Lenovo XClarity Integrator for VMware vCenter Installation and User Guide

Version 7.7.0

Note

Before using this information and the product it supports, read the information in Appendix C "Notices" on page 75.

Twenty-third Edition (June 2022)

Contents

Figures

Tables

About this publication

This book provides instructions for installing and using Lenovo XClarity Integrator for VMware vCenter, *Version 7.7.0*.

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 you 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 you 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 you 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. You 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. You 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 your workloads or notify you. 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 you are using, choose 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)**
7.0 (U1, U2, U3)	X	√
6.7 (U1, U2, U3)	√	√
6.5 (U2, U3)	√	√
6.5 (U1)	√	X
6.5	√	X
6.0 and earlier versions	√	X

Note: If the version of your VMware vCenter is earlier than 6.5 (U2) or if you want to use LXCI with the vSphere Flex client, do not upgrade LXCI to version 6.0.0.

Supported versions of Lenovo XClarity Administrator

Table 3. Lenovo XClarity Administrator version support matrix

LXCA	**LXCI version**									
	5.5.0	**6.2.0**	**7.0.0**	**7.1.0**	**7.2.0**	**7.3.0**	**7.4.0**	**7.5.0**	**7.6.0**	**7.7.0**
3.6	X	X	X	X	X	X	X	X	√	√
3.5	X	X	X	X	X	X	X	√	√	√
3.4	X	X	X	X	X	X	√	√	√	√
3.3	X	X	X	X	X	√	√	√	√	√
3.2	X	X	X	X	√	√	√	√	√	√

Table 3. Lenovo XClarity Administrator version support matrix (continued)

LXCA	LXCI version									
	5.5.0	6.2.0	7.0.0	7.1.0	7.2.0	7.3.0	7.4.0	7.5.0	7.6.0	7.7.0
3.1	X	X	X	√	√	√	X	X	X	X
3.0	X	X	√	√	√	X	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.

- 7.0
- 6.7
- 6.5
- 6.0

You 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) • SR635 (7Y98, 7Y99)	• SR645 (7D2X, 7D2Y) • SR650 (7X05, 7X06) • SR650 V2 (7Z72, 7Z73) • SR655 (7Y00, 7Z01) • SR665 (7D2V, 7D2W) • SR670 V2 (7Z22, 7Z23) • SR850 (7X18, 7X19) • SR850 V2 (7D31,7D32,7D33) • SR850P (7D2F, 7D2G, 7D2H) • SR860 (7X69, 7X70) • SR860 V2 (7Z59, 7Z60, 7D42) • SR950 (7X12) • ST250 (7Y45, 7Y46) • ST250 V2 (7D8F, 7D8G, 7D8H) • ST258(7Y27) • ST550 (7X09, 7X10) • ST558 (7Y15, 7Y16) (China only) • ST650 V2 (7Z74, 7Z75, 7Z76)
ThinkServer	• SR588 V2 (7D53) • SR590 V2 (7D53)	• SR660 V2 (7D6L) • SR668 V2 (7D6L)
ThinkEdge	• SE450 (7D8T)	

Table 4. Supported Lenovo servers (continued)

Series	Server models	
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, 7D82) • ThinkAgile VX Series Appliance (7Y11, 7Y12, 7Y13, 7Y14, 7Y91, 7Y92, 7Y93, 7Y94, 7Z13, 7Z58, 7Z62, 7Z63) • ThinkAgile VX Series Certified Node (7Y92, 7Y93, 7Y94, 7Z12, 7Z58)
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)
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, SR645, SR650, SR650 V2, SR850P, SR950
- Only the following servers are supported for Hardware Topology:
  - ThinkAgile VX Series Appliance (7Y93, 7Y94)
  - Lenovo ThinkAgile VX Integrated System (7D43)
- 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 minimum 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 your 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 on your 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 7
- "Access between XClarity Integrator and managed devices" on page 7

Access to the XClarity Integrator servers

If the XClarity Integrator server and all managed devices are behind a firewall, and you intend to access those devices from a browser that is outside of the firewall, you must 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. If you 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 8.

Access between XClarity Integrator and managed devices

If managed devices (such as compute nodes or rack servers) are behind a firewall and if you intend to manage those devices from a XClarity Integrator server that is outside of that firewall, you must 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** • IPMI – TCP on port **623** [1] • 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 your 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

If you set proxy in vCenter and you intend to use vLCM function to update the firmware, you should allow the connection from vCenter to Lenovo XClarity Integrator (protocol HTTPS, port 443) in the proxy configuration of your 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 Web Client.

Step 1. Log in to the vSphere Web 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 your virtual server and click **Next**.

Note: Skip the settings displayed in the **IP Allocation Settings** section. You will configure the IP allocation settings 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 based on your needs by following the steps in "Configuring network access" on page 56, 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 53.

Step 16. Restart the vSphere Client service:

Note: This step is only applicable to the versions earlier than V7.0 of vCenter.

a. Log in to the shell console of your vCenter server.

b. Stop vsphere-ui service:
Run `service-control --stop vsphere-ui` and press **Enter**.

c. Remove the directory `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/com.lenovo.lxci-*.*` on your vCenter Server.

d. Restart vsphere-ui service:
Run `service-control --start vsphere-ui` and press **Enter**.

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

Procedure

You 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 39.

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

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

Upgrading Lenovo XClarity Integrator 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, first you need to get the update package. 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: If you are using Lenovo XClarity Integrator v5.0.2 or v5.1.0, you must 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. You can download the patch from the Lenovo XClarity Integrator for VMware Web site.

Procedure

Step 1. 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**, and select the files that you want to import. Ensure that you select all four files (.txt, .chg, .xml and .tgz). and then click **Open**. The selected files are listed in the Import dialog.

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.
- You can monitor the update progress from the virtual appliance's console in vSphere client or vCenter Web client.

Step 7. When the appliance's 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 you see `update finished` and there are no errors 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. Register Lenovo XClarity Integrator to VMware vCenter.

Step 9. Restart the vSphere Client service:

Note: This step is only applicable to the versions earlier than V7.0 of vCenter.

a. Log in to the shell console of your vCenter server.

b. Stop vsphere-ui service:
Run `service-control --stop vsphere-ui` and press **Enter**.

c. Remove the directory `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/com.lenovo.lxci-*.*` on your vCenter Server.

d. Restart vsphere-ui service:
Run `service-control --start vsphere-ui` and press **Enter**.

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. For more information, see "Backing up data" on page 59.
3. Deregister the plug-in from the vCenter. For more information, see "Configuring vCenter connections" on page 53.
4. Turn off the appliance from the vSphere Web Client and delete it from the inventory.
5. Stop the vSphere Web 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 Web Client service.

Chapter 3. Configuring Lenovo XClarity Integrator

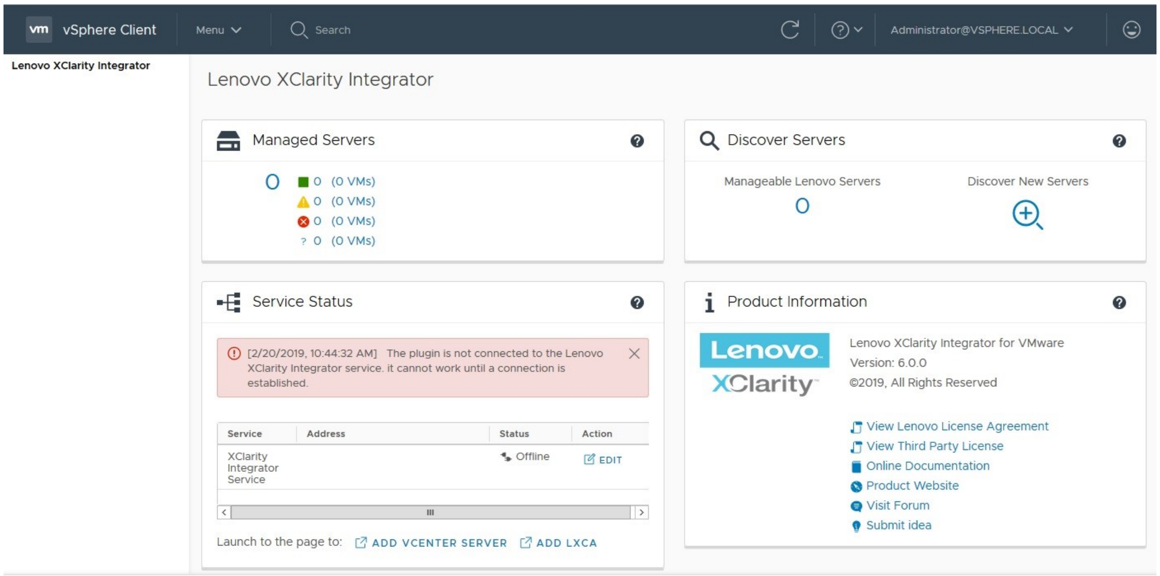
The topics in this section provide information about configuring the Lenovo XClarity Integrator on your server.

Configuring Lenovo XClarity Integrator server connection

Before you use Lenovo XClarity Integrator within the vSphere client, you must configure access to the Lenovo XClarity Integrator server.

Procedure

Step 1. From 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.



[2/20/2019, 10:44:32 AM] The plugin is not connected to the Lenovo XClarity Integrator service. it cannot work until a connection is established.

Service	Address	Status	Action
XClarity Integrator Service		Offline	EDIT

Lenovo XClarity Integrator for VMware
Version: 6.0.0
©2019, All Rights Reserved

- View Lenovo License Agreement
- View Third Party License
- Online Documentation
- Product Website
- Visit Forum
- Submit idea

Figure 1. Lenovo XClarity Integrator administration page

Step 2. In the **Service Status** section, locate **XClarity Integrator Service**, and click **EDIT**.

Step 3. Input values for the following parameters.

- **Host**: IP address or hostname of Lenovo XClarity Integrator virtual appliance.
- **User name and password**: credentials that you created when you deployed Lenovo XClarity Integrator.

Step 4. Click **OK** to display the connection status.

Note: If you change the host address or credentials of the Lenovo XClarity Integrator server, the plug-in disconnects with the Lenovo XClarity Integrator server. To resolve this issue, click **Edit Connection** and input a new IP address or new credentials.

Discovering and managing the BMC

You 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 your 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

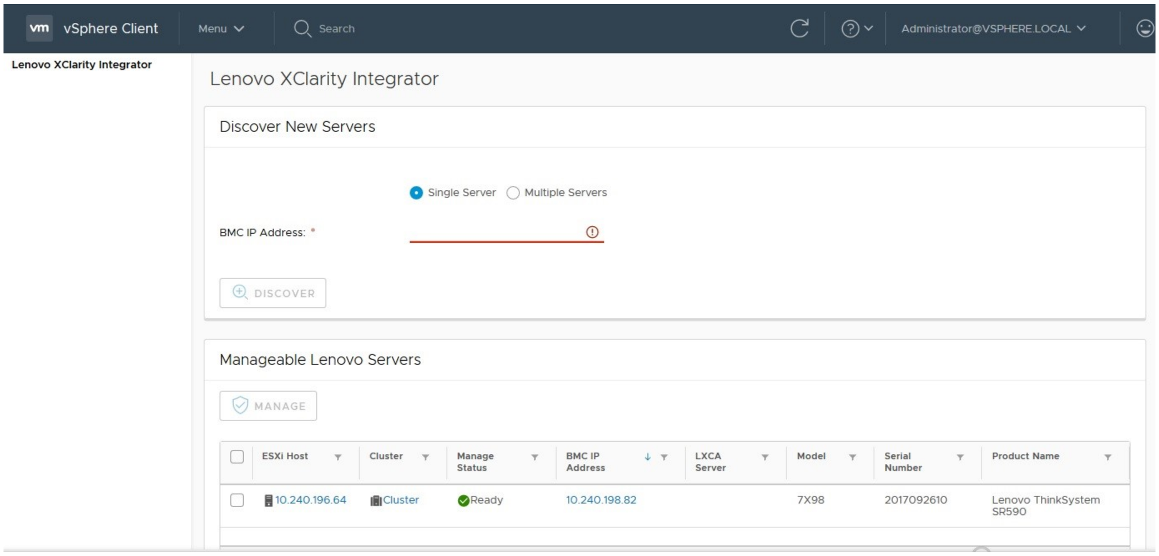
You can discover and manage the BMC directly by providing the BMC address and credential.

Procedure

To discover and manage the BMC directly, complete the following steps:

Step 1. From 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 **Discover servers** section, click **Discover New Servers**. The server discover page is displayed.



Lenovo XClarity Integrator

Discover New Servers

● Single Server ○ Multiple Servers

BMC IP Address: *

Manageable Lenovo Servers

□	ESXi Host	Cluster	Manage Status	BMC IP Address	LXCA Server	Model	Serial Number	Product Name
□	10.240.196.64	Cluster	Ready	10.240.198.82		7X98	2017092610	Lenovo ThinkSystem SR590

Figure 2. 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.

Note: It is recommended that an IP address range contains less than 60 IP addresses.

Step 4. Click **Discover**.
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 5. Select the server that you want to manage.
Only the servers that the management status is “Ready” are selectable. You can select multiple servers if they use the same BMC credential.

Step 6. Click **Manage**. A dialog box is displayed, requesting the BMC credential.

Step 7. Input the BMC user name and password and then 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.

Discovering and managing the BMC through LXCA

If Lenovo XClarity Administrator is available in your environment, and ESXi servers have already been managed by Lenovo XClarity Administrator, you do not need to discover or manage the servers in Lenovo XClarity Integrator. You 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 Lenovo XClarity Administrator to Lenovo XClarity Integrator, ensure that the LXCA account has the privilege to manage all the servers that you want to manage with Lenovo XClarity Integrator.

Configuring Lenovo XClarity Administrator

Lenovo XClarity Integrator provides an integrated method for managing your 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 you can manage servers in vSphere Web Client by using Lenovo XClarity Administrator functions, such as chassis map, configuration pattern, and firmware policy deployment.

Before you begin

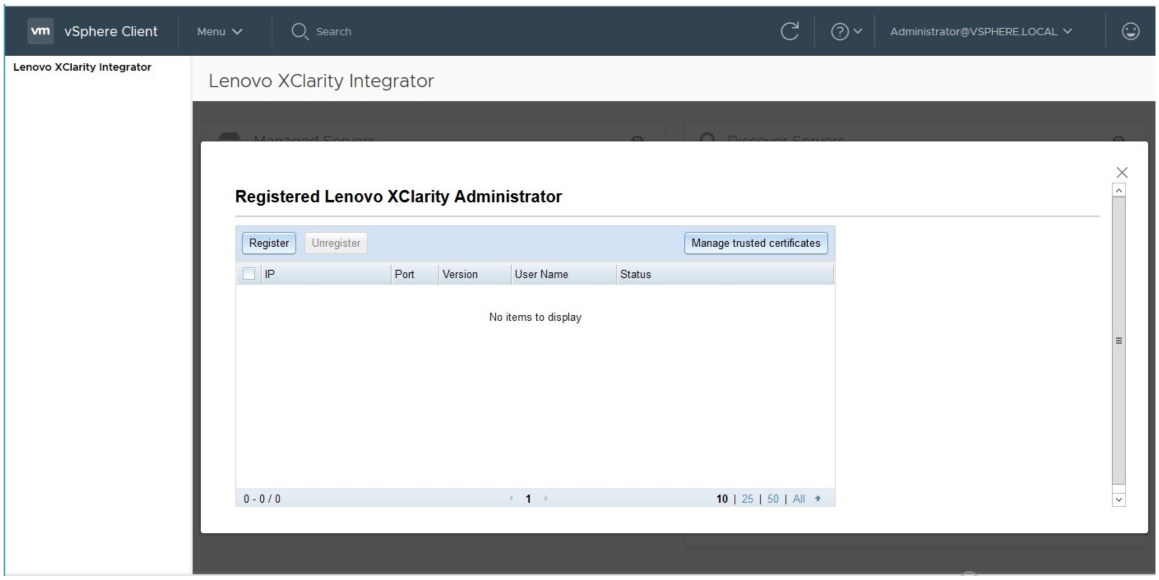
Before you register Lenovo XClarity Administrator to Lenovo XClarity Integrator, ensure the following:

- Lenovo XClarity Administrator is working in your environment.
- You have the *LenovoXClarityIntegrator.Administration* privileges.

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 LXCA**. The **Registered Lenovo XClarity Administrator** page is displayed.


vm vSphere Client
Menu
Search
Administrator@VSPHERE.LOCAL
Lenovo XClarity Integrator
Lenovo XClarity Integrator
Register
Unregister
Manage trusted certificates

Registered Lenovo XClarity Administrator

IP	Port	Version	User Name	Status

No items to display

0 - 0 / 0 1 10 | 25 | 50 | All

Figure 3. Registered Lenovo XClarity Administrator page

Step 3. Click **Register**. The Lenovo XClarity Administrator registration page is displayed.

Step 4. Input the hostname or the IP address of Lenovo XClarity Administrator, and do one of the following based on your needs:

- Select the **Use an existing account** check box, input the user name and the password, and click **OK**.

  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 the **Create a new account by connecting with this administrative account** check box, input the user name and the password, and click **OK**.

  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.

Step 5. If the **View Certificate** page is displayed, click **Trust this certificate** to confirm that Lenovo XClarity Administrator is trusted.

After the registration is completed, Lenovo XClarity Administrator is displayed on the LXCA Management page.

Notes:

- If Lenovo XClarity Administrator runs in only an IPv6 environment, manually download the server certificate for the Lenovo XClarity Administrator instance, and import it in to Lenovo XClarity Integrator by clicking **Manage trusted certificates → Add**; otherwise, Lenovo XClarity Administrator cannot be registered.

- If you have registered a Lenovo XClarity Administrator instance in Lenovo XClarity Integrator with the version v4.1.0 or earlier, manually download the server certificate for the Lenovo XClarity Administrator instance, and import it in to Lenovo XClarity Integrator by clicking **Manage trusted certificates → Add**. If the server certificate is not added to Lenovo XClarity Integrator, Lenovo XClarity Integrator cannot connect to Lenovo XClarity Administrator. You can also choose to un-register and then re-register the Lenovo XClarity Administrator to view and accept the server certificate instead.

What to do next

After completing the registration, you can perform these actions:

- Unregister Lenovo XClarity Administrator by clicking **Unregister**.
- Manage trusted certificates by clicking **Manage trusted certificates**.

Downloading the Lenovo XClarity Administrator server certificate

You can download a copy of the current Lenovo XClarity Administrator server certificate, in PEM format, to your local system.

Procedure

Complete the following steps to download the server certificate.

Step 1. Log in to Lenovo XClarity Administrator.

Step 2. From the Lenovo XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

Step 3. Click **Server Certificate** under the **Certificate Management**section. The **Server Certificate** page is displayed.

Step 4. Click the **Download Certificate** tab.

Step 5. Click **Download Certificate**. The Server Certificate dialog is displayed.

Step 6. Click **Save to pem** to save the server certificate as a PEM file on your local system.

Note: DER format is not supported.

Managing trusted certificates

Lenovo XClarity Integrator provides an integrated method for managing the trusted Lenovo XClarity Administrator certificates.

Procedure

From the Lenovo XClarity Integrator Administration page, click **Manage trusted certificates** to display the **Trusted Certificates** page. From this page you can perform the following actions:

- Manually add a trusted Lenovo XClarity Administrator certificate by clicking **Add**.
- View detail information for of a trusted certificate by clicking **View**.
- Delete a trusted certificate by clicking **Delete**.
- Update the trusted certificates list by clicking **Refresh**.
- Return to the Lenovo XClarity Integrator Administration page. by clicking **LXCA Registration**.

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 your 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 you use some functions such as firmware update, chassis map, and system settings. In this case, you need to download Lenovo XClarity Integrator root certificate and import it into your Web browser's list of trusted certificates or add it into security exceptions depending on the browser you are using.

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 on which you installed Lenovo XClarity Integrator.
3. Click **Get Certificate**.
4. Click **Confirm Security Exception**, and then refresh your browser.

Chapter 4. Viewing a summary of your 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.

You can select one of the following four sections on the dashboard based on your needs:

- **Discover Servers**. Refer to "Discover Servers section" on page 23.
- **Managed Servers**. Refer to "Managed Servers section" on page 23.
- **Service Status**. Refer to "Service Status section" on page 24.
- **Product Information**. Refer to "Product Information section" on page 24.

Discover Servers section

This section enables you to view the amount of manageable Lenovo servers. You 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 you to view the amount of managed Lenovo servers and the amount of virtual machines on these servers grouped by server status. You 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 based on your needs:

- 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. You 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 your XClarity Integrator have been registered. You can click **EDIT** to enter the Lenovo XClarity Integrator for VMware vCenter administrator Web page. For more information, see "Configuring vCenter connections" on page 53.
- XClarity Administrator

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

Product Information section

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

You 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:

- VMware vCenter Server has an out-of-band (OOB) network connection with the BMC of the managed ESXi servers.
- You 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 "Configuring Lenovo XClarity Administrator" on page 17).
  - 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** based on your needs:

- 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** based on your needs:

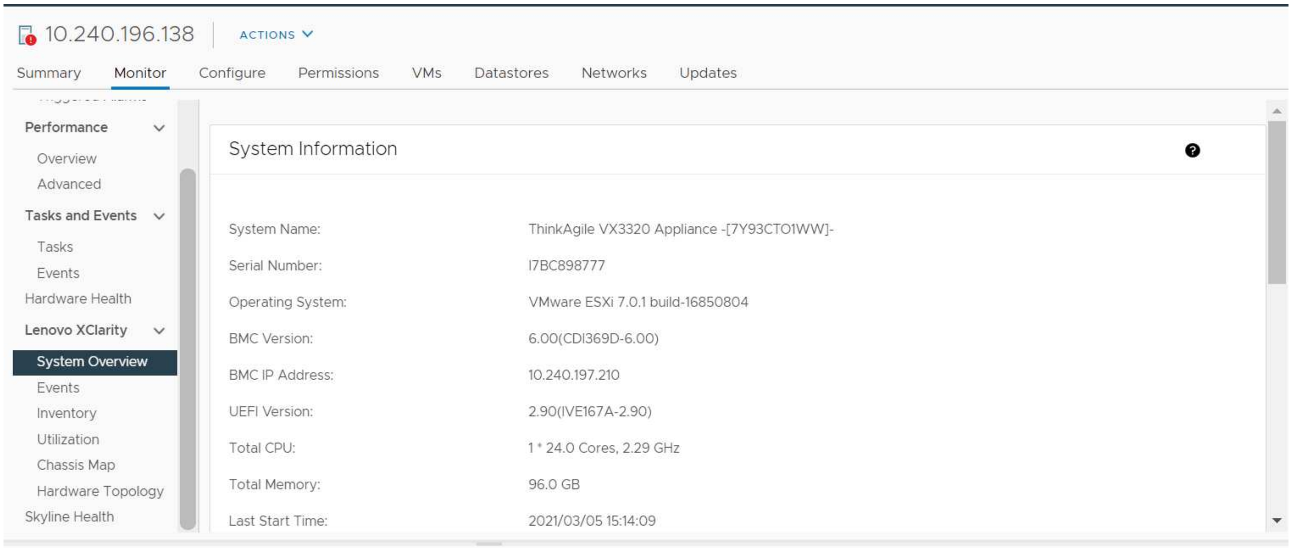
- Firmware Updates
- Power Policy
- Configuration

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 based on your needs:

- Launch Remote Console
- Launch BMC Interface

Viewing system information

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



System Information

System Name:	ThinkAgile VX3320 Appliance -[7Y93CTO1WW]-
Serial Number:	I7BC898777
Operating System:	VMware ESXi 7.0.1 build-16850804
BMC Version:	6.00(CDI369D-6.00)
BMC IP Address:	10.240.197.210
UEFI Version:	2.90(IVE167A-2.90)
Total CPU:	1 * 24.0 Cores, 2.29 GHz
Total Memory:	96.0 GB
Last Start Time:	2021/03/05 15:14:09

Figure 4. 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

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

The following icons indicate the severity of each event.

- ✖ : Critical
- ⚠ : Warning
- ℹ : Informational

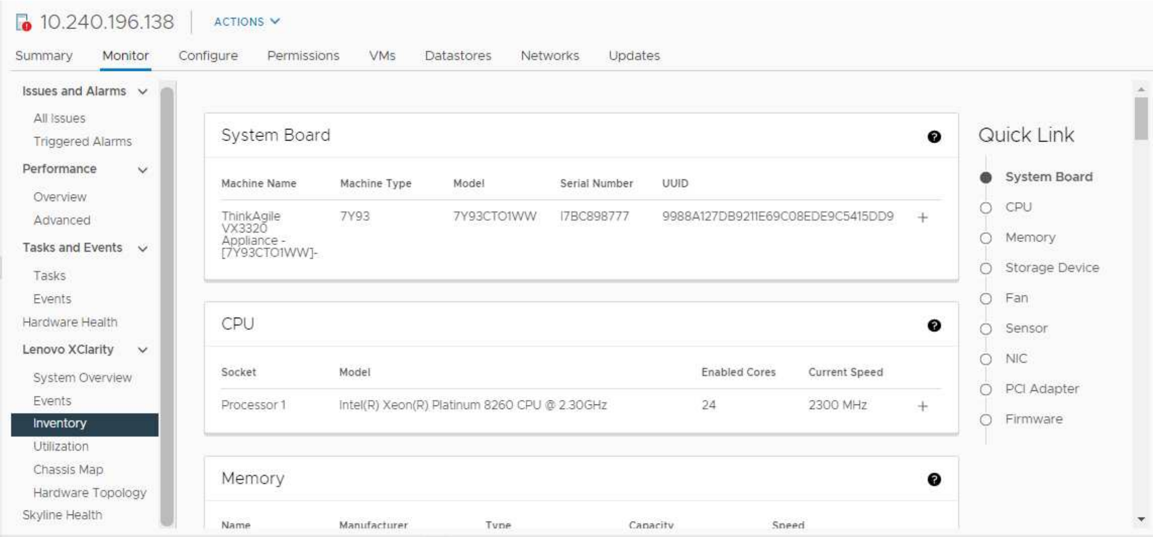
On this page, you can perform the following operations:

- 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. You 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 section you want to view. In a specific section, click the + sign to view the details.



System Board

Machine Name	Machine Type	Model	Serial Number	UUID	
ThinkAgile VX3320 Appliance - [7Y93CTO1WW]-	7Y93	7Y93CTO1WW	I7BC898777	9988A127DB9211E69C08EDE9C5415DD9	+

CPU

Socket	Model	Enabled Cores	Current Speed	
Processor 1	Intel(R) Xeon(R) Platinum 8260 CPU @ 2.30GHz	24	2300 MHz	+

Memory

Name	Manufacturer	Type	Capacity	Speed

Figure 5. 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.

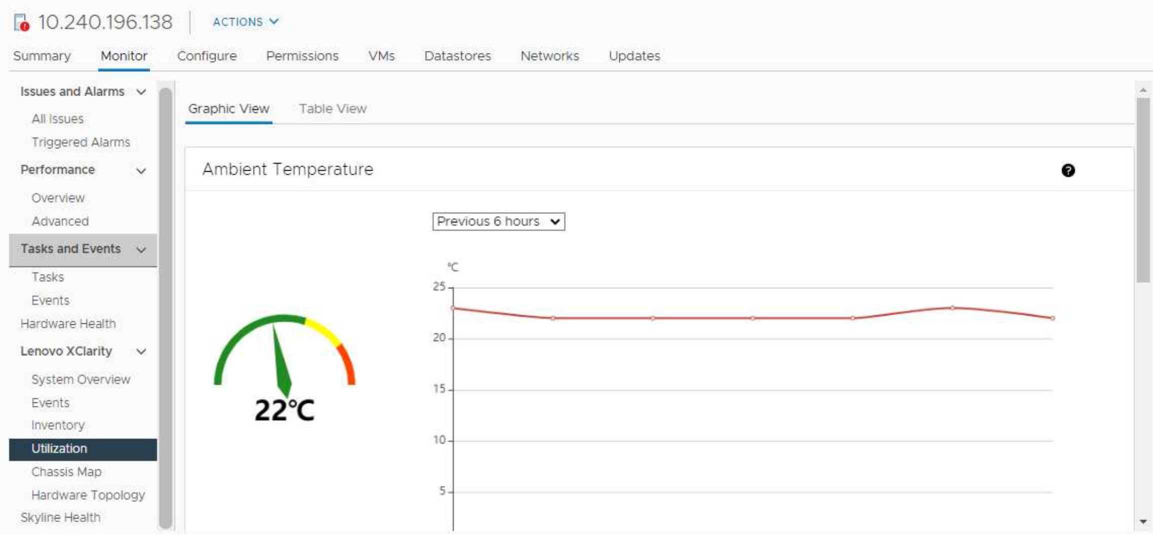


Figure 6. Utilization page

	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. From this interface, you can 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.

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 based on your needs:
   - To view the general host information, refer to "Viewing general host information" on page 28.
   - To view vSAN disk information, refer to "Viewing vSAN disk information" on page 29.
   - To view power supply information, refer to "Viewing health status of power supply units (PSU)" on page 30.
   - To remove a vSAN disk, refer to "Removing a vSAN disk" on page 30.
   - To replace a vSAN dis, refer to "Replacing a vSAN disk" on page 31.

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
  - ID: Location LED state
  - !: Fault LED state.
- **Hardware Health**
  - Normal
  - Warning
  - Critical

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

Actions

On the right of this pane, you can also click **VIEW ACTIONS** and **HOST ACTIONS**:

- Under **VIEW ACTIONS**:
  - **View Detail Inventory**: Click it to access the **Inventory** page.

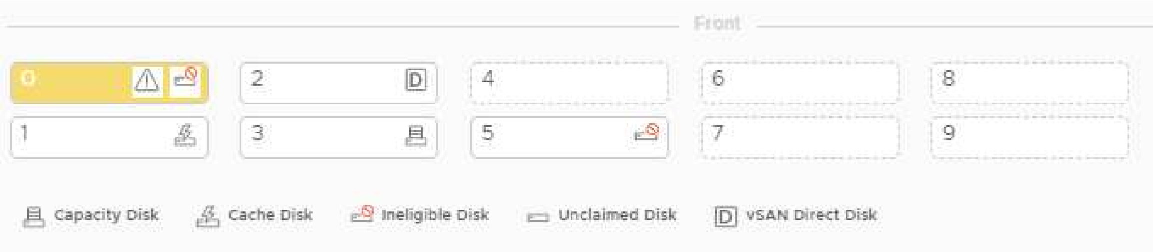
- **View Reference Photo**: Click it to access the product reference page. This page displays the actual front and rear views of this machine and directs you to access the product guide on Lenovo Press.
- **Refresh Hardware Topology**: Click it to update the hardware topology information.

- 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 7. Hardware topology



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

The hardware topology illustrates:

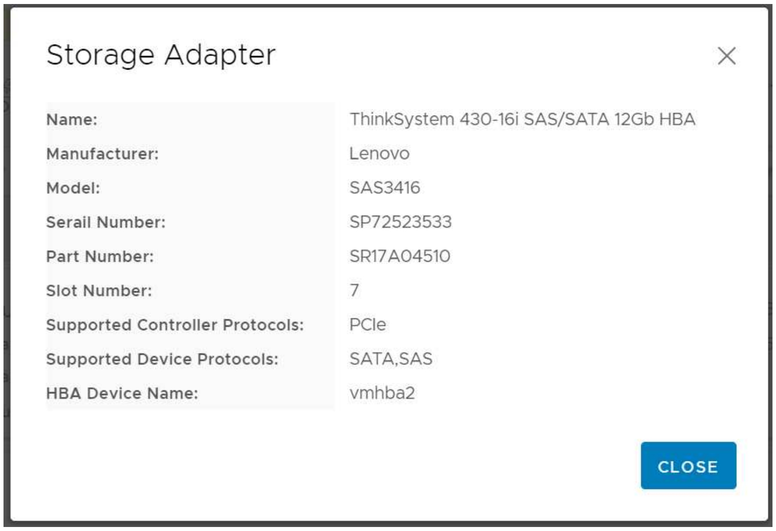
- Disk location: The slot without any disk installed is displayed with dotted lines.
- Disk status: Different colors indicate different disk status:
  - White: Normal state
  - Yellow: Warning state
  - Red: Critical state
- Disk type: The disk type icons of capacity disk, cache disk, ineligible disk,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

You 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 you 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: You can click the controller name to view more details.

Figure 8. Controller details



Storage Adapter

Name:	ThinkSystem 430-16i SAS/SATA 12Gb HBA
Manufacturer:	Lenovo
Model:	SAS3416
Serail Number:	SP72523533
Part Number:	SR17A04510
Slot Number:	7
Supported Controller Protocols:	PCIe
Supported Device Protocols:	SATA,SAS
HBA Device Name:	vmhba2

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.

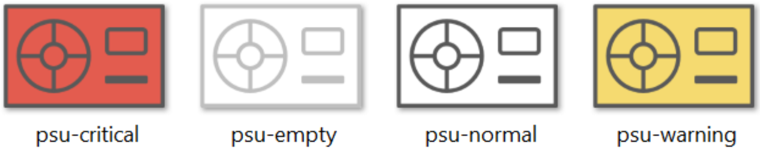


Figure 9. Health status of PSU

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:

- 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, you 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. You 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.

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. You 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.

Note: If the cache disk or the last capacity disk is removed from the disk group, the entire disk group will be removed, and **Auto Claim New Disk** will be disabled. When necessary, you should re-create the disk group manually.

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

Cluster hardware topology

The cluster hardware topology allows you 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. You 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 28.
- To change LED status, launch BMC interface, or launch remote contole, click **HOST ACTIONS**. For more information, refer to: "Actions" on page 28.

Launching the BMC Web interface

You 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

You can launch a remote-control session for a managed server and perform operations on this server as if you were 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 your Web browser. The remote-control session for the server is launched.

Working with the Firmware Updates function

The Firmware Updates function enables you to obtain and deploy UpdateXpress System Pack (UXSP) or individual firmware updates to the current ESXi server that you are operating against.

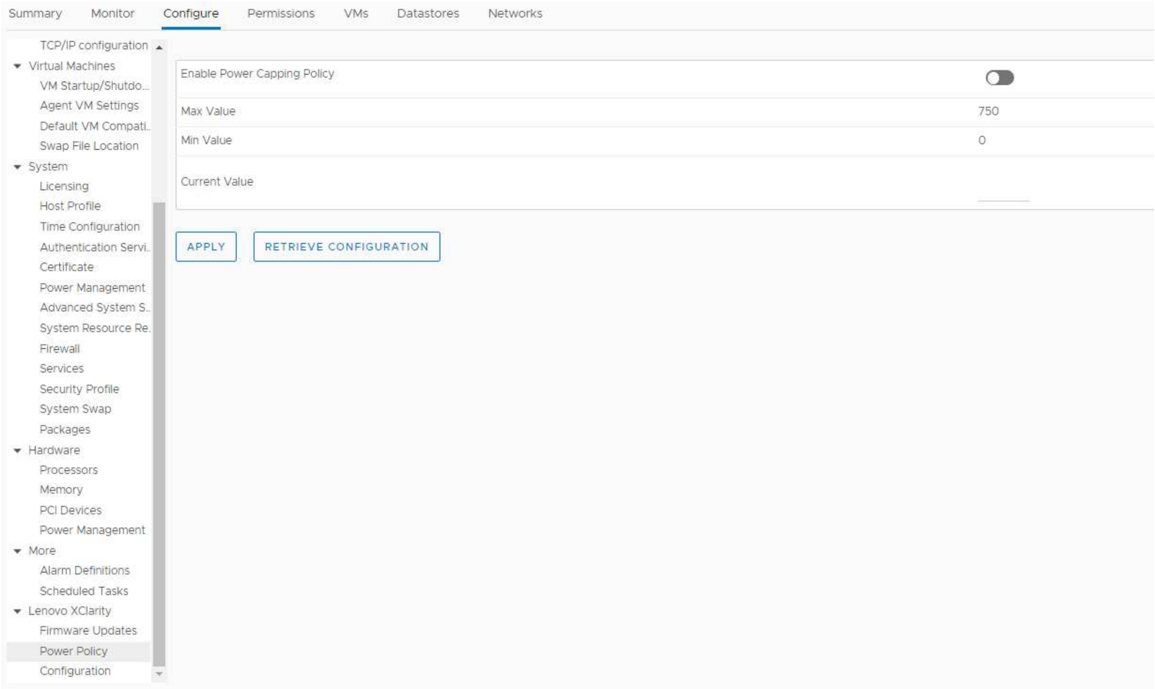
Updating a single ESXi server is similar with updating servers by using the Rolling System Update function. The only difference is that when you create an update task, the current ESXi is shown and can be selected. For more information about how to update preferences and manage update tasks, see "Working with the Rolling System Update function" on page 41.

Working with the Power Policy function

The Power Policy function enables you 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 you 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.



Enable Power Capping Policy	○
Max Value	750
Min Value	0
Current Value	

Figure 10. Power Policy configuration page

Working with the System Settings function

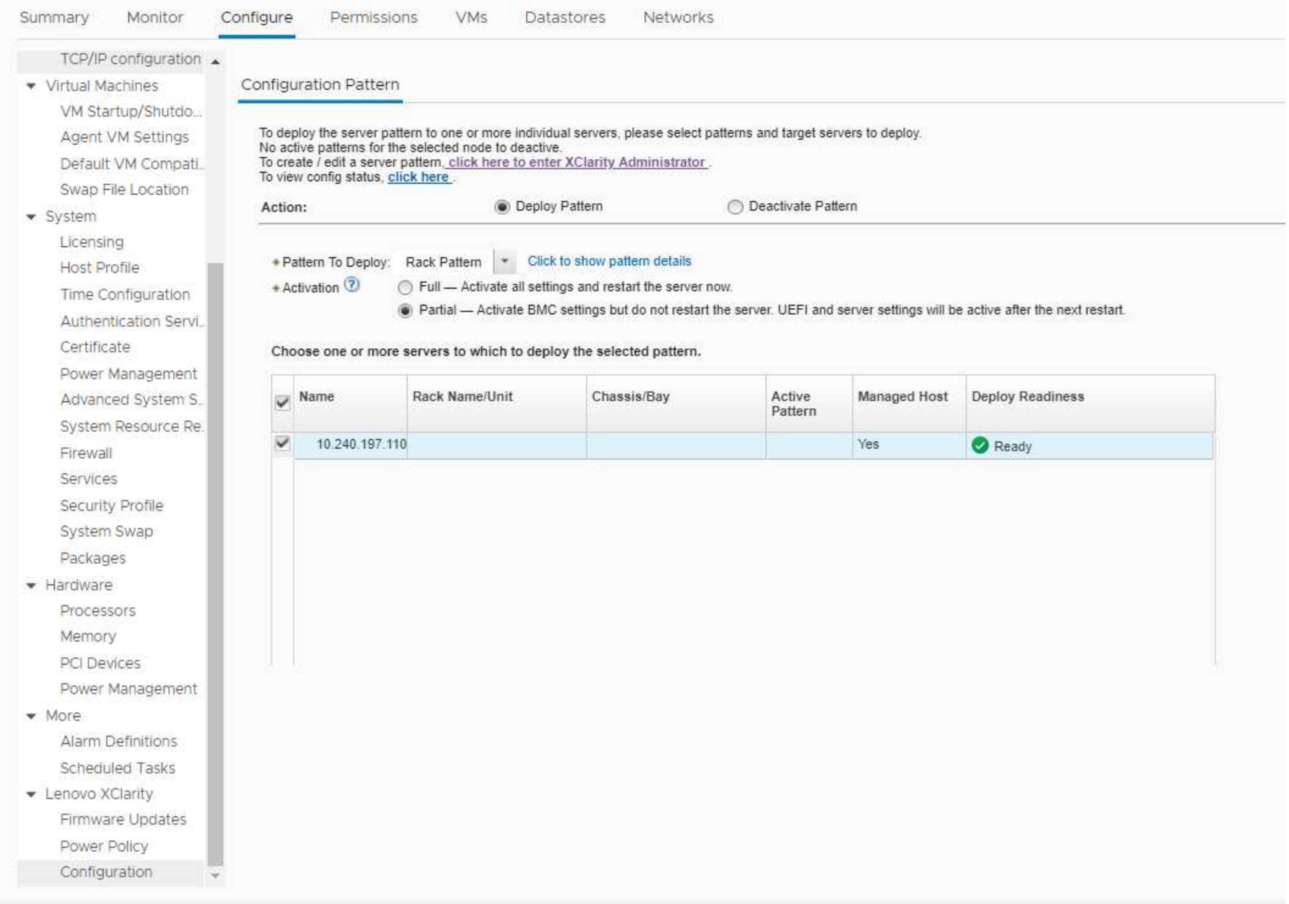
The System settings function enables you to manage the system settings of a host. If the server is managed by Lenovo XClarity Administrator, and Lenovo XClarity Administrator is registered in this Lenovo XClarity Integrator, you can deploy a configuration pattern to the host; otherwise you can only view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

Deploying a configuration pattern on a server

After you have registered the Lenovo XClarity Administrator in Lenovo XClarity Integrator, you 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, you can create server patterns by clicking the link to open Lenovo XClarity Administrator. This task is performed on the **Configuration Pattern** page.



To deploy the server pattern to one or more individual servers, please select patterns and target servers to deploy.
No active patterns for the selected node to deactive.
To create / edit a server pattern, click here to enter XClarity Administrator .
To view config status, click here .

Action: ● Deploy Pattern ○ Deactivate Pattern

* Pattern To Deploy: Rack Pattern

* Activation ○ Full — Activate all settings and restart the server now.
● Partial — Activate BMC settings but do not restart the server. UEFI and server settings will be active after the next restart.

Choose one or more servers to which to deploy the selected pattern.

☑	Name	Rack Name/Unit	Chassis/Bay	Active Pattern	Managed Host	Deploy Readiness
☑	10.240.197.110				Yes	✓ Ready

Figure 11. Configuration Pattern page

Procedure

Step 1. Click **Configure → Lenovo XClarity → Configuration**. The **Configuration Pattern** page is displayed.

Step 2. Select one of the following actions:

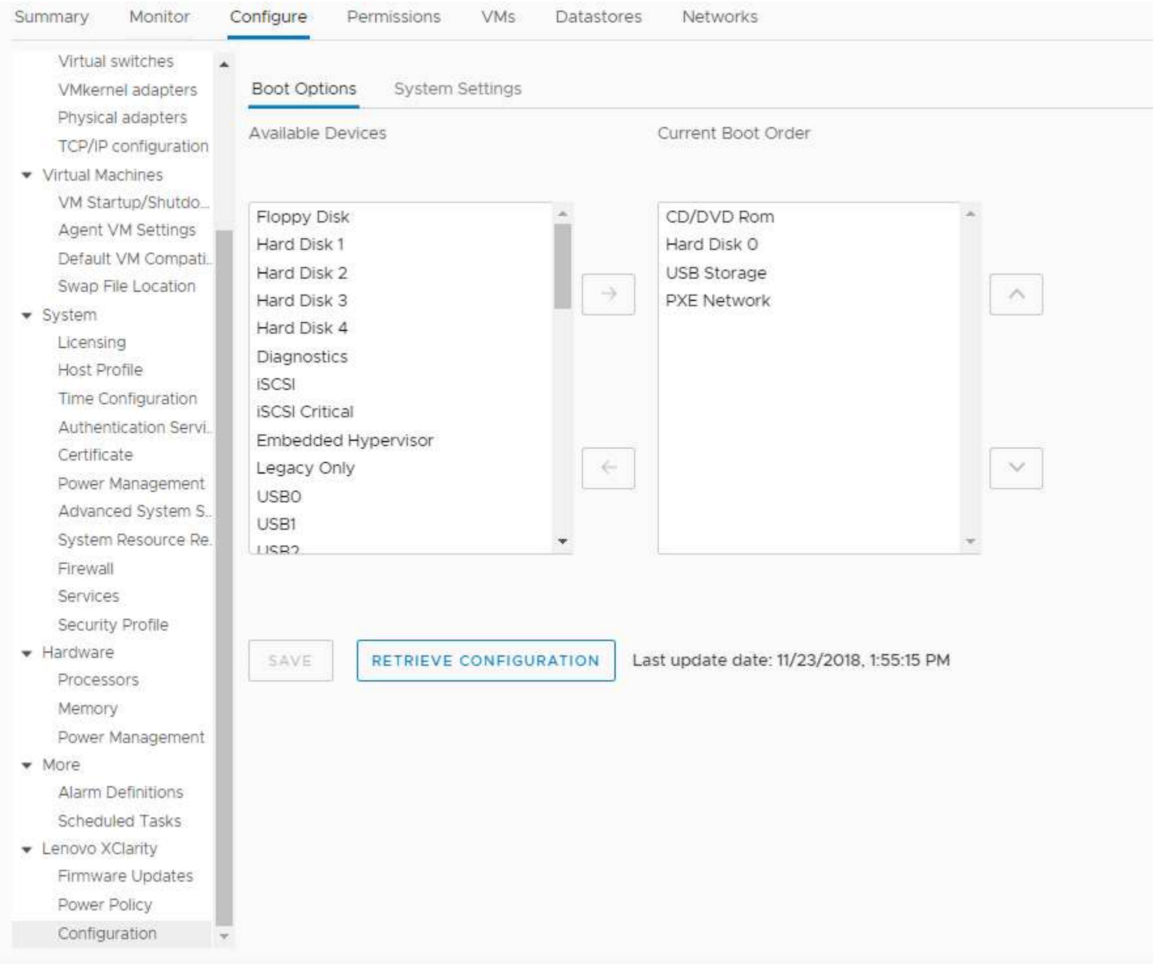
- **Deploy pattern**. Deploys the selected pattern to your servers.
- **Deactivate pattern**. Deactivates the pattern from your servers.

Step 3. Select a predefined pattern and apply it to your server.

Working with the Boot Options function

On the **Boot Options** pane, the left column displays the optional devices and the right column displays the current boot order. To change the order, you can move a boot order option up, or down, or between the two columns, by clicking the corresponding arrow buttons.

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 you have made any changes.



Available Devices

Floppy Disk
Hard Disk 1
Hard Disk 2
Hard Disk 3
Hard Disk 4
Diagnostics
iSCSI
iSCSI Critical
Embedded Hypervisor
Legacy Only
USB0
USB1
USB2

Current Boot Order

CD/DVD Rom
Hard Disk 0
USB Storage
PXE Network

Last update date: 11/23/2018, 1:55:15 PM

Figure 12. Boot Options pane

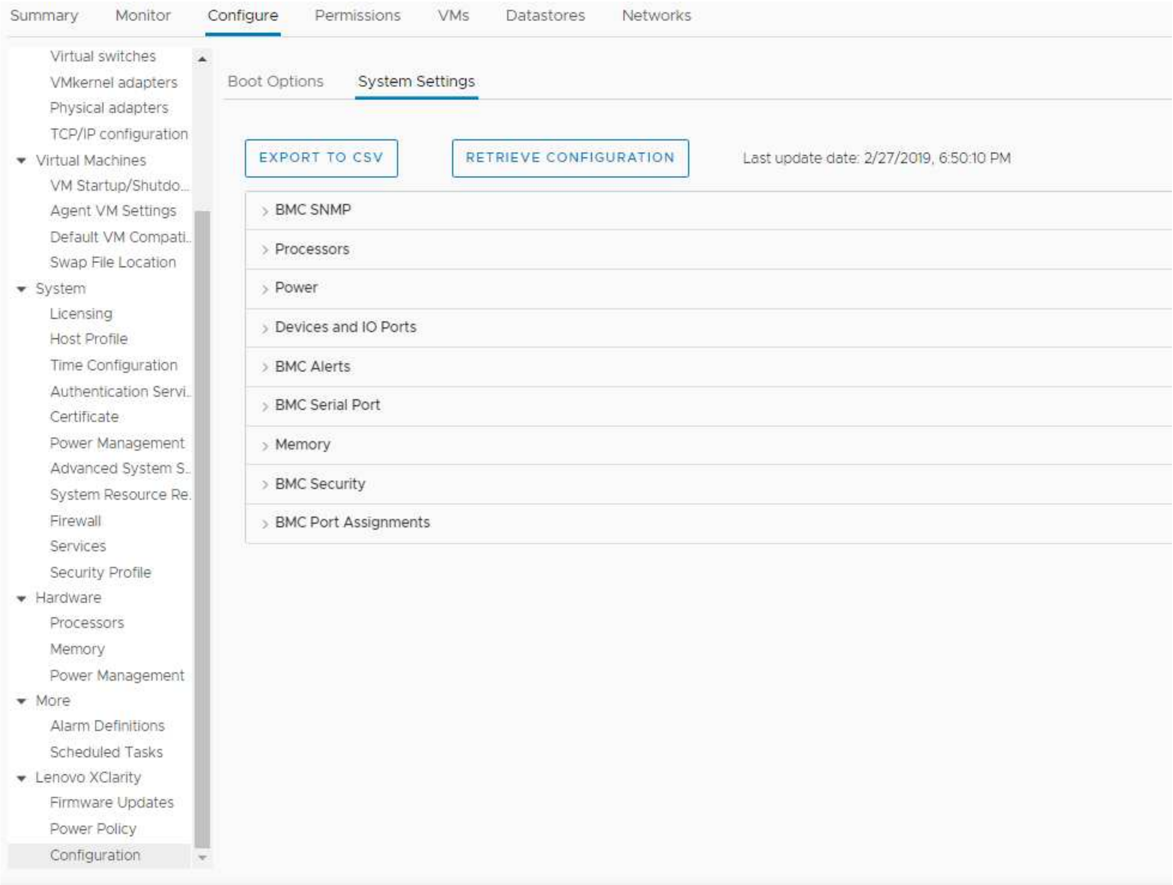
Viewing and exporting system settings

You can view and export the system settings of your 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.



Last update date: 2/27/2019, 6:50:10 PM

Figure 13. System Settings pane

Step 2. Do one of the followings based on your needs:

- 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** based on your needs:

- **Rolling Update**
- **Rolling Reboot**

Working with 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 10.

Importing base ESXi and Lenovo addons

You 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. You can download Lenovo custom ESXi image from https://vmware.lenovo.com/content/custom_iso.

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

Managing firmware packages

You 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 of the following based on your needs:

- To download the required firmware package, select the firmware package from the list, and click **DOWNLOAD**.

- 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 delete the firmware package, select the required firmware package and click **DELETE**.
- To copy the firmware package for customization, select the 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.

  Note: 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**.

Managing the cluster through an image

You 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

You 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.
- 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, you can 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

You 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

You 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.

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.

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.

Procedure

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

Step 2. On the left navigation pane, click **Rolling Update** under **Lenovo XClarity**.

Configuring the Rolling System Update preferences

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

Specify the update repository location

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

Procedure

Step 1. On the left navigation pane, click **Rolling Update** under **Lenovo XClarity**. 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 based on your needs.

- 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. If you accept the default settings, leave it as it is.
- If you want to use an external folder as the firmware repository, click **EDIT** on the right in the **Repository folder** section. In the displayed **Repository Settings** page, select **Use Remote Repository**, enter the network address of the repository in the format of \\<*IP_address*>\<*repository_path*>, and enter the user name and password if required. Then, click **OK** to save the changes.

  Notes:

  - For repository setup on a host using IPv6 addresses, you must specify the network address using the fully qualified domain name (FQDN).
  - The write permission of the shared folder must be granted.
  - Lenovo XClarity Integrator 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. On the Preferences pane, click **EDIT** on the right of **Download metadata from the Lenovo website** to configure the update package download settings.

a. If the Lenovo XClarity Integrator 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. Based on your needs, select **Download from website** and set the frequency for automatically and periodically downloading the update packages.

Step 4. If needed, 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.
- You can cancel the pagekage download process at anytime by clicking **CANCEL**.

- The time of the lastest download is displayed on the bottom left corner of the pane.

Creating a Rolling System Update task

You can create an update task and schedule the host firmware update at a planned time period.

About this task

You can update the host firmware with or without a policy.

- **Update with a policy**

  To ensure that the firmware on the server are compliant, you can create firmware-compliance policies, and apply the policies to the managed servers. 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.

- **Update without a policy**

  If Lenovo XClarity Administrator is not available in your environment, select the individual firmware updates or UXSP for each server. Before the update, ensured that:

  – Baseboard Management Controller (BMC) access is granted.

  – The update repository is configured, and the firmware are downloaded (see "Configuring the Rolling System Update preferences" on page 42).

Procedure

Complete the following steps to create the Rolling System Update task:

Step 1. On the **Task Manager** page, click **Create** to launch the create task wizard.

Step 2. Input a task name, select one of the following task types based on your needs, and click **Next**.

- **Update with Policy**
- **Update without Policy**

Notes:

- Ensure that the task type you selected meet the corresponding requirements of **Update with Policy** or **Update without Policy** before update.
- Non-ascii characters cannot be used in task name.

Step 3. Do one of the following based on your needs, and click **Next**.

- If **Update with Policy** is selected, select an available firmware policy from the **Policy** drop-down list for each host. If necessary, check the firmware version defined in the policy and customize firmware selection.
- If **Update without Policy** is selected, select the firmware for each host that you want to update.

Step 4. Select one or more than one of the following update options based on your needs, and click **Next**.

- **Update Parallelization**: Specifies how many hosts to be updated at the same time.

  Notes:

  – If there is only one Rolling System Update task, ensure that the quantity of the specified host does not exceed eight.

  - If there is more than one Rolling System Update task, ensure that the quantity of the specified host for all tasks does not exceed eight.

- **Perform VM Evacuation**: Specifies whether to migrate the virtual machines before updating the host. For the vSAN cluster, you can also select **Decommission Mode** from the drop-down list.
- **Reboot after Update**: Specifies whether to restart the after updating firmware. This option is only visible when creating an update without policy.

  The operating system shall be restarted when updating some adapters. In this case, this option is selected automatically and cannot be canceled.
- **Stop On Error**: Specifies whether to stop the whole update task when the update for one host in the cluster fails.
- **Schedule**: Schedules the task to run at a planned time period.

Step 5. Check the task summary if necessary, and click **Save**.

Managing Rolling System Update tasks

You can use the Rolling System Update function to manage rolling update tasks.

About this task

The Rolling System Update function provides a task manager for managing rolling-update tasks. A task contains all of the information and options for a rolling update.

You can perform the following tasks using the task manager:

- Create a Rolling System Update task. Each cluster can have only one active task.
- Edit a Rolling System Update task that has not started.
- Copy a Rolling System Update task that has completed.
- Remove a Rolling System Update task from task list.
- Cancel a Rolling System Update task that is running.
- View Rolling System Update tasks status.

Procedure

Step 1. Click **Rolling Update** under **Lenovo XClarity** on the left pane . The **Task Manager** page is displayed on the right pane.

Step 2. Perform one of the following steps:

- Create a task
- Copy a task
- Edit a task
- Remove a task
- Cancel a task
- Refresh the task list from the page

If you click **Create** or **Edit**, you can use the Create/Edit Task wizard to create or edit a task.

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.
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.

Table 12. Rolling System Update *task status (continued)*

Target	Status	Description
	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.

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 enables you 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 a cluster from the inventory tree and click the **Configure** tab.

Step 2. On the left navigation pane, click **Rolling Reboot** under **Lenovo XClarity**.

The task table provides the following detailed information about an RSR task:

- Task Name
- Status
- Progress
- Start Time
- End Time

Table 13. Rolling System Reboot task functions

Task function	Description
Create	Creates a new RSR task.
Copy	Create a new RSR task from an existing RSR task.
Edit	Edit an RSR task that has not been started.

Table 13. Rolling System Reboot task functions (continued)

Task function	Description
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

Select **Configure → Lenovo XClarity → Rolling Reboot** and complete the following steps.

Step 1. Click **Create** to open the Rolling System Reboot wizard. The **Create** button is enabled only if a task has a status of Finished, Canceled, or Failed in the task list. The **Name and Type** page is displayed.

Step 2. Enter a name for the task you are creating in the **Task Name** field and select the hosts you want to restart.

Step 3. Click **Next**. The restart options and screen is displayed.

Parallelization

The default is 1.

Specifies the number of hosts that can be restarted concurrently.

Rebooting multiple hosts concurrently requires more system resources.

You should carefully set the value according to the current available system resources; such as CPU and memory on the vCenter Server.

Perform VM Evacuation

This option is only visible in the vSAN cluster, you can specify decommission mode when migrating VMs.

Stop On Error

Specifies whether to stop the whole task when failing to restart the host.

Schedule

Specifies a time to initiate the task.

Step 4. Click **Next**. The **Summary** page is displayed.

Step 5. Click **Finish** to save the task. RSR initiates the task according to the schedule.

Editing a not-started RSR task

Use the **Edit** Rolling System Reboot (RSR) option to make changes to a task that has not started and has a task type of *Reboot Only*. Only editing a not-started task is supported.

Procedure

Select **Configure → Lenovo XClarity → Rolling Reboot** and complete the following steps.

Step 1. Select a not-started RSR task in the list and click **Edit**. The Rolling System Reboot wizard opens. The machine type and hosts are listed.

Step 2. Edit the task and then click **Finish** to save changes.

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

Select **Configure → Lenovo XClarity → Rolling Reboot** and complete the following steps.

Step 1. Select one or more RSR tasks that are not currently running, from the list.

Step 2. 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

Select **Configure → Lenovo XClarity → Rolling Reboot** and complete the following steps.

Step 1. Select a running RSR task from the list.

Step 2. Click **Cancel**. RSR completes updating the host that has started and only cancels the others. This task may take several minutes to complete.

Cloning a completed RSR task

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

Procedure

Select **Lenovo XClarity Integrator → Rolling System Reboot → Task Manager** and complete the following steps.

Step 1. Select a finished, failed or canceled RSR task from the list.

Step 2. Click **Copy** to open the Rolling System Reboot wizard.

Step 3. Edit the original selection and click **Finish** to save the new task.

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 46.

Table 14. Rolling System Reboot task status

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

Table 14. Rolling System Reboot task status (continued)

Target	Status	Description
	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 that you have requested BMC access for each host in the cluster; otherwise, Lenovo Proactive HA provider might not display correctly.

If the same host with BMC access was previously deleted and added back, you must 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 Web 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 you can select the events and hosts for ignoring failure conditions. For more information, see the VMware vSphere user guide.

Note: According to VMware you can use other automation level and remediation settings, but there are some limitations. For example, if you 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 was previously deleted and added back, you must request BMC access again even if the user interface indicates that the host can access the BMC. Otherwise, you cannot move the host to the Proactive HA enabled cluster.

Re-using Lenovo Proactive HA Provider

The Lenovo Proactive HA provider is automatically registered in VMware vCenter when you register Lenovo XClarity Integrator in VMware vCenter, either in the wizard or administration page. When you deregister Lenovo XClarity Integrator from VMware vCenter, you are asked whether you want to also deregister Proactive HA provider. Normally you can keep the provider in VMware vCenter so that it can be reused the next time you register 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 you see "Provider com.lenovo.HealthUpdateProvider_ver101 has not posted an update in 300 seconds" in the event list of Proactive HA enabled cluster, the heartbeat may 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 Web Client. This provides administrators with a single, heterogeneous view of all host system events within the managed environment.

Procedure

Complete the following prerequisite steps to assist you with managing hardware events.

Step 1. On the **Cluster overview** page, find the BMCs and request BMC access to ensure that the vCenter server has an out-of-band (OOB) network connection with the BMC managed ESXi servers.

Step 2. Enable TCP on the https port that you selected for Lenovo XClarity Integrator for VMware vCenter. The default is 9500 when you install Lenovo XClarity Integrator for VMware. Lenovo XClarity Integrator for VMware vCenter listens on this port for incoming indications.

What to do next

Select the **Events** tab in vSphere Web 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 Web Client window along the toolbar above the vSphere Web 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. You can register Lenovo XClarity Integrator for VMware vCenter to additional vCenter servers. You also can unregister Lenovo XClarity Integrator for VMware vCenter from a vCenter server.

Registering Lenovo XClarity Integrator to vCenter server

You 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 you use a dedicated service user, 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.

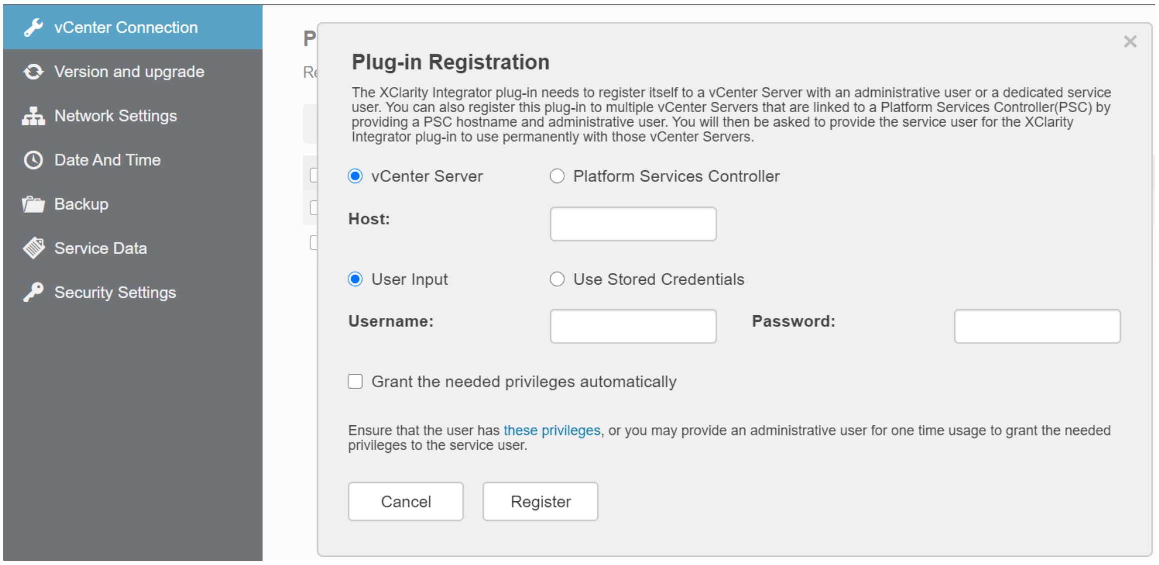
Registering LXCI to one vCenter server

You 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.



Plug-in Registration

The XClarity Integrator plug-in needs to register itself to a vCenter Server with an administrative user or a dedicated service user. You can also register this plug-in to multiple vCenter Servers that are linked to a Platform Services Controller(PSC) by providing a PSC hostname and administrative user. You will then be asked to provide the service user for the XClarity Integrator plug-in to use permanently with those vCenter Servers.

● vCenter Server ○ Platform Services Controller

Host:

● User Input ○ Use Stored Credentials

Username: **Password:**

□ Grant the needed privileges automatically

Ensure that the user has these privileges, or you may provide an administrative user for one time usage to grant the needed privileges to the service user.

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 based on your needs:

- 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

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

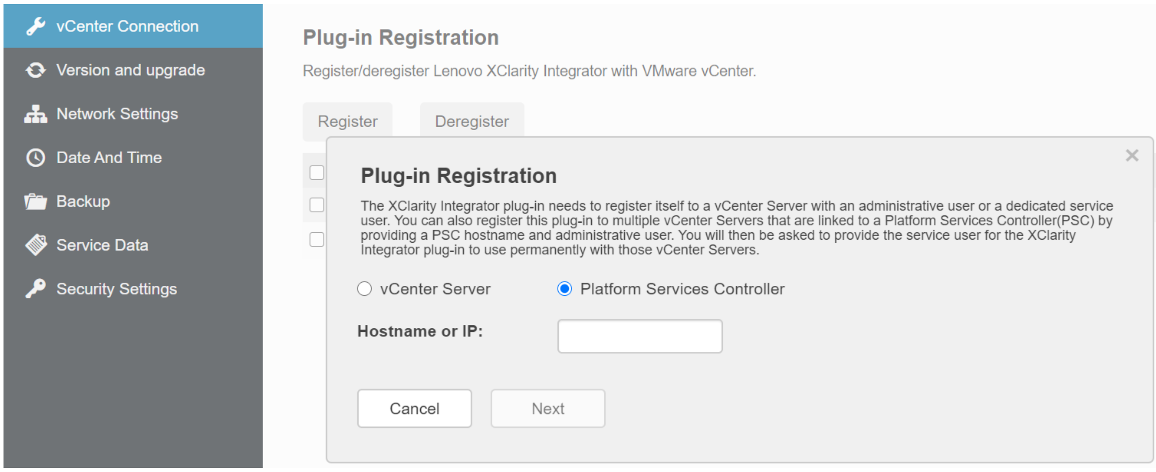
Procedure

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 you input the FQDN, ensure that the DNS is configured on the **Network Settings** page.



Plug-in Registration

Register/deregister Lenovo XClarity Integrator with VMware vCenter.

Plug-in Registration

The XClarity Integrator plug-in needs to register itself to a vCenter Server with an administrative user or a dedicated service user. You can also register this plug-in to multiple vCenter Servers that are linked to a Platform Services Controller(PSC) by providing a PSC hostname and administrative user. You will then be asked to provide the service user for the XClarity Integrator plug-in to use permanently with those vCenter Servers.

○ vCenter Server ● Platform Services Controller

Hostname or IP:

Step 3. From the **Host** list, select the vCenter servers that you want to register to, and click **Next**.

Step 4. Do one of the following based on your needs:

- 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 vCenter servers you selected.
- 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

You can unregister Lenovo XClarity Integrator from vCenter server.

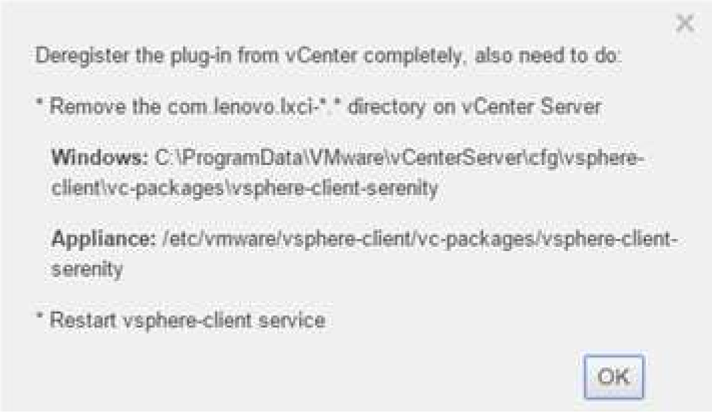
Procedure

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 that you want 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

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

Step 5. Restart the “vsphere-client” service.

Updating management server software

On this setting page, you 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.

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, you 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. You 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.

Unless you have strong reason, you should not change network settings after they are set in the wizard. If you must change the network settings, perform the following steps to reconfigure the virtual appliance.

Attention: If you change the settings incorrectly, you might lose connection to the virtual appliance.

1. Regenerate the server certificate (see “Working with security certificates” on page 64).
2. Unregister vCenter and re-register again (see “Configuring vCenter connections” on page 53.
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

You 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. If you 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.
- If you use the hostname to connect vCenter and vCenter managed EXSi hosts, you must configure a DNS for Lenovo XClarity Integrator so Lenovo XClarity Integrator can access vCenter and ESXi hosts through the hostname.

Step 3. Click **Save**.

Configuring Eth0 IP settings

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

About this task

When you 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, you can choose to use a statically assigned IP address, obtain an IP address from a DHCP server, or disable IPv4.

For IPv6, you 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 baseboard management controller (BMC) network, which is normally within the Eth1 subnet, you are allowed to configure the default gateway for only Eth0.

- If you specify a default gateway, it must be a valid IP address and must use the same network mask (the same subnet) as the IP address for Eth0.
- If Eth0 uses DHCP to obtain an IP address, the default gateway must also use DHCP and you cannot manually change this.

Step 4. Click **Save**.

Configuring Eth1 IP settings

You 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”. You 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 choose the VM network to which you want Eth1 to connect.
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. If you choose to use DHCP to assign IP addresses for both interfaces (Eth0 and Eth1), the DHCP server must not assign the same subnet for the IP addresses of the two interfaces.

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

For IPv6, you 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

You 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

You 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**.

Setting the date and time

You 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 your region and time zone.

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

Note: Lenovo XClarity Integrator only supports NTP Version 4.

Step 3. Click **Save**.

Backing up, restoring, and migrating data

You can back up, restore and migrate data for Lenovo XClarity Integrator for VMware vCenter.

Backing up data

You can back up data for a Lenovo XClarity Integrator virtual appliance.

Procedure

Step 1. From the Lenovo XClarity Integrator menu, click **Backup**.

Step 2. Click the **Backup** tab, and then click the **Backup** button. A dialog is displayed asking for a password for protecting the backup file.

Step 3. Specify a password in the **Password** and **Confirm Password** fields. The password must be at least nine ASCII characters.

Step 4. Click **OK** to start the backup process.

Step 5. When the backup completes, a download link **Click Here to Download** is displayed next to the **Backup** button. Click the link to download the backup file.

Note: Ensure that you record the password and store the back-up file in a safe location. When restoring data using the back-up file, you will be asked to specify the password.

Restoring data

You can restore previously backed up data to the same virtual appliance or migrate the data to a newly deployed virtual appliance.

Before you begin

To migrated to a newly deployed virtual appliance:

- Ensure that you are logged out of vSphere Web Client.
- If you are migrating backup data to a newly deployed virtual appliance, ensure the following conditions are met.
  - You must first uninstall the old Lenovo XClarity Integrator virtual appliance (see "Uninstalling Lenovo XClarity Integrator for VMware vCenter" on page 13).
  - You must use the exact same network settings as old Lenovo XClarity Integrator virtual appliance in the newly deployed appliance.
  - You must register the same vCenter as old Lenovo XClarity Integrator virtual appliance to the newly deployed appliance.

Procedure

Step 1. From the Lenovo XClarity Integrator menu, click **Backup**.

Step 2. Click the **Restore/Migrate** tab.

Step 3. Click the **Choose File** button to select the data file to be restored.

Step 4. Click the **Restore** button. A dialog is displayed asking for the password for the data file.

Step 5. Click **OK**. The appliance starts to restore/migrate the data file.

The virtual appliance restarts after the restoration process completes. You are redirect to login page after 10 seconds.

Note: Because the Lenovo XClarity Administrator certificates are not migrated, you must re-register the Lenovo XClarity Administrator instances if you want to re-use them.

Migrating data from a Windows-based LXCI

You can migrate data from a Window-based Lenovo XClarity Integrator to a Lenovo XClarity Integrator virtual appliance

Before you begin

The data being migrated must be backed up from a Windows-based Lenovo XClarity Integrator, not Lenovo XClarity Integrator virtual appliance.

The data being migrated does not include user information and passwords. You must update password for Lenovo XClarity Integrator, BMCs, and host passwords manually after migration.

Procedure

Step 1. Uninstall the old Windows-based Lenovo XClarity Integrator, not Lenovo XClarity Integrator (see "Uninstalling Lenovo XClarity Integrator for VMware vCenter" on page 13).

Step 2. Export data from Windows-based Lenovo XClarity Integrator using the following postgreSQL command:

`pg_dump -F c -p 9501 -U postgres uim_service >` *[target_data_file][target_data_file]*

For example:

```
pg_dump -F c -p 9501 -U postgres uim_service > d:\db_backup
```

Step 3. Deploy a Lenovo XClarity Integrator virtual appliance

Note: You must register the same vCenter as the Windows-based Lenovo XClarity Integrator to the newly deployed virtual appliance.

Step 4. Import the data file into the newly deployed virtual appliance.

a. From the Lenovo XClarity Integrator menu, click **Backup**.

b. Click the **Migrate Data from Windows** tab.

c. Click the **Choose File** button to select the data file to be migrated.

d. Click **Migrate** button. The data file is uploaded to the virtual appliance and migration begins.

The virtual appliance will restart after the migration process completes. You are redirect to login page after 10 seconds

Collecting service data

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

Procedure

Step 1. Optional: If required, click **Change level** to change log level to "Debug". Ensure that you restore the log level to Information after problem resolved

Step 2. Click **Collect Log**. The **Download Log** link is displayed.

Step 3. 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

You can choose to 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 you configure LDAP Client.
- Ensure that the LDAP users that can login this XClarity Integrator web interface are the members of the LXCI-SUPERVISOR group in your LDAP server.

  Create the group and add the users to it in your LDAP server before configuring this LDAP Client:

  1. From the external authentication server, create a user account. For instructions, see the documentation of your LDAP server.
  2. Create a group in your LDAP server with the name of "LXCI-SUPERVISOR". 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 that you 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, you 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. 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: If you change the client password in the external authentication server, ensure that you also updated the new password in LXCI for VMware vCenter. If the client password is changed in the external LDAP server, you 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 user ID and password that you specify are used only to test the connection to the authentication server. If successful, the LDAP client settings are saved, but the test login credential that you specified are not saved. All future binds use the user name and password that you used to log in to LXCI for VMware vCenter.

       Notes:

       - You should log in to LXCI for VMware vCenter using a fully-qualified user ID (for example, `administrator@domain.com` or `DOMAIN\admin`).
       - You should use a fully qualified test client name for the binding method.
  3. In the **Root DN** field, specify the top-most entry in your LDAP directory tree. In this case, searches are started using the specified root distinguished name as the search base.
  4. 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.
  5. In the **Group Search Attribute** field, specify the attribute name that is used to identify the groups to which a user belongs.
  6. 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:

- There are mis-configuration or changes in your LDAP server. You can log in using the local account. It is recommended to keep a record of your local account and password.
- The root distinguished name is incorrect.
- The user is not a member of the LXCI-SUPERVISOR group in your 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 you log 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 LXCI-SUPERVISOR group in your 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 you install a customized server certificate in Lenovo XClarity Integrator, you must 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 you connect to Lenovo XClarity Integrator, your browser displays a security message prompting you to accept the new certificate as an exception into the browser. To avoid the security messages, you can import the CA signing chain of the server certificate into your Web browser's list of trusted certificates.

For more information about importing certificates, see "Importing the Lenovo XClarity Integrator certificate in your Web browser" on page 20.

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. You 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 your 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 your browser connection to the Lenovo XClarity Integrator Web interface is terminated. You need to log in to the Lenovo XClarity Integrator Web interface again to continue your work.

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

Restoring the Lenovo XClarity Integrator-generated server certificate

You 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. You 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 your browser connection to the Lenovo XClarity Integrator Web interface is terminated. You need to log in to the Lenovo XClarity Integrator Web interface again to continue your work.

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

Regenerating Certificate Authority (CA) Root

You 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, you shall regenerate server certificate. Refer to “Restoring the Lenovo XClarity Integrator-generated server certificate” on page 65.
2. After regenerating CA root, you shall re-trust the CA in all client PCs. Refer to “Importing the Lenovo XClarity Integrator certificate in your Web browser” on page 20.

Downloading and installing Certificate Authority (CA) Root

You 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 your browser is Firefox, a dialog will be displayed in step 3. This dialog asks whether you trust the certificate. Check **Trust this CA to identify websites**, click **OK** and skip Step 4 to Step 9.

Downloading Server Certificate

You 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

You 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 your local.
- To remove a trusted certificate:
  1. Select the target certificate.
  2. Click **Remove**. A pop-up dialog will be displayed for you to confirm whether to remove the certificate.
  3. Click **Yes**.

Shutting down or restarting Lenovo XClarity Integrator

You can shut down or restart Lenovo XClarity Integrator. However, Lenovo XClarity Integrator will be disconnected after being shut down or restarted, so you 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.

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 you have installed the Lenovo XClarity Integrator certificate by following the instructions in "Importing the Lenovo XClarity Integrator certificate in your Web browser" on page 20.

Step 2. If you have used the vCenter FQDN 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 Web Client after installation

After you install Lenovo XClarity Integrator and register it with vCenter successfully, vSphere Web 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 Web 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

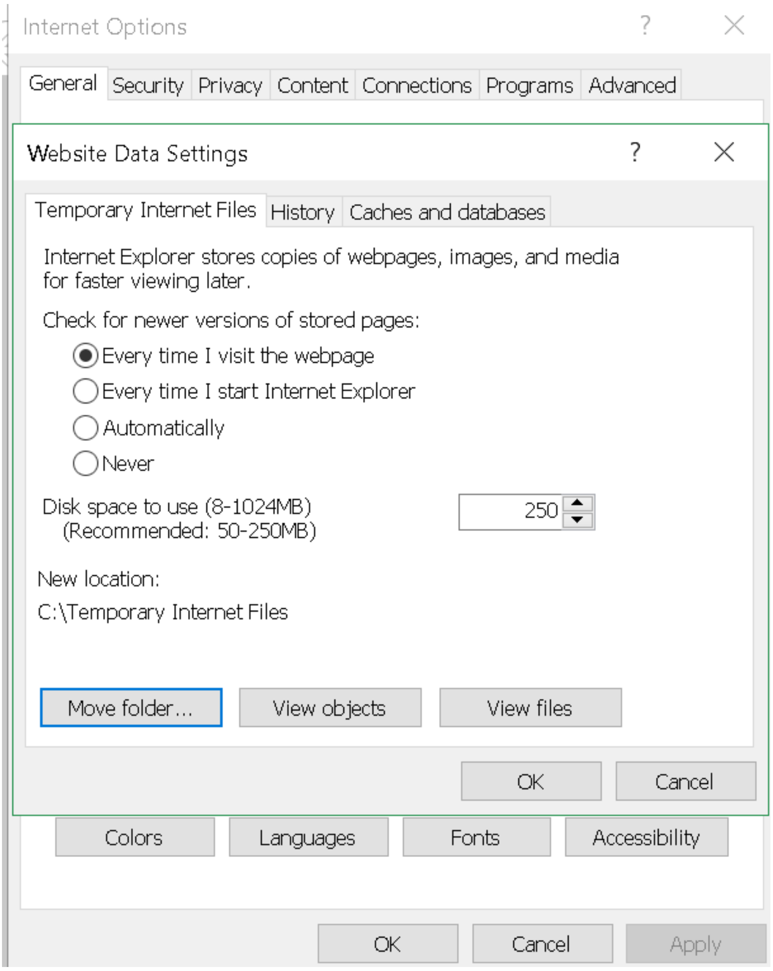
The cache mechanism of the Internet Explorer might impact the use of Lenovo XClarity Integrator. You need to set the Internet options every time you use Internet Explorer 11 or later versions to visit the Lenovo XClarity Integrator Web page.

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**.



Internet Explorer stores copies of webpages, images, and media for faster viewing later.

Check for newer versions of stored pages:

- ● Every time I visit the webpage
- ○ Every time I start Internet Explorer
- ○ Automatically
- ○ Never

Disk space to use (8-1024MB)
(Recommended: 50-250MB) 250

New location:
C:\Temporary Internet Files

Figure 14. 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.

You need to 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 your 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. You can operate all features by using the keyboard instead of the mouse.

You 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. © 2021 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.

Lenovo