **EDIT** on the right of **Download metadata from the Lenovo website** to configure the update package download settings.

a. If the LXCI server cannot access the Internet directly, configure the Internet settings on the Lenovo XClarity Integrator appliance administration page. After logging into the Web page, click **Network Settings** on the left pane and click **Internet Settings** on the right pane. Then, configure the proxy settings.

b. Select **Download from website** and **Periodically download** to set the frequency for automatically and periodically downloading the update packages.

c. Click **OK**

Step 4. (Optional) Click **CHECK NOW** on the bottom right corner of the pane to download the latest update package from the Lenovo Web site.

   Notes:
   • **CHECK NOW** is only available when **Download from website** is selected in the previous step.
   • The time of the latest download is displayed on the bottom left corner of the pane.

Managing Rolling System Update tasks

The Rolling System Update (RSU) function enable users to create and manage rolling system update tasks. An RSU task contains all of the information and options required for a rolling system update.

Procedure

Step 1. Select the target cluster from the inventory tree and click the **Configure** tab.

Step 2. On the left navigation pane, click **Rolling Update** under **Lenovo XClarity Integrator**. The **Rolling Update** page is displayed on the right pane.

The task table provides the following detailed information about an RSU task:
• Task Name
• Type
• State
• Create Time
• Start Time
• End Time

*Table 12. **Rolling System Update** task status*

Target	Status	Description
Rolling Update Task	Not Started	The task has not started.
	Running	The task is running.
	Canceled	The task is canceled.
	Failed	Downloading firmware package failed.
	Finished	The task has completed.

Table 12. Rolling System Update task status (continued)

Target	Status	Description
Host	Not Started	The update for the host has not started.
	Migrating	The host is entering maintenance mode.
	Maintenance	The host is in maintenance mode.
	Updating	The firmware of the host is updating.
	Reboot	The host is restarting after updating completes.
	Exit Maintenance	The host is exiting maintenance mode.
	Success	The firmware update succeeded.
	Failed	The causes of host failure: • Cannot get the update package. • Cannot enter maintenance mode. • Cannot update the firmware. • Cannot restart the host. • Cannot exit maintenance mode.
Firmware	Not Started	The firmware update has not started.
	Running	The firmware update is running.
	Success	The firmware update succeeded.
	Failed	The firmware update failed.

Step 3. Perform one of the following steps:

Table 13. Rolling System Update task functions

Task function	Description
CREATE	Create a new RSU task.
COPY	Create a new RSU task from an existing RSU task.
EDIT	Edit an RSU task that has not been started.
REMOVE	Remove an RSU task from the task list.
CANCEL	Stop a running RSU task.
REFRESH	Refresh the RSU list.

Creating an RSU task

Use the **CREATE** option to create a new Rolling System Update (RSU) task and schedule the host firmware update at a planned time period.

Procedure

Step 1. Select **Configure ➙ Lenovo XClarity Integrator ➙ Rolling Update**, and click **Rolling Update** tab on the top.

Step 2. On the **Rolling Update** page, click **CREATE** to launch the create task wizard.

Step 3. On the **Create Task** page, input the task name, select one to the following task types, and click **NEXT**.
- **Update with a policy from XClarity Administrator**: Select this option to ensure that the firmware on the server are compliant. Before the update, ensured that:
  – Servers running ESXi is added to and managed by Lenovo XClarity Administrator.

- – Firmware-compliance policies are created in Lenovo XClarity Administrator.
- – Firmware are downloaded from Lenovo XClarity Administrator.
- – Lenovo XClarity Administrator is registered in Lenovo XClarity Integrator.
- – If the firmware of one server is updated in other ways instead of Lenovo XClarity Administrator, before creating the rolling update task (with a policy) in vCenter, it is recommended to refresh the inventory information for this server in Lenovo XClarity Administrator.
- **Update without a policy**: If Lenovo XClarity Administrator is not available, select the individual firmware updates or UXSP for each server. Before the update, ensured that:
  - – BMC access is granted.
  - – The update repository is configured, and the firmware are downloaded (see "Configuring the Rolling System Update preferences" on page 40).

Notes:
- Ensure that the target task type meet the requirements before the update.
- Non-ascii characters cannot be used in task name.

Step 4. On the **Select Version** page, select the machine type, host, and policy, and click **NEXT**.

Step 5. On the **Task Options** page, select or toggle one or more of the following options, and click **NEXT**.
- **Reboot after Update**: Specifies whether to restart OS the after updating firmware. This option is mandatory if **Update without a policy** is selected.
- **Number of nodes to be updated in parallel**: Specifies the number of hosts to be updated at the same time. For updating with a policy from LXCA method, the maximum number is 16; for updating without a policy method, the maximum number is eight. One LXCI instance supports to update the firmware in parallel for 32 hosts at most.
- **Allow updating to a firmware version lower than the current version**: Specify whether to allow the firmware version earlier than the current version.
- **Run Memory Test**: Run a memory test once the firmware update is completed after the server is restarted. This option is supported in all ThinkSystem servers except for ThinkSystem SR635, SR645, SR655, and SR665 servers. Users can check the memory test results in the event view of LXCI, or check the job status in LXCA.
- **Perform VM Evacuation**: Specifies whether to migrate the virtual machines before updating the host.
- **Stop the overall task if any node fails**: Specifies whether to stop the whole update task when the update for one host in the cluster fails.
- **Perform the update**: Select the time of performing the update. Select **Now** to perform the update right now, or set the value in **Schedule Time** to perform the update on the schedule time.

Step 6. On the **Confirm** page, confirm the information, and click **FINISH**.

Cloning a completed RSU task

Use the **COPY** option to clone a new Rolling System Update (RSU) task using a task that has a status of finished, failed, or canceled.

Procedure

Step 1. Select **Configure ➙ Lenovo XClarity Integrator ➙ Rolling Update**, and click the **Rolling Update** tab on the top.

Step 2. On the **Rolling Update** page, select a finished, failed or canceled RSU task from the list.

Step 3. Click **COPY** to launch the copy task wizard.

Step 4. Edit the original selection and click **FINISH** to save the new task.

Editing a not-started RSU task

Use the **EDIT** option to edit a not-started Rolling System Update (RSU) task.

Procedure

Step 1.   Select **Configure ➞ Lenovo XClarity Integrator ➞ Rolling Update**.

Step 2.   Select a not-started RSU task in the list and click **EDIT** to launch the create task wizard.

Step 3.   Edit the task and then click **FINISH** to save changes.

Removing an RSU task

Use the **REMOVE** option to remove a Rolling System Update (RSU) task from the task list if it is not currently running. All RSU tasks that are not currently running can be removed.

Procedure

Step 1.   Select **Configure ➞ Lenovo XClarity Integrator ➞ Rolling Update**.

Step 2.   Select one or more RSU tasks that are not currently running from the list.

Step 3.   Click **REMOVE**. The selected tasks are removed from the task list.

Canceling a running RSU task

Use the **CANCEL** option to cancel a Rolling System Update (RSU) task while it is running. When a task is canceled, the task status changes to `Canceling`.

Procedure

Step 1.   Select **Configure ➞ Lenovo XClarity Integrator ➞ Rolling Update**.

Step 2.   Select a running RSU task from the list.

Step 3.   Click **CANCEL**. RSU completes updating the host that has started and only cancels the others. This task may take several minutes to complete.

Refreshing the RSU task list

Use the **REFRESH** option to refresh the Rolling System Update (RSU) task list.

Procedure

Step 1.   Select **Configure ➞ Lenovo XClarity Integrator ➞ Rolling Update**.

Step 2.   Click **REFRESH** to refresh the RSU task list.

Working with the Rolling System Reboot function

The Rolling System Reboot (RSR) function restarts a server while a system continues running without interrupting any running application services by dynamic VM migration.

Before you begin

The following prerequisites are necessary for using the Rolling System Reboot function:
- The following servers are not supported:
  - ThinkAgile HX series server
- VMware vCenter Enterprise or Enterprise Plus Edition with DRS is needed.
- DRS is enabled and running in fully automated mode.

Managing Rolling System Reboot tasks

The Rolling System Reboot (RSR) function supports to create and manage rolling restart tasks. An RSR task contains all of the information and options required for a rolling restart.

Procedure

Step 1. Select the target cluster from the inventory tree and click the **Configure** tab.

Step 2. On the left navigation pane, click **Rolling Reboot** under **Lenovo XClarity Integrator**. The **Rolling Reboot** page is displayed on the right pane.

The task table provides the following detailed information about an RSR task:
- Task Name
- Status
- Progress
- Start Time
- End Time

Step 3. Perform one of the following steps:

Table 14. Rolling System Reboot task functions

Task function	Description
CREATE	Creates a new RSR task.
EDIT	Edit an RSR task that has not been started.
COPY	Create a new RSR task from an existing RSR task.
DELETE	Remove an RSR task from the task list.
CANCEL	Stop a running RSR task.

Creating an RSR task

Use the **CREATE** option to create a new Rolling System Reboot (RSR) task. Each cluster can have only one active RSR task.

Procedure

Step 1. Select **Configure ➙ Lenovo XClarity Integrator ➙ Rolling Reboot**.

Step 2. Click **CREATE** to launch the create task wizard.

Note: The **CREATE** button is enabled only if a task is in the **Finished**, **Canceled**, or **Failed** status in the task list.

Step 3. On the **Select hosts** page, input the task name and select one or more target hosts, and click **NEXT**

Step 4. On the **Reboot options**, select or toggle one or more of the following options, and click **NEXT**.
- **Parallelization**: Specifies the number of hosts that can be restarted concurrently. Rebooting multiple hosts concurrently requires more system resources. It is recommended to set the value according to the current available system resources of the cluster, for example, CPU and memory on the vCenter Server. The default value is 1, and the maximum value is 4.
- **Stop On Error**: Specifies whether to continue update if one host is failed.
- **Recommission Mode**: This option is only visible in the vSAN cluster. Users can specify decommission mode when migrating virtual machines.
- **Schedule**: Specifies a time to initiate the task.

Step 5. On the **Summary** page, confirm the information, and click **FINISH**. RSR will initiate the task according to the schedule.

Editing a not-started RSR task

Use the **EDIT** option to edit a not-started Rolling System Reboot (RSR) task.

Procedure

Step 1. Select **Configure ➙ Lenovo XClarity Integrator ➙ Rolling Reboot**.

Step 2. Select a not-started RSR task in the list and click **EDIT** to launch the create task wizard.

Step 3. Edit the task and then click **FINISH** to save changes.

Cloning a completed RSR task

Use the **COPY** option to clone a new Rolling System Reboot (RSR) task using a task that has a status of finished, failed, or canceled.

Procedure

Step 1. Select **Configure ➙ Lenovo XClarity Integrator ➙ Rolling Reboot**.

Step 2. Select a finished, failed or canceled RSR task from the list.

Step 3. Click **COPY** to launch the copy task wizard.

Step 4. Edit the original selection and click **FINISH** to save the new task.

Deleting an RSR task

Use the **DELETE** option to remove a Rolling System Reboot (RSR) task from the task list if it is not currently running. All RSR tasks that are not currently running can be deleted.

Procedure

Step 1. Select **Configure ➙ Lenovo XClarity Integrator ➙ Rolling Reboot**.

Step 2. Select one or more RSR tasks that are not currently running from the list.

Step 3. Click **DELETE**. The selected tasks are removed from the task list.

Canceling a running RSR task

Use the **CANCEL** option to cancel a Rolling System Reboot (RSR) task while it is running. When a task is canceled, the task status changes to `Canceling`.

Procedure

Step 1. Select **Configure ➙ Lenovo XClarity Integrator ➙ Rolling Reboot**.

Step 2. Select a running RSR task from the list.

Step 3. Click **CANCEL**. RSR completes updating the host that has started and only cancels the others. This task may take several minutes to complete.

Viewing the RSR task report

The Rolling System Reboot Report view provides detailed task status information.

Procedure

Select **Configure ➙ Lenovo XClarity ➙ Rolling Reboot**, and click a status link in the **Status** column to open the Rolling System Reboot Report view. The table below lists the status for tasks and hosts. For detailed information about the Rolling System Reboot tasks, refer to "Working with the Rolling System Reboot function" on page 44.

Table 15. Rolling System Reboot task status

Target	Status	Description
Rolling Reboot Task	Not Started	The task has not started.
	Running	The task is running.

Table 15. Rolling System Reboot task status (continued)

Target	Status	Description
	Canceled	The task is canceled.
	Failed	Causes of task failure: • Downloading firmware package failed. • Restarting ESXi host failed. • VM migration failed. • Firmware update failed
	Finished	The task has completed.
Host	Not Started	The update for the host has not started.
	Migrating	The host is entering maintenance mode.
	Maintenance	The host is in maintenance mode.
	Reboot	The host is restarting after updating completes.
	Exit Maintenance	The host is exiting maintenance mode.
	Success	The firmware update succeeded.
	Failed	The causes of host failure: • Cannot enter maintenance mode. • Cannot restart the host. • Cannot exit maintenance mode.

Working with Proactive HA

VMware vSphere v6.5 adds the new Proactive HA feature, which is an enhancement of the original High Availability (HA) feature. Lenovo XClarity Integrator for VMware vCenter supports the Proactive HA feature by registering a Lenovo Proactive HA provider to VMware vCenter.

Before you begin
• Ensure that VMware vSphere v6.5 or later is installed.
• Ensure that Lenovo XClarity Integrator is successfully registered in VMware vCenter.

Enabling VMware vCenter Proactive HA with Lenovo Proactive HA Provider for a cluster

Before you begin

If the cluster is not an empty cluster, ensure to request BMC access for each host in the cluster; otherwise, Lenovo Proactive HA provider might not display correctly.

If the same host with BMC access has been deleted but added back, users should request BMC access again even if the user interface indicates that the host can access the BMC; otherwise, Lenovo Proactive HA provider might not display correctly.

Procedure

Step 1. In the vSphere Client, click the cluster to be configured.

Step 2. Select **Configure ➙ vSphere Availability**, and then click **Edit** on the right hand side of the page. A configuration dialog displays.

Step 3. Under **vSphere DRS**, select **Turn ON vSphere DRS**.

Step 4. Under **vSphere Availability**, select **Turn ON Proactive HA**.

Step 5.   Under **Proactive HA Failures and Responses**, set the **Automation Level** to `Automated` and set **Remediation** to `Mixed Mode` or `Maintenance Mode`.

Step 6.   Under the Proactive HA provider list, select the **com.lenovo.HealthUpdateProvider_ver100** provider.

Step 7.   Optional: Choose to ignore certain failure conditions for specific hosts or the entire cluster by clicking **Edit** on the right side of the dialog. Another dialog displays in which users can select the events and hosts for ignoring failure conditions. For more information, see the VMware vSphere user guide.

Note: According to VMware, users can use other automation level and remediation settings, but there are some limitations. For example, if users use "manual" and "quarantine" mode, the host must have at least 1 VM; otherwise, incoming health event are not received.

Adding a host to a Proactive HA enabled (with Lenovo Provider) cluster

Procedure

Step 1.   Add the host to a DataCenter or any other Proactive HA disabled cluster.

Step 2.   Request BMC access of the host (see "Discovering and managing the BMC" on page 15).

Step 3.   Move the host to the Proactive HA enabled cluster.

Note: If the same host with BMC access has been deleted but added back, users should request BMC access again even if the user interface indicates that the host can access the BMC; otherwise, the host cannot be removed to the Proactive HA enabled cluster.

Re-using Lenovo Proactive HA Provider

The Lenovo Proactive HA provider is automatically registered in VMware vCenter when registering Lenovo XClarity Integrator in VMware vCenter, either in the wizard or administration page. When users deregister Lenovo XClarity Integrator from VMware vCenter, a window will be prompted to ask whether to also deregister Proactive HA provider. Normally users can keep the provider in VMware vCenter so that it can be reused the next time registering Lenovo XClarity Integrator to VMware vCenter and the provider setting in VMware vCenter is kept.

Proactive HA Heartbeat

Lenovo XClarity Integrator needs the heartbeat with VMware vCenter to ensure Proactive HA work correctly. If the message "Provider com.lenovo.HealthUpdateProvider_ver101 has not posted an update in 300 seconds" is displayed in the event list of Proactive HA enabled cluster, the heartbeat might be dead because of some corner reasons. Check the network to check whether Lenovo XClarity Integrator can correctly communicate with VMware vCenter, and whether the Lenovo XClarity Integrator appliance is available. If the problem still exists, restart Lenovo XClarity Integrator.

Managing hardware events

Hardware events and alarms are integrated into vCenter. Lenovo XClarity Integrator for VMware vCenter loads events from out-of-band (OOB) BMC nodes into the vCenter server, allowing administrators to view and manage them from vSphere Client. This provides administrators with a single, heterogeneous view of all host system events within the managed environment.

What to do next

Select the **Events** tab in vSphere Client to view Lenovo hardware events.

Alarms

When a Lenovo event is delivered to VMware vCenter Server, the overall host status changes based on the corresponding event severity. An alarm is triggered when the changes to the host status meet the criteria assigned by the administrator.

When an alarm occurs, an icon is displayed to the right of the vSphere Client window along the toolbar above the vSphere Client tabs or on the host icon in the inventory tree.

To view a list of all alarms contained in the **Alarms** tab, click the alarms icon.

Chapter 7. Administering Lenovo XClarity Integrator

This chapter provides information about using the Lenovo XClarity Integrator for VMware vCenter administrator Web page to collect service data, register the plug-in, and backup and restore appliance configurations.

Configuring vCenter connections

When Lenovo XClarity Integrator for VMware vCenter is initially deployed, it is registered in a vCenter server. Users can register Lenovo XClarity Integrator for VMware vCenter to additional vCenter servers. Users also can unregister Lenovo XClarity Integrator for VMware vCenter from a vCenter server.

Registering Lenovo XClarity Integrator to vCenter server

Users can register Lenovo XClarity Integrator to one vCenter server or multiple vCenter servers in linked mode.

Before you begin

Prepare a vCenter user name and password for registering Lenovo XClarity Integrator to the vCenter server. The vCenter user can be a vCenter administrator or a dedicated service user with low security privilege. If a dedicated service user is used, the following privileges are required:
- Alarms.Create
- Datacenter.Create
- Extension.Register
- Extension.Unregister
- Extension.Update
- Global.LogEvent
- HealthUpdateProvider.Register
- HealthUpdateProvider.Unregister
- HealthUpdateProvider.Update
- Host.Config.Maintenance
- Host.Inventory.ModifyCluster
- Resource.ColdMigrate
- Resource.HotMigrate
- Sessions.ValidateSession

Note: These privileges can be manually or automatically granted to the vCenter user in registration.

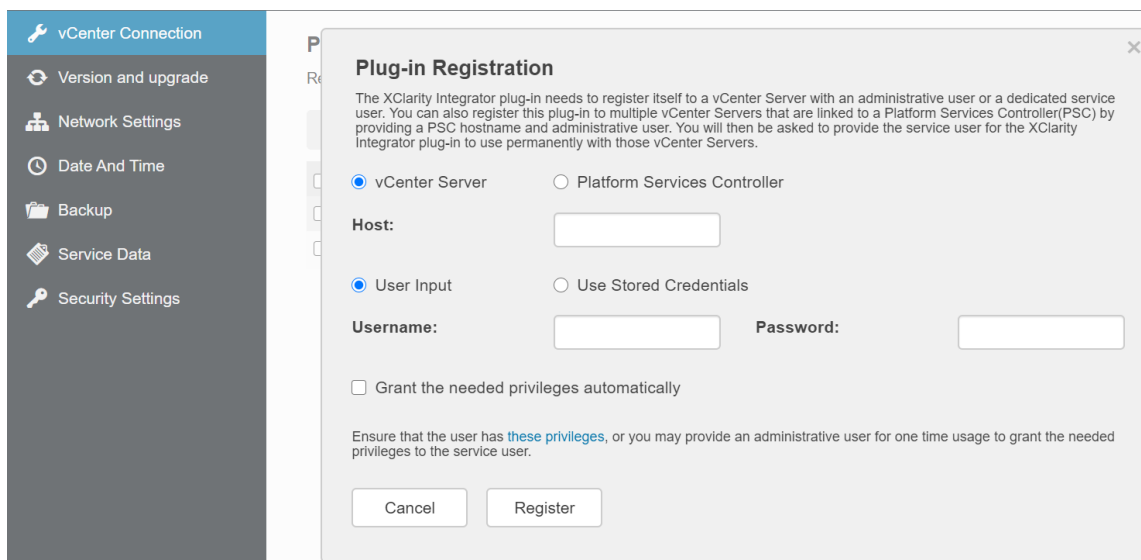### Registering LXCI to one vCenter server

Users can register Lenovo XClarity Integrator to one vCenter server or multiple vCenter servers separately.

Procedure

Complete the following steps to register Lenovo XClarity Integrator to a vCenter server:

Step 1.   On the **vCenter Connection** page, click **Register**. The **Plug-in Registration** page is displayed.

Step 2. Select **vCenter Server**. In the **Host** field, input the fully qualified domain name (FQDN) or IP address of the vCenter server.

> **Note:** If the vCenter is configured with the FQDN, it is recommended to input the vCenter FQDN instead of the IP address. Meanwhile, ensure that the DNS is configured on the **Network Settings** pane.

Step 3. Do one of the following:
- To manually register, select **User Input**, and input the vCenter user name in the **Username** field and the password in the **Password** field.
- To register through credentials, select **Use Stored Credentials → Manage → Create**. In the Create new stored credentials window, input the vCenter user name in the **User name** field and the password in the **Password** field and the **Confirm Password** field, click **Save → Close**, and select the credential from the drop-down list.

> **Note:** If the vCenter user does not have the privileges required by Lenovo XClarity Integrator, select the **Grant the needed privileges automatically** check box, input an administrative user account in the **Administrative user** field, and input the password in the **Password** field. Lenovo XClarity Integrator will automatically grant the privileges to the vCenter user through the administrative user account. However, Lenovo XClarity Integrator will not save the administrative account information.

Step 4. Click **Register**.

Registering LXCI to multiple vCenter servers in linked mode

Users can register Lenovo XClarity Integrator to multiple vCenter servers connected to Platform Services Controller (PSC) in linked mode by using a PSC hostname.

Procedure

Complete the following steps to register Lenovo XClarity Integrator to multiple vCenter servers in linked mode:

Step 1. On the **vCenter Connection** page, click **Register**. The **Plug-in Registration** page is displayed.

Step 2. Select **Platform Services Controller**, input the fully qualified domain name (FQDN) or IP address of PSC in the **Hostname or IP** field, and click **Next**.

> **Note:** If the FQDN is input, ensure that the DNS is configured on the Network Settings page.
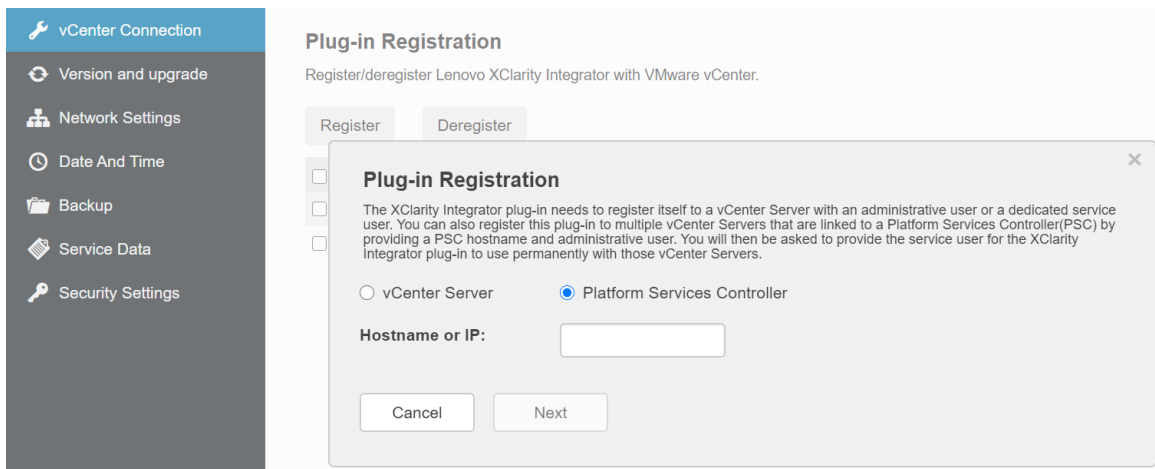
Step 3. From the **Host** list, select the target vCenter servers, and click **Next**.

Step 4. Do one of the following:
- To manually register, select **User Input**, and input the vCenter user name in the **Username** field and the password in the **Password** field.
- To register through credentials, select **Use Stored Credentials ➙ Manage ➙ Create**. In the **Create new stored credentials** window, input the vCenter user name in the **User name** field and the password in the **Password** field and the **Confirm Password** field, click **Save ➙ Close**, and select the credential from the drop-down list.

   Notes:
   - The vCenter user should have access to all the target vCenter servers.
   - If the vCenter user does not have the privileges required by Lenovo XClarity Integrator, select the **Grant the needed privileges automatically** check box, input an administrative user account in the **Administrative user** field, and input the password in the **Password** field. Lenovo XClarity Integrator will automatically grant the privileges to the vCenter user through the administrative user account. However, Lenovo XClarity Integrator will not save the administrative account information.

Step 5. Click **Register**.

Unregistering Lenovo XClarity Integrator from vCenter server

Users can unregister Lenovo XClarity Integrator from vCenter server.

Procedure

Step 1. Select one or more than one vCenter server, and then click **Deregister**. A confirmation dialog is displayed.

Step 2. Click **Yes** to confirm to unregister Lenovo XClarity Integrator.

Step 3. Click **Yes** again to complete the unregistration process.

   If successful, a dialog similar to the following figure is displayed.

Deregister the plug-in from vCenter completely, also need to do:

* Remove the com.lenovo.lxci-*.* directory on vCenter Server

Windows: C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity

Appliance: /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity

* Restart vsphere-client service

OK
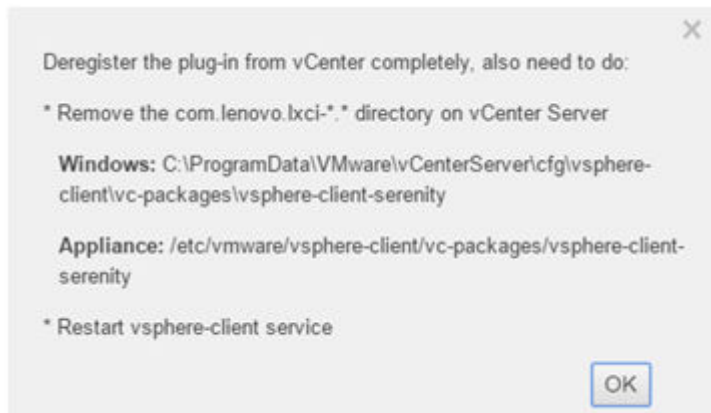
Step 4.   On the vCenter server, remove the `com.lenovo.lxci-*.*` directory.

Step 5.   Restart the "vsphere-client" service.

Editing the server credential

Users can edit the server credential.

Procedure

Step 1.   Select the target vCenter server, and click **Edit Credential**.

Step 2.   On the Edit selected credential window, input user name and password, and click **Save**.

Updating management server software

On this setting page, users can download the latest update packages from the LXCI web site, and update the management server software to the latest version.

Procedure

Step 1.   Click **Version and upgrade** on the left navigation pane. The **Update Management Server** page is displayed.

Step 2.   On the **Update Management Server** page, click **Check for Updates** to check new update packages applicable to the current LXCI server.

   Note: If LXCI instance is connected to Internet, it will automatically check the updates and notify user once a week.

Step 3.   Select the required package from the list, and click **Download**.

Step 4.   Select the required package from the list, and click **Perform Update**.

Configuring network access

In this setting page, users can configure host-name, domain name, DNS, and IP settings for Eth0 and Eth1 interfaces.

Before you begin

When a Lenovo XClarity Integrator is initially deployed, the Eth0 interface is enabled for connecting both the VMWare vCenter and baseboard management controller (BMC) network. Users can optionally enable the Eth1 interface for the BMC network connection. After the Eth1 interface is enabled, Eth0 interface is no longer available for BMC connections.

It is not recommended to change network settings set in the wizard. If the network settings should be changed, perform the following steps to reconfigure the virtual appliance.

Attention: The incorrect changes on the settings might cause disconnection to the virtual appliance.
1. Regenerate the server certificate (see "Working with security certificates" on page 60).
2. Unregister vCenter and re-register again (see "Configuring vCenter connections" on page 51.
3. Clean up Lenovo XClarity Integrator on the vCenter server (see "Uninstalling Lenovo XClarity Integrator for VMware vCenter" on page 13).
4. In the following cases, disable management over all hosts that are managed by Lenovo XClarity Integrator, and then manage the hosts again.
   - Eth0 is changed and Eth1 is disabled.
   - Eth1 is changed.

Configuring the hostname, domain name, and DNS

Users can configure the hostname, domain name, and DNS from the Network Settings page.

Procedure

Step 1.   Click **Network Settings** on the left navigation pane, and click **IP and DNS Settings** tab on the right pane.

Step 2.   On the **Host Name, Domain Name and DNS for virtual appliance** area, change the hostname, DNS, and domain name.

   Notes:
   - The domain name is optional. To configure both the hostname and domain name, a fully qualified domain name (FQDN) is defined. In this case, this FQDN is used for vCenter registration and server-certificate generation. Ensure that the DNS is correctly set in vCenter.
   - To use the hostname to connect vCenter and vCenter managed EXSi hosts, configure a DNS for Lenovo XClarity Integrator to make Lenovo XClarity Integrator access vCenter and ESXi hosts through the hostname.

Step 3.   Click **Save**.

Configuring Eth0 IP settings

Users can change the Eth0 IP address and gateway settings from the Network Settings page.

About this task

When users change IP settings for the Eth0 interface, connection to Lenovo XClarity Integrator Web interface is lost. Check the VM console for the new Eth0 IP address, and reopen Lenovo XClarity Integrator Web interface to continue the setup.

Procedure

Step 1.   Click **Network Settings** on the left navigation pane, and click **IP and DNS Settings** tab on the right pane.

Step 2.   On the **IP Settings** area, specify the IPv4 address, IPv6 address or both for the Eth0 interface.

   For IPv4, users can use a statically assigned IP address, obtain an IP address from a DHCP server, or disable IPv4.

   For IPv6, users can assign an IPv6 address to the interface using one of the following assignment methods:
   - Use a statically assigned IP address
   - Use a stateful address configuration (DHCPv6)

- Use a stateless address auto configuration

Step 3.   Specify the default gateway.

  Notes:
  - Because Eth1 is intentionally used for connecting to the BMC network, which is normally within the Eth1 subnet, users are allowed to configure the default gateway for only Eth0.
  - If users specify a default gateway, the input must be a valid IP address and must use the same network mask (the same subnet) as the IP address for Eth0.
  - If Eth0 uses DHCP to obtain an IP address, the default gateway must also use DHCP and cannot be changed.

Step 4.   Click **Save**.

Configuring Eth1 IP settings

Users can enable the Eth1 interface for the baseboard management controller (BMC) network and change the Eth1 IP address and gateway settings on the **Network Settings** page.

About this task

By default, both Eth0 and Eth1 are connected to the same VM network with label "VM Network". Users can configure Eth1 to connect to a different network by completing the following steps:
  1. Edit Lenovo XClarity Integrator VM settings
  2. Select **Network adapter 2**, and select the target VM network.
  3. Save the settings.

Procedure

Step 1.   Click **Network Settings** on the left navigation pane, and click **IP and DNS Settings** tab on the right pane.

Step 2.   On the **IP Settings** area, select **Enable Eth1** to enable Eth1. The IP setting fields are displayed.

Step 3.   Specify the IPv4 address, IPv6 address or both for the Eth1 interface.

  Note: The IP addresses that are assigned to the Eth1 interface must be in a different subnet from the IP addresses that are assigned to the Eth0 interface. 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.

  For IPv4, users can use a statically assigned IP address, obtain an IP address from a DHCP server, or disable IPv4

  For IPv6, users can assign an IPv6 address to the interface using one of the following assignment methods:
  - Use a statically assigned IP address
  - Use a stateful address configuration (DHCPv6)
  - Use a stateless address auto configuration

Step 4.   Click **Save**.

Configuring proxy

Users can set proxy for LXCI to connect Internet on the **Network Settings** page.

Note: Only HTTP protocol is supported.

Procedure

Step 1. Click **Network Settings** on the left navigation pane, and click **Internet Settings** tab on the right pane.

Step 2. On the **Proxy settings** area, select **Use HTTP proxy**, and input proxy, port, user name, and password.

> **Notes:**
> - The proxy should be an IPv4/IPv6 address or a FQDN
> - The proxy port should be an integer between 0 and 65535.

Step 3. Click **Save**.

Configuring advanced routing

Users can add, edit, and remove the route on the **Network Settings** page.

Procedure

Step 1. Click **Network Settings** on the left navigation pane, and click **Advanced Routing** tab on the right pane.

Step 2. Do one of the following:
- To add the route:
   1. Click **Add**. The Advanced Route Settings window is displayed.
   2. On the Advanced Route Settings window, select interface and route type from the drop-down list, and input destination, netmask, and gateway.
   3. Click **Save**.
- To edit the route:
   1. Select the target route and click **Edit**. The Advanced Route Settings window is displayed.
   2. On the Advanced Route Settings window, select interface and route type from the drop-down list, and edit destination, netmask, and gateway.
   3. Click **Save**.
- To remove the route, select the target route, and click **Remove**.

Testing network connection

Users can test network connection on the **Network Settings** page.

Procedure

Step 1. Click **Network Settings** on the left navigation pane, and click **Test Connection** tab on the right pane.

Step 2. Select the method for testing connection from the drop-down list, and input host name, port number, count, probes, and time out.

Step 3. Click **Test Connection**. The test result will be displayed on the **Result** area.

Setting the date and time

Users can change the date and time from the **Date and Time** page.

Procedure

Perform the following steps from the **Date and Time** page.

Step 1. Specify the region and time zone.

Step 2. Specify the date and time. Users can set the date or time manually or let Lenovo XClarity Integrator synchronize with an NTP server.

> **Notes:**

- Lenovo XClarity Integrator only supports NTP Version 4.
- Use comma (,) to separate if multiple NTP server addresses are added.

Step 3.   Click **Save**.

Collecting service data

Users can collect Lenovo XClarity Integrator logs and send to Lenovo Service for support.

Procedure

Step 1.   Click **Service Data** on the left navigation pane.

Step 2.   (Optional) Enable **Send LXCI audit logs to vCenter**.

Step 3.   On the **Collect Log** page, select the log level from the drop-down list.

> **Note:** If required, users select **Debug**. Ensure to restore the log level to Information after problem resolved.

Step 4.   Click **Collect Log**. The **Download Log** link is displayed.

Step 5.   Click the **Download Log** link to download the log.

Managing authentication and authorization

Lenovo XClarity Integrator for VMware vCenter provides security mechanisms to verify the user credentials and control access to resources and tasks.

Setting up an external LDAP authentication server

Users can use an external LDAP authentication server instead of the local LXCI for VMware vCenter authentication server on the management node.

Before you begin
- The initial setup of LXCI for VMware vCenter must be completed before setting up the external authentication server.
- The following external authentication servers are supported:
  – Microsoft Active Directory. It must reside on an outboard Microsoft Windows server that is able to communicate with LXCI for VMware vCenter appliance.
- LXCI for VMware vCenter performs a connectivity check every 10 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, specify only known, reachable LDAP servers when configuring LDAP Client.
- Ensure that the LDAP users that can login this XClarity Integrator web interface are the members of the LDAP group in the LDAP server.

  Create the group and add the users to it in the LDAP server before configuring this LDAP Client:
  1. From the external authentication server, create a user account. For instructions, see the documentation of the LDAP server.
  2. Create a group in the LDAP server. The LDAP group name can be the default name **LXCI-SUPERVISOR** or other user-defined names. The group must exist within the context of the root distinguished name defined in the LDAP client.
  3. Add the user as a member of the group created previously.

Procedure

To configure LXCI for VMware vCenter to use an external authentication server, complete the following steps.

Step 1. Set up the user-authentication method for Microsoft Active Directory, do one of the following:
- To use non-secure authentication, no additional configuration is required. The Windows Active Directory domain controllers use non-secure LDAP authentication by default.
- To use secure LDAP authentication:
    1. Set up the domain controllers to allow secure LDAP authentication. For more information about setting configuring secure LDAP authentication in Active Directory, see https:// social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx.
    2. 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.
    3. Import the LDAP server certificate, the intermediate certificates(if any), and the root certificate of the certificate authority signing the server certificate.
        a. From the left navigation pane of LXCI for VMware vCenter menu, click **Security Settings**.
        b. Click **Trusted Certificates** in the Certificate Management section.
        c. Click **Add**.
        d. In the Add window, click **Choose File** to upload the target certificate.
        e. Click **Upload Certificate**.

Step 2. Configure the LXCI for VMware vCenter LDAP client:

a. From the left navigation pane of LXCI for VMware vCenter, click **Security Settings ➙ LDAP Client**.

b. Select one of these user-authentication methods:

- **Allow logons from local users**. Authentication is performed using the local authentication. When this option is selected, users can only log in to LXCI with the local account.

- **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. If this method is selected, do the following:
    1. Input one or more server addresses and ports.
    2. Input LDAP group name.

        Note: By default, the LDAP group name is **LXCI-SUPERVISOR**. Users can also input other names.
    3. Select one of these binding methods:
        – **Configured Credentials**. Use this binding method to use the client name and password to bind LXCI for VMware vCenter 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, sAMAccountName, NetBIOS name, or UserPrincipalName. The client user 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: To change the client password in the external authentication server, ensure that the new password in LXCI for VMware vCenter is updated . If the client password is changed in the external LDAP server, users can log in to the Integrator using local account to update the new password.
        – **Login Credentials**. Use this binding method to use a LDAP user name and password to bind LXCI for VMware vCenter to the external authentication server.

The specified user ID and password are used only to test the connection to the authentication server. If successful, the LDAP client settings will be saved, but the test login credential specified will not be saved. All future binds use the user name and password used to log in to LXCI for VMware vCenter.

Notes:
– Users should log in to LXCI for VMware vCenter using a fully-qualified user ID (for example, `administrator@domain.com` or `DOMAIN\admin`).
– Users should use a fully qualified test client name for the binding method.

4. In the **Root DN** field, specify the top-most entry in the LDAP directory tree. In this case, searches are started using the specified root distinguished name as the search base.

5. In the **User Search Attribute** field, 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 DN 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.

6. In the **Group Search Attribute** field, specify the attribute name that is used to identify the groups to which a user belongs.

7. In the **Group Name Attribute** field, specify the attribute name that is used to identify the group name that is configured by the LDAP server.

c. Click **Save**.

The LXCI for VMware vCenter attempts to test the configuration to detect common errors. If the test fails, error messages are displayed that indicate the source of the errors. For the **Configured Credentials** binding method, if the test succeeds and connections to the specified servers complete successfully, user authentication might still fail if:
• If mis-configuration or changes are in the LDAP server, users can log in using the local account. It is recommended to keep a record of the local account and password.
• The root distinguished name is incorrect.
• The user is not a member of the LDAP group in the LDAP server.

d. Click **OK**.

Results

LXCI for VMware vCenter validates the LDAP server connection. If the validation passes, user authentication occurs on the external authentication server when logging in to LXCI for VMware vCenter.

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 LXCI for VMware vCenter, and user accounts must be defined as members of the LDAP group in the LDAP server. Otherwise, user authentication fails.

Working with security certificates

Lenovo XClarity Integrator and the supporting software (Lenovo XClarity Administrator and VMWare vCenter) use SSL certificates to establish secure connections between each other. By default, Lenovo XClarity Integrator uses Lenovo XClarity Integrator-generated certificates that are self-signed and issued by an internal certificate authority (CA).

Generating a customized externally-signed server certificate

When installing a customized server certificate in Lenovo XClarity Integrator, users should provide the certificate bundle that contains the entire CA signing chain.

About this task

If the new server certificate is not signed by a trusted international third party (such as VeriSign), the next time connecting to Lenovo XClarity Integrator, a security message will be prompted users to accept the new certificate as an exception into the browser. To avoid the security messages, users can import the CA signing chain of the server certificate into the Web browser list of trusted certificates.

For more information about importing certificates, see "Importing the Lenovo XClarity Integrator certificate in Web browser" on page 19.

Procedure

Complete the following steps to generate a customized server certificate.

Step 1. Generate a certificate signing request (CSR) for Lenovo XClarity Integrator.

    a. On the left navigation pane, click **Security Settings**.

    b. Click **Server Certificate** to display the **Server Certificate** page.

    c. Click the **Generate Certificate Signing Request (CSR)** tab.

    d. Fill in the fields in the Generate Certificate Signing Request (CSR) page:
- Country
- State or Province
- City or Locality
- Organization
- Organization Unit (optional)
- Common Name

    Attention: Select a common name that matches the IP address or hostname of Lenovo XClarity Integrator virtual appliance. Failure to select the correct value might result in connections that are not trusted. Users can allow Lenovo XClarity Integrator to generate the common name automatically by specifying "Generated by LXCI."

    e. Click **Generate CSR File** to download the generated file.

Step 2. Submit all CSRs to the trusted CA for signing. The trusted CA returns a certificate bundle for each CSR. The certificate bundle contains the signed certificate and the complete certificate authority (CA) chain of trust.

Step 3. Upload the externally-signed server certificate to Lenovo XClarity Integrator.

    Note: The certificate being uploaded must have been created from the Certificate Signing Request that was most recently created using the **Generate CSR File** button. The uploaded file must contain the complete certificate chain, including the root certificate and any intermediate certificates. The order of certificates in the file must be server certificate, intermediate certificates, and then root certificate.

    1. On the left navigation pane, click **Security Settings**.
    2. Click **Server Certificate** on the setting page.
    3. Click the **Upload Certificate** tab.
    4. Click the **Choose File** button to select the certificate file (.der, .pem or .cer).
    5. Click the **Upload Certificate** button. The certificate file is uploaded.

After uploading the server certificate, Lenovo XClarity Integrator is restarted and the browser connection to the Lenovo XClarity Integrator Web interface is terminated. To continue the task, log in to the Lenovo XClarity Integrator Web interface again.

Note: Update VMware vCenter registration after the new server certificate is uploaded.

Restoring the Lenovo XClarity Integrator-generated server certificate

Users can generate a new server certificate to reinstate a Lenovo XClarity Integrator-generated certificate if Lenovo XClarity Integrator currently uses a customized server certificate. The customized server certificate is then replaced and the new self-signed server certificate is used on the Lenovo XClarity Integrator.

Procedure

Complete these steps to generate a new server certificate and sign the certificate with the currently generated CA root certificate:

Step 1. On the left navigation pane, click **Security Settings**.

Step 2. Click **Server Certificate** on the setting page.

Step 3. Click the **Regenerate Server Certificate** tab.

Step 4. Fill in the fields in the **Regenerate Server Certificate** page:
- Country
- State or Province
- City or Locality
- Organization
- Organization Unit
- Common Name

Note: Select a common name that matches the IP address or hostname of the Lenovo XClarity Integrator virtual appliance. Failure to select the correct value might result in connections that are not trusted. Users can allow Lenovo XClarity Integrator to generate the common name automatically by specifying "Generated by LXCI".

Step 5. Click **Regenerate Certificate**

When the new server certificate is regenerated, Lenovo XClarity Integrator is restarted and the browser connection to the Lenovo XClarity Integrator Web interface is terminated. To continue the work, log in to the Lenovo XClarity Integrator Web interface again.

Note: Update VMWare vCenter registration after the server certificate is regenerated.

Regenerating Certificate Authority (CA) Root

Users can regenerate Certificate Authority (CA) Root.

Procedure

Step 1. On the left navigation pane, click **Security Settings**.

Step 2. Click **Certificate Authority** on the setting page.

Step 3. Click **Regenerate Certificate Authority Root Certificate**.

Notes:
1. After regenerating CA root, users should regenerate server certificate. Refer to "Restoring the Lenovo XClarity Integrator-generated server certificate" on page 62.
2. After regenerating CA root, users should re-trust the CA in all client PCs. Refer to "Importing the Lenovo XClarity Integrator certificate in Web browser" on page 19.

Downloading and installing Certificate Authority (CA) Root

Users can download and install Certificate Authority (CA) Root.

Procedure

Step 1.   On the left navigation pane, click **Security Settings**.

Step 2.   Click **Certificate Authority** on the setting page.

Step 3.   Click **Download Certificate Authority Root Certificate**.

Step 4.   Double-click the ca.der file.

Step 5.   Click the **General** tab, and click **Install Certificate**.

Step 6.   Click **Next**.

Step 7.   In the Certificate Store page, select **Place all certificates in the following store**, and click **Browse**.

Step 8.   Select **Trusted Root Certificate Authorities**, and click **OK**.

Step 9.   Click **Finish**.

>   **Note:** If users' browser is Firefox, a dialog will be displayed in step 3. This dialog asks whether to trust the certificate. Check **Trust this CA to identify websites**, click **OK** and skip Step 4 to Step 9.

Downloading Server Certificate

Users can download Server Certificate.

Procedure

Step 1.   On the left navigation pane, click **Security Settings**.

Step 2.   Click **Server Certificate** on the setting page.

Step 3.   Click the **Download Certificate** tab.

Step 4.   Click **Download Certificate**.

Managing Trusted Certificates

Users can add, download or remove the trusted certificates.

Procedure

Step 1.   On the left navigation pane, click **Security Settings**.

Step 2.   Click **Trusted Certificates** on the setting page.

Step 3.   Do one of the following:
- To add a trusted certificate:
    1. Click **Add**.
    2. In the Add window, click **Choose File** to upload the target certificate.
    3. Click **Upload Certificate**.
- To download a trusted certificate:
    1. Select the target certificate.
    2. Click **Save**. The certificate will be saved in the local.
- To remove a trusted certificate:
    1. Select the target certificate.
    2. Click **Remove**. A pop-up dialog will be displayed for users to confirm whether to remove the certificate.
    3. Click **Yes**.

Shutting down or restarting Lenovo XClarity Integrator

Users can shut down or restart Lenovo XClarity Integrator. However, Lenovo XClarity Integrator will be disconnected after being shut down or restarted, so users should re-connect it after this process.

Before you begin

Ensure that no job is running. All running jobs will be canceled when shutting down or restarting Lenovo XClarity Integrator.

Procedure

Complete the following steps to shut down or restart Lenovo XClarity Integrator:

Step 1.　On the **Lenovo XClarity Integrator for VMware vCenter** page, click **Power Control** on the top right corner. A confirmation dialog with a list of jobs that are running will be prompt.

Step 2.　Click **Shut down** or **Restart**. Lenovo XClarity Integrator will be shut down or restarted, and all running jobs will be canceled.

Appendix A. Troubleshooting

Use this section to troubleshoot and resolve problems with Lenovo XClarity Integrator for VMware vCenter.

The firmware and driver addon list is not displayed

When creating an image for a cluster by using vSphere Lifecycle Manager, if **Lenovo XClarity Integrator** is selected as the hardware support manager, and the proxy is enabled in vCenter but not configured to allow the connection from vCenter to LXCI (protocol HTTPS, port 443), the firmware and driver addon list might not be displayed.

Procedure

Complete the following steps to solve the problem.

Step 1.   Reproduce this issue.

Step 2.   Log in to the vCenter shell console.

Step 3.   In the shell, run the following command:
```
vi /storage/log/vmware/vmware-updatemgr/vum-server/hsm-service.log
```

Step 4.   If the following error message or similar is displayed, the HTTPS request from vCenter to XClarity Integrator is banned by the proxy. Users should disable the proxy or allow the connection from vCenter to Lenovo XClarity Integrator (protocol HTTPS, port 443) in the proxy configuration.
```
HTTPSConnectionPool(host='<XClarity Integrator IP or FQDN', port=443): Max retries exceeded with url:
/hsm/vsphere-lcm/hw-support/v1/packages (Caused by ProxyError('Cannot connect to proxy.', OSError
('XXX failed or timeout: '))).
```

BMC Discovery failure

If the BMC Discovery list does not display correctly, the BMC discovery process has failed.

About this task

If the discovery list fails to display after clicking **Discovery**, complete these steps.

Procedure

Step 1.   Verify that the network connection between vCenter and the host is working.

Step 2.   Try the discovery process again by clicking **Discovery**.

The chassis map, firmware update, or configuration pattern page is not displayed

The chassis map, firmware update, or configuration pattern page might not be displayed.

Procedure

Complete the following steps to solve the problem.

Step 1.   Ensure that the Lenovo XClarity Integrator certificate has been installed by following the instructions in "Importing the Lenovo XClarity Integrator certificate in Web browser" on page 19.

Step 2.   If the vCenter FQDN has been used to registerLenovo XClarity Integrator to the vCenter client, use the vCenter FQDN to open the vSphere client.

Lenovo XClarity Integartor is not displayed on the vSphere Client after installation

After installing Lenovo XClarity Integrator and registering it with vCenter successfully, vSphere Client might fail to download and deploy the Lenovo XClarity Integrator plug-in. In this case, Lenovo XClarity Integrator is not displayed on the vSphere Client.

Procedure

Check the `vsphere_client_virgo.log` file for the following error message:
```
Error downloading https://[********LXCI IP********]:443/IVPUI.zip. Make sure that the URL is reachable;
then logout/login to force another download. java.net.ConnectionException: Network is unreachable.
```

Note: The log file is located in the `C:\ProgramData\VMware\vCenterServer\logs\vsphere-client\logs` or `/storage/log/vmware/vsphere-client/logs` directory, depending on version of vCenter.

If the error message in present in the log file, perform one of the following steps:
- For windows vCenter, open a Web browser on the VMware vCenter Server and access the URL that is displayed in the error message (for example, `https://[********LXCI IP********]:443/IVPUI.zip`). If it doesn't work, verify that Lenovo XClarity Integrator server is running.
- For vCenter virtual appliance, run the command `curl <URL>` on the VMware vCenter Server, where `<URL>` is the URL that is displayed in the error message (for example, `https://[********LXCI IP********]:443/IVPUI.zip`).

If an error messages is displayed similar to "SSL certificate problem, verify that the CA cert is OK" or "Certificate verify failed", import the Lenovo XClarity Integrator certificate to the VMware vCenter Server appliance by performing the following steps:
1. Open Lenovo XClarity Integrator appliance management Web page, and then log in to the Web page.
2. Click **Security Settings** on the left pane, and then click **Certificate Authority**.
3. Click **Download Certificate Authority Root Certificate**.
4. Import Lenovo XClarity Integrator certificate to the VMware vCenter Server as Trusted Root Certificate.

Data displayed on Lenovo XClarity Integrator is not up to date when Lenovo XClarity Integrator is opened on Internet Explorer 11 or later versions

The cache mechanism of the Internet Explorer might impact the use of Lenovo XClarity Integrator. Users should set the Internet options once using Internet Explorer 11 or later versions to visit the Lenovo XClarity Integrator Web page.

Procedure

Step 1.   Open the Internet Explorer browser and click **Tools ➙ Internet options**. The Internet Options window is displayed.

Step 2.   Click the **General** tab and click **Settings**. The Website Data Settings window is displayed.

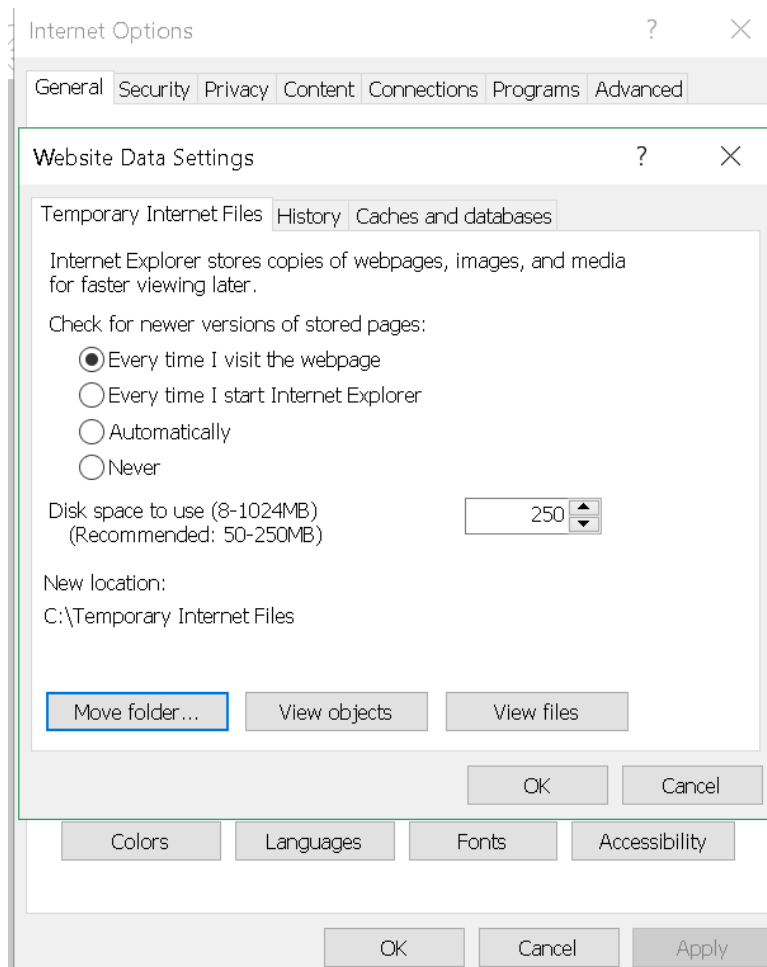Step 3.   Select **Every time I visit the webpage** and click **OK**.

Figure 13. Internet Explorer settings

Step 4.   Click **OK** in the Internet Options window.

Hardware events of a host are lost when this host is managed by two vCenter clients

One host can be managed by only one vCenter client. If a host is added to a new vCenter client without removing from the original vCenter, hardware events of this host will not be received by the LXCI on the original vCenter client.

Users should remove the host from the original vCenter.

Appendix B. Accessibility features

Accessibility features help users who have physical disabilities, such as restricted mobility or limited vision, to use information technology products successfully.

Lenovo strives to provide products with usable access for everyone, regardless of age or ability.

The *Lenovo XClarity Integrator for VMware vCenter Installation and User Guide* supports the accessibility features of the system-management software in which they are integrated. Refer to the system management software documentation for specific information about accessibility features and keyboard navigation.

The VMware vCenter topic collection and its related publications are accessibility-enabled for screen-reader technology. Users can operate all features by using the keyboard instead of the mouse.

Users can view the publications for Lenovo XClarity Integrator for VMware vCenterin Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader. Publications are available for download from the Lenovo XClarity Integrator for VMware Web site.

Lenovo and accessibility

See the Lenovo Accessibility Web site for more information about the commitment that Lenovo has to accessibility.

Appendix C. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information about 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.
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.

Trademarks

LENOVO, FLEX SYSTEM, SYSTEM X, and NEXTSCALE SYSTEM are trademarks of Lenovo. Intel and 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. All other trademarks are the property of their respective owners. © 2024 Lenovo.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

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.

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.