Lenovo XClarity Integrator for Microsoft Windows Admin Center Installation and User Guide

Version 5.0

Note:

Before using this information and the product it supports, read the information in Appendix A "Notices" on page 71.

Twenty-second Edition (February 2025)

Contents

About this publication

This publication provides instructions on installing Lenovo® XClarity Integrator for Microsoft® Windows Admin Center (hereinafter referred to as LXCI for WAC), and using its integrated features to manage the servers in users' environment.

Conventions and terminology

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

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

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

Term	Acronym	Definition
Baseboard Management Controller	BMC	A specialized service processor that monitors the physical state of a computer, network server or other hardware device by using sensors, and by communicating with the system administrator. The BMC is a part of the Intelligent Platform Management Interface (IPMI), and is contained in the system board or the main circuit board of the device to be monitored.
Chassis Management Module	CMM	A service processor used to configure and manage components in a Flex chassis.
Compute node	/	An independent server supported in a Flex chassis. The compute node contains one or more microprocessors, memories, storages, and network controllers. It is equipped with its own operating system and applications.
Features on Demand	FoD	A tool that activates features without installing hardware or connecting to other devices.
Host Bus Adapter	HBA	The host system that connects a computer to other network and storage devices.
Integrated Management Module	IMM	A custom BMC that developed by Lenovo. IMM consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities into a single chip on the server system board.
Lenovo XClarity Administrator	LXCA	A hardware management tool packaged as an appliance for monitoring and managing the Lenovo servers or network products.
Lenovo XClarity Integrator	LXCI	A tool suite that enables IT administrators to integrate the management features of the Lenovo servers with Microsoft Admin Center.
Unified Extensible Firmware Interface	UEFI	A specification that details the interface between the operating system and the platform firmware at boot time. It is not specific to any processor architecture.

Term	Acronym	Definition
Windows Admin Center	WAC	An evolution of Windows Server in-box management tool. WAC is a single pane of glass that consolidates all aspects of local and remote server management.
XClarity Controller	XCC	The next generation of custom BMC developed by Lenovo. XCC enhances the current functions of IMM, and provides more functions. For example, HTML, enhanced remote presence capabilities, REST API (Redfish schema), and so on.

Web resources

The following Web sites provide the resources for understanding, using, and troubleshooting Lenovo XClarity Integrator, Lenovo XClarity Administrator, the Flex System servers, and the System x servers.

Lenovo XClarity Integrator for Windows Admin Center

This Web site provides the latest information about Lenovo XClarity Integrator for Windows Admin Center:

- Lenovo XClarity Integrator for Windows Admin Center 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 the system management capability:

- System Management with Lenovo XClarity Solution Web site

Lenovo technical support portal

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

- Lenovo Support Portal Web site

Lenovo ServerProven pages

The following Web sites assist users to obtain information about hardware compatibility:

- Lenovo ServerProven: Compatibility for hardware, applications, and middleware

Microsoft Windows Admin Center Web site

This Web site provides the detailed information about Microsoft Windows Admin Center (WAC):

- Microsoft Windows Admin Center Web site

ThinkAgile MX Certified Node Best Recipe

This Web site provides the ThinkAgile MX certified node best recipe:

- ThinkAgile MX Certified Node Best Recipe

Chapter 1. Overview

Lenovo XClarity Integrator for Microsoft Windows Admin Center (LXCI for WAC) is a plug-in that integrates functions for managing, monitoring, and updating the Lenovo servers and their components with Windows OS or software application management system. It supports to view Lenovo server hardware and firmware inventories, events, alerts, and health status, update firmware/driver, cluster-aware rolling update of firmware/driver for Windows cluster nodes, display Lenovo ThinkAgile MX server topology view, and facilitate storage pool operations through wizards. Lenovo XClarity Administrator (LXCA) (optional) streamlines the Lenovo server management job, especially for large-scale deployment.

System requirements

This topic lists the system requirements for the Lenovo XClarity Integrator.

Prepare users' environment

Lenovo XClarity Integrator is an extension of Windows Admin Center. It works in the same environment as Windows Admin Center. For more information, refer to Windows Admin Center and Install Windows Admin Center.

Supported software

Software type	Software version
Windows Admin Center	2410
Lenovo XClarity Administrator	3.0.0, 3.1.0, 3.1.1, 3.2.0, 3.3.0, 3.4.0, 3.5.0, 3.6.0, 4.0.x, 4.1.x, 4.2.x

Supported operating systems

Server type	Windows version	Windows Server version	Azure Stack HCI version
Management server (installed with LXCI)	10, 11	2016, 2019, 2022, 2025	/
Managed server (managed by LXCI)	/	2016, 2019, 2022, 2025	20H2, 21H2, 22H2, 23H2

Supported Web browser

Web browser type	Web browser version
Google Chrome	93.0.4577.82 or later versions
Microsoft Edge	93.0.961.52 or later versions
Note: LXCI for WAC saves some settings in local database of the browser. To prevent the loss of the saved settings, do not clear cookies and site data.	

Port requirements

Depending on the firewall in the environment, several ports should be available. If these ports are blocked or used by another process, some Lenovo XClarity Integrator functions might not work.

- All out-bounding connections initialized from Windows Admin Center are allowed.
- Lenovo XClarity Integrator does not require any additional in-bounding connections other than those required by Windows Admin Center.

Supported hardware

Supported hardware is listed in the following table.

Note: Some features are supported only by specific server models. Refer to Features supported by specific server models.

Table 1. Supported hardware

System	Server models	
Lenovo ThinkSystem	• SD530 (7X20, 7X21, 7X22) • SD530 V3 (7DD3, 7DDA) • SD550 V3 (7DD2, 7DD9) • SD630 V2 (7D1K) • SD650 (7X58) • SD650 V2 (7D1M) • SD650-N V2 (7D1N) • SE350 (7Z46, 7D1X, 7D27, 7D1R) • SE350 V2 (7DA9) • SE360 V2 (7DAM) • 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) • SR250 V3 (7DCM, 7DCL) • SR258 (7Y53) • SR530 (7X07, 7X08) • SR550 (7X03, 7X04) • SR570 (7Y02,7Y03) • SR590 (7X98,7X99) • SR630 (7X01,7X02) • SR630 V2 (7Z70, 7Z71) • SR630 V3 (7D72, 7D73, 7D74) • SR630 V4 (7DG8, 7DG9, 7DGA, 7DGB) • SR635 (7Y98, 7Y99)	• SR635 V3 (7D9H, 7D9G) • SR645 (7D2X, 7D2Y) • SR645 V3 (7D9C, 7D9D) • SR650 (7X05, 7X06) • SR650 V2 (7Z72, 7Z73) • SR650 V3 (7D75, 7D76, 7D77) • SR650 V4 (7DGC, 7DGD, 7DGE, 7DGF) • SR655 (7Y00, 7Z01) • SR655 V3 (7D9E, 7D9F) • SR665 (7D2V, 7D2W) • SR665 V3 (7D9A, 7D9B) • SR670 (7Y36, 7Y37, 7Y38) • SR670 V2 (7Z22, 7Z23) • SR850 (7X18, 7X19) • SR850 V2 (7D31, 7D32, 7D33) • SR850 V3 (7D96, 7D97, 7D98) • SR850P (7D2F, 7D2G, 7D2H) • SR860 (7X69, 7X70) • SR860 V2 (7Z59, 7Z60, 7D42) • SR860 V3 (7D93, 7D94, 7D95) • SR950 (7X11, 7X12, 7X13) • ST250 (7Y45, 7Y46) • ST250 V2 (7D8F, 7D8G, 7D8H) • ST258 (7Y47) • ST550 (7X09, 7X10) • ST558 (7Y15, 7Y16) (China only) • ST650 V2/ST658 V2 (China only) (7Z74, 7Z75, 7Z76) • ST650 V3 (7D7A, 7D7B, 7D7C)
Lenovo ThinkAgile	• MX Series appliance server (7D19, 7D1B, 7D2U, 7D5R, 7D5S, 7D5T, 7D6U, 7D6S, 7D66, 7D67, 7D6B, 7Z20)	• SXM Series appliance server (9565, 7Y34)
Lenovo ThinkServer	• nx360 M5 (5465)	• sd350 M5 (5493)
Lenovo ThinkEdge	• SE450 (7D8T)	• SE455 V3 (7DBY)

Table 1. Supported hardware (continued)

System	Server models	
Lenovo Flex System	• x240 Compute Node(7162, 2588) • x240 M5 Compute Node (2591, 9532)	• x440 Compute Node (7167, 2590) • x280, x480, x880 X6 Compute Node (7196, 4258)
Lenovo System x	• x3250 M6 (3633, 3943) • x3500 M5 (5464) • x3550 M5 (5463, 8869) • x3630 M4 (8103)	• x3650 M5 (8871, 5462) • x3750 M4 (8753) • x3850 X6 (6241) • x3950 X6 (6241)

Features supported by specific server models

The following table lists the features that are supported only by specific server models.

Table 2. Features supported by specific server models

Feature	Server models supporting the feature	
Storage Spaces Direct (Azure Stack HCI) cluster disk management	• ThinkAgile MX3520 appliance on SR650 (7D5R) • ThinkAgile MX certified node on SR650 (7Z20) • ThinkSystem SR650 (7X05, 7X06)	• ThinkSystem SR650 V2 (7Z72, 7Z73) • ThinkSystem SR650 V3 (7D75, 7D76, 7D77)
System update with best recipes	• ThinkAgile MX1020 appliance on SE350 (7D5S, 7D5T) • ThinkAgile MX1021 certified node on SE350 (7D1B, 7D2U) • ThinkAgile MX3330 appliance on SR630 V2 (7D19) • ThinkAgile MX3331 certified node on SR630 V2 (7D67) • ThinkAgile MX3530 appliance on SR650 V2 (7D6B)	• ThinkAgile MX3531 certified node on SR650 V2 (7D66) • ThinkAgile MX3520 appliance on SR650 (7D5R) • ThinkAgile MX certified node on SR650 (7Z20) • ThinkAgile MX630 V3 (7D6U) • ThinkAgile MX650 V3 (7D6S)
Azure Stack HCI cluster deployment [Note 1]	• ThinkAgile MX1020 appliance on SE350 (7D5S, 7D5T) • ThinkAgile MX1021 certified node on SE350 (7D1B, 7D2U) • ThinkAgile MX3330 appliance on SR630 V2 (7D19) • ThinkAgile MX3331 certified node on SR630 V2 (7D67) • ThinkAgile MX3520 appliance on SR650 (7D5R) • ThinkAgile MX3530 appliance on SR650 V2 (7D6B) • ThinkAgile MX3531 certified node on SR650 V2 (7D66)	• ThinkAgile MX certified node on SR650 (7Z20) • ThinkAgile MX630 V3 (7D6U) • ThinkAgile MX650 V3 (7D6S) • ThinkSystem SE350 (7Z46, 7D1X, 7D27, 7D1R) • ThinkSystem SR630 V2 (7Z70, 7Z71) • ThinkSystem SR650 (7X05, 7X06) • ThinkSystem SR650 V2 (7Z72, 7Z73) • ThinkSystem SR650 V3 (7D75, 7D76, 7D77)

Table 2. Features supported by specific server models (continued)

Feature	Server models supporting the feature	
Cluster-Aware Updating (CAU) Note 1	• ThinkAgile MX1020 appliance on SE350 (7D5S, 7D5T) • ThinkAgile MX1021 certified node on SE350 (7D1B, 7D2U) • ThinkAgile MX3330 appliance on SR630 V2 (7D19) • ThinkAgile MX3331 certified node on SR630 V2 (7D67) • ThinkAgile MX3520 appliance on SR650 (7D5R) • ThinkAgile MX3530 appliance on SR650 V2 (7D6B)	• ThinkAgile MX3531 certified node on SR650 V2 (7D66) • ThinkAgile MX certified node on SR650 (7Z20) • ThinkSystem SE350 (7Z46, 7D1X, 7D27, 7D1R) • ThinkSystem SR630 V2 (7Z70, 7Z71) • ThinkSystem SR650 (7X05, 7X06) • ThinkSystem SR650 V2 (7Z72, 7Z73) • ThinkSystem SR650 V3 (7D75, 7D76, 7D77)
Native OS management Note 2 and 3	All servers except for the ThinkServer or ThinkSystem SR635 (7Y98,7Y99)/SR655 (7Y00, 7Z01) servers.	
Notes: 1. The Microsoft Azure Stack HCI operating system must be used to support this feature. 2. IPMI over KCS Access, Ethernet Over USB, and REST/CIM Over HTTPS must be enabled to support this feature. 3. By default, native OS management is disabled for servers enabled with Storage Spaces Direct. Users can enable it by referring to "Configuring native OS management" on page 12.		

Chapter 2. Installing Lenovo XClarity Integrator

This chapter describes how to install, update, and uninstall Lenovo XClarity Integrator.

Installing Lenovo XClarity Integrator

This section describes how to install Lenovo XClarity Integrator.

Lenovo XClarity Integrator can be installed as an extension. Users can select one of the following installation ways:

- Install Lenovo XClarity Integrator from Windows Admin Center Feed. Refer to "Installing Lenovo XClarity Integrator from Windows Admin Center Feed" on page 5.
- Install Lenovo XClarity Integrator from a local shared folder. Refer to "Installing Lenovo XClarity Integrator from a local shared folder" on page 5.
- Installing Lenovo XClarity Integrator from a local file system folder. Refer to "Installing Lenovo XClarity Integrator from a local file system folder" on page 6.

Installing Lenovo XClarity Integrator from Windows Admin Center Feed

This section describes how to install Lenovo XClarity Integrator from Windows Admin Center Feed.

Note: For more information, refer to Install and Manage Extensions.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. Click the settings icon ⚙ in the top right corner.
The Settings page is displayed.

Step 3. On the Settings page, click **Extensions** in the left navigation pane.
The **Extensions** pane is displayed.

Step 4. In the **Extensions** pane:

a. Click the **Feeds** tab.

b. On the **Feeds** tab, click **Add**. The **Add package source** pane is displayed on the right.

c. In the **Add package source** pane, input https://aka.ms/sme-extension-feed, and click **Add**.

Note: If this Web site is in the **Package feeds** area, select this Web site.

Step 5. Return to the **Extensions** pane:

a. Click the **Available extensions** tab.

b. On the **Available extensions** tab, select **Lenovo XClarity Integrator** from the list. The license information will be displayed.

c. Read the license information. If users accept the license information, click **Install**.

d. When the "Install this extension?" window is displayed, click **Confirm** to continue. When a notification prompts Lenovo XClarity Integrator is installed, users can work with Lenovo XClarity Integrator.

Installing Lenovo XClarity Integrator from a local shared folder

This section describes how to install Lenovo XClarity Integrator from a local shared folder.

Procedure

Step 1. Download the installation package (lnvgy_sw_xclarity_integrator_for_wac.*.nupkg) from the windows-admin-center-feed site or Lenovo WAC home page.

Step 2. Put the installation package into a shared folder. For example, //localhost/sharedFolder.

Step 3. Log in to Windows Admin Center.

Step 4. Click the settings icon ⚙ in the top right corner.
The Settings page is displayed.

Step 5. On the Settings page, click **Extensions** in the left navigation pane.

Step 6. In the **Extensions** pane:

a. Click the **Feeds** tab, and click **Add**.

b. Input the shared folder path, and click **Add**.

Step 7. Return to the **Extensions** pane:

a. Click the **Available extensions** tab.

b. On the **Available extensions** tab, select **Lenovo XClarity Integrator** from the list. The license information will be displayed.

c. Read the license information. To accept the license information, click **Install**.

d. When the “Install this extension?” window is displayed, click **Confirm** to continue. When a notification prompts Lenovo XClarity Integrator is installed, users can work with Lenovo XClarity Integrator.

Installing Lenovo XClarity Integrator from a local file system folder

This section describes how to install Lenovo XClarity Integrator from a local file system folder.

Procedure

Step 1. Download the installation package (lnvgy_sw_xclarity_integrator_for_wac.*.nupkg) from the windows-admin-center-feed site or Lenovo WAC home page.

Step 2. Put the installation package into a local file system folder. For example, c:\lenovo\.

Step 3. Log in to Windows Admin Center.

Step 4. Click the settings icon ⚙ in the top right corner.
The Settings page is displayed.

Step 5. On the Settings page, click **Extensions** in the left navigation pane.

Step 6. In the **Extensions** pane:

a. Click the **Feeds** tab and click **Add**

b. Input the shared folder path, and click **Add**.

Step 7. Return to the **Extensions** pane:

a. Click the **Available extensions** tab.

b. On the **Available extensions** tab, select **Lenovo XClarity Integrator** from the list. The license information will be displayed.

c. Read the license information. To accept the license information, click **Install**.

d. When the “Install this extension?” window is displayed, click **Confirm** to continue. When a notification prompts Lenovo XClarity Integrator is installed, users can work with Lenovo XClarity Integrator.

Updating Lenovo XClarity Integrator

This section describes how to update Lenovo XClarity Integrator.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. Click the settings icon ⚙ in the top right corner.
The Settings page is displayed.

Step 3. On the Settings page, click **Extensions** in the left navigation pane.
The **Extensions** pane is displayed.

Step 4. In the **Extensions** pane:

a. Click the **Installed extensions** tab.

b. On the **Installed extensions** tab, select the Lenovo XClarity Integrator with the status “Update available (version)”.

c. Click **Update**.

d. When the “Update this extension?” window is displayed, click **Confirm** to continue.

Uninstalling Lenovo XClarity Integrator

This section describes how to uninstall Lenovo XClarity Integrator.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. Click the settings icon ⚙ in the top right corner.
The Settings page is displayed.

Step 3. On the Settings page, click **Extensions** in the left navigation pane.
The **Extensions** pane is displayed.

Step 4. In the **Extensions** pane:

a. Click the **Installed extensions** tab.

b. On the **Installed extensions** tab, select **Lenovo XClarity Integrator** from the list.

c. Click **Uninstall**.

d. When the “Uninstall this extension?” window is displayed, click **Confirm** to continue.

Updating Lenovo XClarity Integrator settings

This section describes how to update Lenovo XClarity Integrator settings, including supported LXCA versions and information about supported Lenovo servers.

Procedure

Step 1. In any of Lenovo extensions, click the more icon ⋯ in the top right corner.
A menu is displayed.

Step 2. In the menu, click **Settings**.

Step 3. On the Update page, click **Check Updates** to check online or click the **here** link to manually download and import the update file.

Step 4. Click **Close** after the settings are updated.

Checking and installing updates

This section describes how to check and install updates.

Users can use this function to check and download available component updates from Lenovo Web site and install them. These updates are used to improve functions of Lenovo XClarity Integrator or fix bugs. For example, users can update Lenovo XClarity Administrator Compatibility Configuration File to support later versions of Lenovo XClarity Administrator.

Select one of the following installation ways:

- "Checking and installing the latest updates from Lenovo Web site" on page 8
- "Installing local updates" on page 8
- "Checking change history" on page 8

Note: WAC will automatically check whether the update is available after the Lenovo extension is input.

Checking and installing the latest updates from Lenovo Web site

Procedure

Step 1. In any of Lenovo extensions, click the more icon ··· in the top right corner.
A menu is displayed.

Step 2. In the menu, click **Settings → Update**.

Step 3. On the Update page, do one or more of the following:

- Enable or disable **Check update automatically** or **Install update automatically**.

  Note: By default, if **Check update automatically** is disabled, **Install update automatically** will be disabled and hidden.
- Click **Check Updates** to import the latest updates.
- Click **Install Updates** to download and install updates.

Installing local updates

Procedure

Step 1. In any of Lenovo extensions, click the more icon ··· in the top right corner.
A menu is displayed.

Step 2. In the menu, click **Settings → Update**.

Step 3. On the Update page, click **Manually download and import updates** to manually download and import the update file.
The Install an update page is displayed.

Step 4. On the Install an update page, right-click the download link and select **Save link as...** to download the update file.

Step 5. Select the update file downloaded from the Lenovo Web site.

Step 6. Click **Install Updates** to install it.

Checking change history

Procedure

Step 1. In any of Lenovo extensions, click the more icon ··· in the top right corner.
A menu is displayed.

Step 2. In the menu, click **Settings → Update → Change history**.

Step 3. On the Change history page, check the update time, method, original version, and target version of components.

Chapter 3. Configuring Lenovo XClarity Integrator

This chapter describes how to configure Lenovo XClarity Integrator settings.

Collecting usage data

This section describes how to improve the product by sending usage data.

We collect information about how to use the product and basic statistics about the servers managed by Windows Admin Center. We will never collect any sensitive or personal information. The information will help us improve user experience of the product. Users can select whether to send the information to us or not by doing the following steps.

Procedure

Step 1. In any of Lenovo extensions, click the more icon ⋯ in the top right corner.
A menu is displayed.

Step 2. In the menu, click **Settings**.

Step 3. On the Privacy page, select whether to send usage data to us or not.

Step 4. Click **Apply**.

Configuring HTTP Proxy settings

This section describes how to configure HTTP Proxy settings for Internet access.

Procedure

Step 1. In any of Lenovo extensions, click the more icon ⋯ in the top right corner.
A menu is displayed.

Step 2. In the menu, click **Settings**.

Step 3. On the Internet Access page:

- If there is no need to use HTTP Proxy:
  1. Leave the HTTP Proxy configuration as the default.
  2. Click **Test URL**.

     A success message will be displayed if the Internet access test passes.
  3. Click **Close**.
- To enable HTTP Proxy, do the following:
  1. Enable HTTP Proxy.
  2. Specify the Proxy server host and port.
  3. Enable authentication as required.
  4. If authentication is enabled, specify the user name and password.
  5. Click **Test URL**.

     A success message will be displayed if the Internet access test passes.
  6. Click **Apply**.

Configuring log settings

This section describes how to configure log settings.

To configure the log level and maximum disk space occupied by logs for the Windows Admin Center plug-in, do the following:

Step 1. In any of Lenovo extensions, click the more icon ··· in the top right corner.
A menu is displayed.

Step 2. In the menu, click **Settings**.

Step 3. On the Log Configuration page:

a. Configure the log level, which can be **FATAL**, **ERROR**, **WARN**, **INFO**, or **DEBUG**.

Note: FATAL is the highest log level while **DEBUG** is the lowest. Logs with a level higher than the configured log level will all be reported in the log file as well.

b. Configure the maximum log size on the disk based on the disk capacity.

c. Click **Apply**.

Step 4. Click **Download** to download the log files provided.

After configuring log settings for the Windows Admin Center plug-in, users should also configure the log level for the Cluster-Aware Updating plug-in.

Configuring native OS management

This section describes how to enable or disable native OS management for servers enabled with Storage Spaces Direct.

Native OS management is a way to manage the hardware when no Lenovo XClarity Administrator is available. To use this function, log in to the XCC Web GUI and enable IPMI over KCS Access, Ethernet Over USB, and REST/CIM Over HTTPS.

Native OS management is inapplicable to ThinkServer and ThinkSystem SR635/SR655 servers. For servers enabled with Storage Spaces Direct, native OS management is disabled by default, but users can perform the following steps to enable native OS management for them.

Procedure

Step 1. In any of Lenovo extensions, click the more icon ··· in the top right corner.
A menu is displayed.

Step 2. In the menu, click **Settings**.

Step 3. On the Native OS Management page, do one or more of the following:

- To enable or disable the native OS management for servers enabled with Storage Spaces Direct, select **Yes** or **No, thanks** and click **Apply**.
- To set the valid period of inventory cache data, input the number of minutes and click **Apply**.

Notes:

– The range of the valid period is from 10 to 525600 minutes.
– The default value is 10080 minutes.

Managing credentials

This section describes how to add, edit, and delete user account credentials for Windows systems, clusters, Lenovo XClarity Controllers, Lenovo XClarity Administrators and so on.

Procedures

Step 1. Do one of the following to go to the Credential Manager page:

- In any of Lenovo extensions, click the more icon ··· on the top right corner, and then click **Settings → Credential Manager** from the menu.
- On the Report Problem page, go to the Specify your credentials page and click **Open credential manager**. For more information, see "Reporting problem" on page 65.

Step 2. On the Credential Manager page, do one or more of the following:

- To add a credential:
  1. Click **Add**. The Add a credential page is displayed.
  2. On the Add a credential page, input user name, password, and description, and click **Apply**.
- To edit a credential:
  1. Select the target credential from the credential list.
  2. Click **Edit**. The Edit a credential page is displayed.
  3. On the Edit a credential page, update the password or description and click **Apply**.
- To delete a credential:
  1. Select the target credential from the credential list.
  2. Click **Delete**. The Delete Credentials window is displayed.
  3. In the Delete Credentials window, click **OK**.

Configuring the system language/region

This section describes how to switch the system language and region. Currently, languages supported include German, English, Spanish, French, Italian, Japanese, Korean, Brazilian Portuguese, Russian, Simplified Chinese, and Traditional Chinese.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. Click the settings icon ⚙ in the top right corner.
The Settings page is displayed.

Step 3. On the Settings page, click **Language / Region** in the left navigation pane.
The **Language / Region** pane is displayed.

Step 4. In the **Language / Region** pane, select the desired language and region, and then click **Save and reload**.

The system is then reloaded and displayed in the language selected.

Chapter 4. Managing servers and chassis through Lenovo XClarity Integrator

This chapter describes how to manage servers and chassis through Lenovo XClarity Integrator.

If the target server is installed without any OS, it is recommended to manage it through Lenovo XClarity Integrator. Users should connect to Lenovo XClarity Administrator first. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

If the target server is already installed with an OS, it is recommended to manage it through Server Manager or Cluster Manager. Refer to Chapter 5 "Managing servers through Server Manager" on page 31 or Chapter 6 "Managing servers through Cluster Manager" on page 37.

Connecting to Lenovo XClarity Administrator

This chapter descries how to connect to and remove Lenovo XClarity Administrator.

For more information about installing and setting up Lenovo XClarity Administrator, refer to System Management with Lenovo XClarity Solution Web site.

Connecting to a new or existing Lenovo XClarity Administrator

This section describes how to connect to a new or existing Lenovo XClarity Administrator in Lenovo XClarity Integrator.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. In the top left corner, click the drop-down list arrow ⌄ on the right of **Windows Admin Center**.

Step 3. Click **Lenovo XClarity Integrator**.
The All Connections page is displayed.

Step 4. On the All Connections page, users can do one or more of the following:

- To connect to a new Lenovo XClarity Administrator:
  1. Click **Add**. The **Add a Connection** pane is displayed on the right.
  2. In the **Add a Connection** pane, select **Connect to a Lenovo XClarity Administrator**.
  3. In the **Connect to Lenovo XClarity Administrator** pane, input the IP address, user name, and password. Then, click **Submit**. The Lenovo XClarity Administrator is connected.
- To connect to an existing Lenovo XClarity Administrator:
  1. Click **Credential Needed** in the Status column. The **Connect to Lenovo XClarity Administrator** pane is displayed on the right.
  2. In the **Connect to Lenovo XClarity Administrator** pane, input the user name and password.
  3. Click **Submit**. The Lenovo XClarity Administrator is connected.

Notes:

- When inputting the user name and password in the **Connect to Lenovo XClarity Administrator** pane, refer to the user privilege or permission requirements for specific actions. Ensure that the user provided has enough permissions to perform desired operations.
- The version of Lenovo XClarity Administrator should be v2.3.6, v2.4, v2.6, or later to allow LDAP users to log in.

Removing Lenovo XClarity Administrator

This section describes how to remove Lenovo XClarity Administrator.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. In the top left corner, click the drop-down list arrow ⌄ on the right of **Windows Admin Center**.

Step 3. Click **Lenovo XClarity Integrator**.
The All Connections page is displayed.

Step 4. On the All Connections page:

a. Select one or more target Lenovo XClarity Administrators.

b. Click **Remove**.

Note: After the Lenovo XClarity Administrator is removed from Lenovo XClarity Integrator, the servers managed by Lenovo XClarity Administrator will not be removed from Lenovo XClarity Administrator.

Adding Lenovo rack or tower servers

This section describes how to add one or more Lenovo rack or tower servers to Lenovo XClarity Administrator.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

Step 2. Return to the All Connections page, and click **Add**.
The **Add a Connection** pane is displayed on the right.

Step 3. In the **Add a Connection** pane, select **Manage Lenovo Rack or Tower Servers**.
The **Choose a Lenovo XClarity Administrator** pane is displayed.

Step 4. Select a connected Lenovo XClarity Administrator.

Note: If no Lenovo XClarity Administrator is connected, an error message will be displayed.

Step 5. In the **Manage Lenovo Rack or Tower Servers** pane:

a. Input a BMC IP address, click the add icon +, and input another BMC IP address. Repeat this step until all rack or tower servers are added.

b. Input the user name and password.

c. Click **Manage**.

Adding a Lenovo chassis

This section describes how to add a Lenovo chassis to Lenovo XClarity Administrator.

Note: The Flex compute nodes in Lenovo chassis cannot be discovered or managed separately.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

Step 2. Return to the All Connections page, and click **Add**.
The **Add a Connection** pane is displayed on the right.

Step 3. In the **Add a Connection** pane, select **Manage a Lenovo Chassis**.
The **Choose a Lenovo XClarity Administrator** pane is displayed.

Step 4. Select a connected Lenovo XClarity Administrator.

Note: If no Lenovo XClarity Administrator is connected, an error message will be displayed.

Step 5. In the **Manage a Lenovo Chassis** pane:

a. Input the CMM IP address, user name, and password.

b. Input the recovery password for the CMM recovery ID twice.

c. Click **Manage**.

Notes:

- When managing a chassis, the CMM is configured to authenticate users with the Lenovo XClarity Administrator (local CMM user accounts are no longer valid). The RECOVERY_ID is important because it enables users to access the CMM directly if there are issues with the Lenovo XClarity Administrator. Ensure that the password specified is stored in a secure location.
- The recovery password should meet the CMM password policy.
- After the chassis is added, only the servers of this chassis will be displayed in Lenovo XClarity Integrator. Users can view and manage the servers by using the same way as viewing and managing the rack or tower servers.

Powering on, powering off, and restarting one or more servers

This section describes how to power on, power off, and restart one or more servers.

Notes:

- This process takes a few minutes. A job will be created when the process starts. To view the results, click the Jobs icon ☰ in the top right corner and click **Persistent Jobs**.
- The server in the “Unknown”, “Offline”, or “Pending” status cannot be powered on, powered off, or restarted.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to “Connecting to a new or existing Lenovo XClarity Administrator” on page 15.

Step 2. Return to the All Connections page, and click the drop-down list arrow ∨ on the left of the Lenovo XClarity Administrator IP address.
All managed servers are displayed.

Step 3. Users can do one or more of the following:

- To power on, power off, and restart one server:
  1. Select one server.
  2. Click **Power On**, **Power Off**, or **Reboot**.

  Note: Alternatively, users can also power on, power off, and restart a server on the Lenovo Server page. For more information, refer to “Powering on, powering off, and restarting a server” on page 26.
- To power on, power off, and restart several servers:
  1. Select several servers.
  2. Click **Power On**, **Power Off**, or **Reboot**.

Step 4. When the Warning window is displayed, click **Yes** to continue.

Launching the remote control

In Lenovo XClarity Integrator, users can remotely manage the Lenovo servers through the remote control session, including the ThinkSystem, ThinkAgile, ThinkServer, NeXtScale, Converge, Flex System, and System x servers, for example, powering on, powering off the servers, and mounting a local or remote drive in the local console. This section describes how to launch the remote control for a server.

Notes:

- Alternatively, users can also launch the remote control for a server on the Lenovo Server page. For more information, refer to "Launching the remote control on the Lenovo Server page" on page 25.
- For the server in the "Unknown", "Offline", or "Pending" status, the remote control cannot be launched.

Before you begin

If the server is the ThinkServer, Converged, Flex System, NeXtScale, or System x server, ensure that:

- This server is connected to Internet.
- This server is running on the following operating systems (either 32-bit or 64-bit):
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
  - Microsoft Windows 11
- A Java Runtime Environment (JRE) with Java WebStart support is installed. The following JREs are supported.
  - Oracle JRE 7 (see Oracle Java download Web site)
  - Oracle JRE 8, which requires a paid license (see Oracle Java download Web site)
  - Adopt OpenJDK 8 with the IcedTea-Web v1.8 plugin (see the Adopt OpenJDK Web site, IcedTea-Web Web site, and IcedTea-Web usage Web site)

  Note: For the ThinkSystem and ThinkAgile servers, JRE is not required.
- An FoD key for ThinkServer System Manager Premium Upgrade is installed on the ThinkServer servers. For more information, refer to "Viewing the Feature on Demand keys" on page 28.
- An FoD key for remote presence is installed on the Converged, NeXtScale, and System x servers. For more information, refer to "Viewing the Feature on Demand keys" on page 28.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

Step 2. Return to the All Connections page, and click the drop-down list arrow ⌄ on the left of the Lenovo XClarity Administrator IP address.
All managed servers are displayed.

Step 3. Select a server.

Step 4. Click **Launch Remote Control**.

Step 5. When the security warning prompts, click **Accept**.

Viewing the warranty information of all managed servers

This section describes how to view the warranty information of all managed servers.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

Step 2. Return to the All Connections page, and click > in front of the Lenovo XClarity Administrator IP address.
All servers managed by the Lenovo XClarity Administrator are listed.

Step 3. In the server list, users can view **Warranty Status** and **Warranty Expired Date** of all managed servers.

Note: Alternately, users can view the overall information (including the warranty information) of a server on the Lenovo Server page. For more information, refer to "Viewing the overall information of a server" on page 21.

Collecting service data for single server

This section describes how to collect the service data for one or more single severs.

Procedure

Step 1. From the vSphere Client Web page, select the target server.

Step 2. On the server page, select **Lenovo XClarity Integrator → Native OS Management/Lenovo XClarity Administrator → Service Data**.

Step 3. On the Service Data page, select one or more target files, and click **Collect Service Data**.

Step 4. On the Select Service Data Type window, do the following:

a. (Optional) Select **Optional Log**.

Note: By default, the necessary logs will be collected by LXCI. Users can also select the optional logs to help narrow down issues.

b. Click **Credential Needed** to select the existing credential, or add the user name, password, and description of a Windows administrator account, and then click **Apply**/**Close**.

Notes:
- For the cluster node, the account should be the Active Directory domain account included in the local Administrators group.
- For the non-cluster server, the account should be the Active Directory domain account included in the local Administrators group or the built-in administrator account.
- OS credentials are required if one or more of the following operations are required:
  - Firmware/driver update in native OS management mode
  - Clustered roles migration

c. Click **OK**.

Step 5. On the Specify your credentials window, select the type of credentials, input user name and password, and click **OK**.

Step 6. On the Select Service Data Type window, click **OK**.

Step 7. When the Warning window is displayed, click **Yes** to continue.

Collecting service data for all servers

This section describes how to collect the service data for all servers.

Procedure

Step 1. In any of Lenovo extensions, click the more icon ⋯ in the top right corner. A menu is displayed.

Step 2. In the menu, click **Collect Service Data**.

Step 3. On the Service Data page, click **Collect Service Data → OK**.

Step 4. When the Warning window is displayed, click **Yes** to continue. The service data of all servers will be downloaded.

Removing the servers

This section describes how to remove servers from Lenovo XClarity Integrator and Lenovo XClarity Administrator.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

Step 2. Return to the All Connections page, and click the drop-down list arrow ⌄ on the left of Lenovo XClarity Administrator IP address.
All managed servers are displayed.

Step 3. Select one or more servers.

Step 4. Click **Unmanage**.

Step 5. When the Warning window is displayed, click **Yes** to continue.

Note: When one or more Flex servers are removed, their parent chassis and the other managed servers of this chassis will also be removed.

Managing a server

This section describes how to manage a server and its components on the Lenovo Server page.

In this section, do one or more of the following:

- View the overall information of a server. Refer to "Viewing the overall information of a server" on page 21.
- Sync the inventory. Refer to "Syncing the inventory of a server" on page 21.
- Update firmware for a server. Refer to "Updating firmware for a server" on page 21.
- Update firmware for multiple servers. Refer to "Updating firmware for multiple servers" on page 23.
- Launch the remote control on the Lenovo Server page. Refer to "Launching the remote control on the Lenovo Server page" on page 25.
- Power on, power off, and restart a server. Refer to "Powering on, powering off, and restarting a server" on page 26.
- Launch management controller interface. Refer to "Launching the management controller interface for a server" on page 26.
- Manage the inventory data. Refer to "Managing the inventory" on page 26.
- View the alerts. Refer to "Managing the alerts" on page 27.
- View the event logs. Refer to "Managing the event logs" on page 27.
- View the audit logs. Refer to "Managing the audit logs" on page 28.
- View the power consumption and temperature. Refer to "Viewing the power consumption and temperature" on page 28.
- View the FoD keys. Refer to "Viewing the Feature on Demand keys" on page 28.
- Manage service data. Refer to "Managing service data of a server" on page 29.

Logging in to the Lenovo Server page

Before managing a specific server, users should log in to the Lenovo Server page first. This section describes how to log in to the Lenovo Server page of a server.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

Step 2. Return to the All Connections page, and click the drop-down list arrow ⌄ on the left of Lenovo XClarity Administrator IP address.
All managed servers are displayed.

Step 3. Click the name of the server on the list. The Lenovo Server page of this server is displayed.

Notes:

- If Lenovo XClariy Administrator is disconnected from the server, the server status might be "Unknown" or "Offline", and users cannot log in to the Lenovo Server page. In this case, add this server to the Lenovo XClarity Administrator again.
- After the server is added to Lenovo XClarity Administrator, the status might be "Pending" for a few minutes. After this process is completed, users can log in to the Lenovo Server page by clicking the name of this server.
- When the server status is "Offline", users cannot log in to the Lenovo Server page.

Viewing the overall information of a server

This section describes how to view the overall information of a managed server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. In the **Summary** pane of the Lenovo Server page, users can do one or more of the following:

- To view product name, user defined name, status, type model, host names (BMC), and IP addresses (BMC), click the **Summary** tab.
- To view the information of processors, memory, and PCI cards, click the **Installed Devices** tab.
- To view warranty number, start date, expiration date, and status, click the **Warranty** tab.

Note: Alternately, users can view the warranty information of all managed servers on the All Connections page. For more information, refer to "Viewing the warranty information of all managed servers" on page 18.

Syncing the inventory of a server

For a server, syncing the inventory is different from refreshing the inventory. When syncing the inventory, Lenovo XClarity Integrator obtains the inventory information from the server management module. This process takes a few minutes. When refreshing the inventory, Lenovo XClarity Integrator obtains the inventory information from the cache for customer experience and performance concern. This section describes how to sync the inventory of the components of a managed server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. In the **Summary** pane of the Lenovo Server page, click **Sync Inventory**.
The latest inventory information of components will be displayed.

Updating firmware for a server

Users can perform a firmware update job on a server through Lenovo XClarity Integrator, even if the server is installed without any OS.

The following features are supported in the **Updates** pane:

- **Compliance Policies**

If a compliance policy is used, users can still determine components in the policy to be updated for a specific server or all servers in a cluster. It is only available when the server is managed by Lenovo XClarity Administrator.

- **Latest Updates**

  This method does not use any policy, and users need to select a target version for each component to be updated. The target version must be later than the current installed version.

- **Update Logs**

  The **Update Logs** pane supports to delete, cancel, or retry the update jobs of current cluster nodes or servers.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

Step 2. Return to the All Connections page, and click the drop-down list arrow ⌄ on the left of Lenovo XClarity Administrator IP address. All managed servers are displayed.

Step 3. Click the name of the server on the list. The Lenovo Server page of this server is displayed. In the **Menu** pane of the Lenovo Server page, click **Updates**.

Step 4. In the **Updates** pane, select one of the following update methods:

- To assign a compliance policy for firmware updates:
  1. Click **Compliance Policies**.
  2. Select a policy from the drop-down list.

     Notes:
     - Users can click **Show Compliance Policy Definition** to view firmware updates in the policy.
     - Users can click › in front of the device to view firmware updates applicable to it in the policy. If **Compliance** is **Compliant** for a component, the installed version is already the same as or even higher than the target update version in the policy. Therefore, components with **Compliance** being **Not Compliant** are recommended to be updated.
  3. Click **Install Updates**.
- To select a target version for each component to be updated:
  1. Click **Latest Updates**.
  2. Do one of the following:
     - To view the latest firmware and driver updates, click **Reload local repository**.
     - To perform firmware and driver updates, select a target catalog or a target update package, and click **Install Updates**.
     - To manage local repository, click **Manage local repository**, and do one of the following:
       - To refresh catalog, select one or more target catalogs, and click **Refresh Catalog**.
       - To download the update packages, select one or more target catalogs or update packages, and click **Download**.
       - To delete the update packages, select one or more target machine types or update packages, and click **Delete**.
       - To filter out firmware updates or driver updates only, click **Firmware & Driver**, and select **Firmware** or **Driver**.
       - To filter out updates for Windows or Linux only, click **Windows & Linux**, and select **Windows** or **Linux**.
- To delete, cancel, or retry the update jobs of current cluster nodes or servers:
  1. Click **Update Logs**.
  2. Do one of the following:
     - To delete the update job, select one or more update jobs, and click **Delete**.
     - To cancel the update job, select one or more scheduled update jobs, and click **Cancel**.

  - To retry the update job, select an update job in **Failed**, **Stopped**, or **Cancelled** status, and click **Retry**.

Step 5. On the **Update Selection** tab, select or deselect components to be updated.

a. Select or deselect components to be updated in the **Select Items** pane.

Notes:

- Users can click < at the upper right corner of the **Select Items** pane to expand the **Preview** pane, or click × to remove a component.
- Operations on the **Select Items** and **Preview** panes are synchronized in real time.

b. (Optional) Enable **Forced update** to update firmware on the selected components even if the installed version is already up to date or later than the target version for update.

Notes:

- It's not allowed to apply firmware of earlier versions to device options, adapters, or disk drives.
- Forced update is not available if **Latest Updates** is used.

c. Click **Next**.

Step 6. On the **Update Download** tab, download or import update packages as required, and then click **Next**.

Step 7. On the **BitLocker** tab, set the BitLocker following the message, and click **Next**.

Step 8. On the **Options** tab, name and schedule the update job. Then, click **Next**.

Step 9. On the **Summary** tab, check the information about the update job, including the components to be updated, job name, schedule, and assigned policy if any.

Step 10. Click **Submit**.

The system then navigates to the Persistent Job page, and users can check the status of the update job.

Notes:

- If the Persistent Job page or the update wizard is closed, the system will then navigate back to the page before the update wizard is opened.
- To view the update history from any extension, refer to "Viewing the persistent jobs" on page 25.

Updating firmware for multiple servers

Through Lenovo XClarity Integrator, users can perform a batch firmware update job on multiple servers, including servers installed without any OS.

Before performing a batch firmware update job, ensure that the servers belong to the same machine type and are managed by the same Lenovo XClarity Administrator.

The following features are supported in the **Updates** pane:

- **Compliance Policies**

  If a compliance policy is used, users can still determine components in the policy to be updated for a specific server or all servers in a cluster. It is only available when the server is managed by Lenovo XClarity Administrator.
- **Latest Updates**

  This method does not use any policy, and users need to select a target version for each component to be updated. The target version must be later than the current installed version.
- **Update Logs**

The **Update Logs** pane supports to delete, cancel, or retry the update jobs of current cluster nodes or servers.

Procedure

Step 1. Connect to a Lenovo XClarity Administrator. Refer to "Connecting to a new or existing Lenovo XClarity Administrator" on page 15.

Step 2. Return to the All Connections page, and click the drop-down list arrow ⌄ on the left of Lenovo XClarity Administrator IP address. All managed servers are displayed.

Step 3. Select the servers to be updated in batches and click **Firmware Update** from the action pane above the server list. The firmware update wizard is displayed.

Step 4. Select one of the following update methods:

- To assign a compliance policy for firmware updates:
  1. Click **Compliance Policies**.
  2. Select a policy from the drop-down list.

     Notes:

     - Users can click **Show Compliance Policy Definition** to view firmware updates in the policy.
     - Users can click › in front of the device to view firmware updates applicable to it in the policy. If **Compliance** is **Compliant** for a component, the installed version is already the same as or even higher than the target update version in the policy. Therefore, components with **Compliance** being **Not Compliant** are recommended to be updated.
  3. Click **Install Updates**.
- To select a target version for each component to be updated:
  1. Click **Latest Updates**.
  2. Do one of the following:
     - To view the latest firmware and driver updates, click **Reload local repository**.
     - To perform firmware and driver updates, select a target catalog or a target update package, and click **Install Updates**.
     - To manage local repository, click **Manage local repository**, and do one of the following:
       - To refresh catalog, select one or more target catalogs, and click **Refresh Catalog**.
       - To download the update packages, select one or more target catalogs or update packages, and click **Download**.
       - To delete the update packages, select one or more target machine types or update packages, and click **Delete**.
       - To filter out firmware updates or driver updates only, click **Firmware & Driver**, and select **Firmware** or **Driver**.
       - To filter out updates for Windows or Linux only, click **Windows & Linux**, and select **Windows** or **Linux**.
- To delete, cancel, or retry the update jobs of current cluster nodes or servers:
  1. Click **Update Logs**.
  2. Do one of the following:
     - To delete the update job, select one or more update jobs, and click **Delete**.
     - To cancel the update job, select one or more scheduled update jobs, and click **Cancel**.
     - To retry the update job, select an update job in **Failed**, **Stopped**, or **Cancelled** status, and click **Retry**.

Step 5. On the **Update Selection** tab, select or deselect components to be updated.

a. Select or deselect components to be updated in the **Select Items** pane.

Notes:

- Users can click ‹ at the upper right corner of the **Select Items** pane to expand the **Preview** pane, or click × to remove a component.
- Operations on the **Select Items** and **Preview** panes are synchronized in real time.

b. (Optional) Enable **Forced update** to update firmware on the selected components even if the installed version is already up to date or later than the target version for update.

Notes:

- It's not allowed to apply firmware of earlier versions to device options, adapters, or disk drives.
- Forced update is not available if **Latest Updates** is used.

c. Click **Next**.

Step 6. On the **Update Download** tab, download or import update packages as required, and then click **Next**.

Step 7. On the **BitLocker** tab, set the BitLocker following the message, and click **Next**.

Step 8. On the **Options** tab, name and schedule the update job. Then, click **Next**.

Step 9. On the **Summary** tab, check the information about the update job, including the components to be updated, job name, schedule, and assigned policy if any.

Step 10. Click **Submit**.

The system then navigates to the Persistent Job page, and users can check the status of the update job.

Notes:

- If the Persistent Job page or the update wizard is closed, the system will then navigate back to the page before the update wizard is opened.
- To view the update history from any extension, refer to "Viewing the persistent jobs" on page 25.

Viewing the persistent jobs

In any of Lenovo extensions, click the Jobs icon ☰ in the top right corner, and click **Persistent Jobs**.

The Jobs pane is displayed on the right.

Launching the remote control on the Lenovo Server page

This section describes how to launch the remote control for a ThinkSystem, ThinkAgile, ThinkServer, NeXtScale, Converge, Flex System, and System x server on the Lenovo Server page.

Notes:

- Alternatively, users can also launch the remote control on the All Connections page. For more information, refer to "Launching the remote control" on page 18.
- For the server in the "Unknown", "Offline", or "Pending" status, the remote control cannot be launched.

Before you begin

For more information, refer to "Launching the remote control" on page 18.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. In the **Summary** pane of the Lenovo Server page, click **Launch Remote Control**.

Step 3. When the security warning prompts, click **Accept**.

Powering on, powering off, and restarting a server

This section describes how to power on, power off, and restart a server on the Lenovo Server page.

Notes:

- Alternatively, users can also power on, power off, and restart a server on the All Connections page. For more information, refer to "Powering on, powering off, and restarting one or more servers" on page 17.
- This process takes a few minutes. A job will be created when the process starts. To view the results, click the Jobs icon ☰ on the top right corner of the Lenovo Server page, and click **Persistent Jobs**.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. In the **Summary** pane of the Lenovo Server page, click **Power On**, **Power Off**, or **Reboot**.

Step 3. When the Warning window is displayed, click **Yes** to continue.

Launching the management controller interface for a server

This section describes how to launch the management controller interface for a server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. In the **Summary** pane of the Lenovo Server page:

a. Click the **Summary** tab.

b. On the **Summary** tab, select an IP address in the **IP address (BMC)** area.
The management controller interface will be displayed.

c. In the management controller interface, input the BMC user name and password, and click **Log In**.

Managing the inventory

This section describes how to view, sync, and download the inventory data, and check the firmware updates of a server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. On the Lenovo Server page, click **Inventory** in the left navigation pane.
The **Inventory** pane is displayed.

Step 3. In the **Inventory** pane, users can do one or more of the following:

- To obtain the latest inventory data, click **Sync Inventory**.
- To check the firmware updates, click **Reload Local Repository**, and then check the **Latest in Repository** column in the **Firmware** area to view the latest local firmware updates available. To view latest firmware updates on Web, refer to Chapter 8 "Managing the system updates repository" on page 61.

  Notes:

  - This process requires access to Internet. If the firewall is activated in the network, configure firewall to enable the servers managed by Lenovo XClarity Administrator to perform these operations. For more information about firewall and proxy servers of Lenovo XClarity Administrator, refer to Firewalls and proxy servers.
  - This process takes a few minutes.
  - The Lenovo ThinkServer servers do not support this feature.

- To download the inventory data:
  1. Click **Export**.
  2. When the “How do you want to open this file?” window is displayed, click **Save**. The inventory data will be saved in the local file.

Managing the alerts

This section describes how to view and download the alerts of a server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to “Logging in to the Lenovo Server page” on page 20.

Step 2. On the Lenovo Server page, click **Alerts** in the left navigation pane.
The **Alerts** pane is displayed.

Step 3. In the **Alerts** pane, users can do one or more of the following:

- To view the details of an alert:
  1. Select an alert from the Alerts list. The information of this alert will be displayed below the list.
  2. Users can do one or more of the following:
     - To view the property information, click the **Properties** tab.
     - To view the description and solution of this alert, click the **Details** tab.
- To download the alerts data:
  1. Click **Export**.
  2. When the “How do you want to open this file?” window is displayed, click **Save**. The alerts data will be saved in the local file.
- To view more columns in the Alerts list:
  1. Click **Customize Columns**. The **Customize Alerts Columns** pane is displayed on the right.
  2. Select one or more target columns.
  3. Return to the **Alerts** pane. The information of selected columns will be displayed.

Managing the event logs

This section describes how to view and download the event logs of a server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to “Logging in to the Lenovo Server page” on page 20.

Step 2. On the Lenovo Server page, click **Event Log** in the left navigation pane.
The **Event Log** pane is displayed.

Step 3. In the **Event Log** pane, users can do one or more of the following:

- To view the details of an event log:
  1. Select an event log from the Event Log list. The information of this event log will be displayed below the list.
  2. Users can do one or more of the following:
     - To view the property information, click the **Properties** tab.
     - To view the description and solution of this event log, click the **Details** tab.
- To download the event logs:
  1. Click **Export**.
  2. When the “How do you want to open this file?” window is displayed, click **Save**. The event logs will be saved in the local file.
- To view more columns in the Event Log list:
  1. Click **Customize Columns**. The **Customize EventLog Columns** pane is displayed on the right.
  2. Select one or more target columns.
  3. Return to the **Event Log** pane. The information of selected columns will be displayed.

Managing the audit logs

This section describes how to view and download the audit logs of a server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. On the Lenovo Server page, click **Audit Log** in the left navigation pane.
The **Audit Log** pane is displayed.

Step 3. In the **Audit Log** pane, users can do one or more of the following:

- To view the details of an audit log:
  1. Select an audit log from the Audit Log list. The information of this audit log will be displayed below the list.
  2. Users can do one or more of the following:
     - To view the property information, click the **Properties** tab.
     - To view the description and solution of this audit log, click the **Details** tab.
- To download the audit logs:
  1. Click **Export**.
  2. When the "How do you want to open this file?" window is displayed, click **Save**. The audit logs will be saved in the local file.
- To view more columns in the Audit Log list:
  1. Click **Customize Columns**. The **Customize AuditLog Columns** pane is displayed on the right.
  2. Select one or more target columns.
  3. Return to the **Audit Log** pane. The information of selected columns will be displayed.

Viewing the power consumption and temperature

This section describes how to view the power consumption and temperature of a server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. On the Lenovo Server page, click **Power Consumption and Temperature** in the left navigation pane.
The **Power Consumption and Temperature** pane is displayed.

Step 3. In the **Power Consumption and Temperature** pane, users can do one or more of the following:

- View the information of system power consumption, system temperature (Inlet), CPU power consumption, and memory power consumption of the server displayed on this pane.
- To switch between the Celsius and Fahrenheit temperature, click the temperature button °C or °F in the top right corner.

Viewing the Feature on Demand keys

This section describes how to view the FoD keys of a server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to "Logging in to the Lenovo Server page" on page 20.

Step 2. On the Lenovo Server page, users can do one or more of the following:

- To view the information of all FoD keys installed on the server, click **Feature on Demand Keys** in the left navigation pane.
- To download the information of FoD keys:
  1. Click **Export**.

2. When the “How do you want to open this file?” window is displayed, click **Save**. The FoD keys will be saved in the local file.

Managing service data of a server

This section describes how to manage the service data of a server on the Lenovo Server page.

Procedure

Step 1. Log in to the Lenovo Server page. Refer to “Logging in to the Lenovo Server page” on page 20.

Step 2. On the Lenovo Server page, click **Service Data** in the left navigation pane.
The **Service Data** pane is displayed.

Step 3. In the **Service Data** pane, users can do one or more of the following:

- To collect the service data files, click **Collect Service Data**.

  Note: This process takes a few minutes.
- To download the service data files, click **Download Files**.
- To delete the service data files, select one or more service data files, and click **Delete**.
- To export the service data files, select one or more service data files, and click **Export Logs**.

Chapter 5. Managing servers through Server Manager

Users can use Lenovo XClarity Integrator with the Server Manger solution. This chapter describes how to manage the server through Lenovo XClarity Integrator in Server Manager.

Connecting to Lenovo XClarity Integrator in Server Manager

Before managing the server in Server Manager, users should connect to Lenovo XClarity Integrator in Server Manager.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. In the top left corner, click the drop-down list arrow ∨ on the right of **Windows Admin Center**.

Step 3. Click **Server Manager**.
The Server connections page is displayed.

Step 4. On the Server connections page:

a. Select the target server.

b. When the **Specify your credentials** pane is displayed, select an existing account or input a new account.

c. Click **Continue**. The server page is displayed.

Step 5. In the left navigation pane of the server page, click **Lenovo XClarity Integrator** or XC.

Note: If the managed server is not a Lenovo server, Lenovo XClarity Integrator will not be displayed in the left navigation bar.

Managing a server with Lenovo XClarity Administrator

After entering into the Lenovo XClarity Integrator page in Server Manager, a message indicating that the server is currently not managed by a management server might be displayed. This section describes how to manage a server with Lenovo XClarity Administrator in Server Manager.

Note: If the server is not in the “Unknown”, “Pending”, or “Offline” status, and the Lenovo XClarity Administrator that manages this server is connected, this Web page will not be displayed.

Procedure

Step 1. Connect to Lenovo XClarity Integrator in Server Manager. Refer to “Connecting to Lenovo XClarity Integrator in Server Manager” on page 31.

Step 2. Select **Lenovo XClarity Administrator**.

Step 3. Users can do one or more of the following:

- To connect to a current registered Lenovo XClarity Administrator:
  1. Select **Connect to a registered XClarity Administrator management server**.
  2. Select the IP address of a registered Lenovo XClarity Administrator from the drop-down list.
  3. Click **Connect**.

     The **Connect to Lenovo XClarity Administrator** pane will be displayed on the right.
  4. Input the user name and password. Ensure that the user provided meets the user privilege and role requirements and has enough permissions to perform desired operations.
  5. Click **Submit**.

Note: If one or more Lenovo XClarity Administrators are connected, users can select one Lenovo XClarity Administrator to manage the server.

- To manage the server with a connected Lenovo XClarity Administrator:
  1. Select **Add this server to a connected XClarity Administrator management server**.
  2. Select the IP address of a connected Lenovo XClarity Administrator from the drop-down list.
  3. Click **Add to**.

     The **Manage Lenovo Rack or Tower Servers** pane will be displayed on the right.
  4. Input the BMC IP address, user name, and password.
  5. Click **Manage**.
- To connect to a new Lenovo XClarity Administrator:
  1. Select **Connect to a new XClarity Administrator management server**.
  2. Click **Add**.

     The **Connect to Lenovo XClarity Administrator** pane will be displayed on the right.
  3. Input the IP address, user name, and password. Ensure that the user provided meets the user privilege and role requirements and has enough permissions to perform desired operations.
  4. Click **Submit**.
- To disconnect a connected Lenovo XClarity Administrator:
  1. Select **Disconnect a connected XClarity Administrator management server**.
  2. Select the IP address of a registered Lenovo XClarity Administrator from the drop-down list.
  3. Click **Disconnect**.

     A warning window will be displayed for users to confirm your operation.
  4. Click **Yes**.

Managing a server without Lenovo XClarity Administrator

After entering into the Lenovo XClarity Integrator page in Server Manager, a message indicating that the server is currently not managed by a management server might be displayed. This section describes how to manage a server without Lenovo XClarity Administrator, that is, through native OS management in Server Manager.

Native OS management is a way to manage the hardware when no Lenovo XClarity Administrator is available. To use this function, log in to the XCC Web GUI and enable IPMI over KCS Access, Ethernet Over USB, and REST/CIM Over HTTPS.

Note: If the server is not in the “Unknown”, “Pending”, or “Offline” status, and the Lenovo XClarity Administrator that manages this server is connected, this Web page will not be displayed.

Procedure

Step 1. Connect to Lenovo XClarity Integrator in Server Manager. Refer to “Connecting to Lenovo XClarity Integrator in Server Manager” on page 31.

Step 2. Select **Native OS Management**.

Step 3. Click **Take Me There**. If the **Native OS Management** window pops up, do the following:

a. Click **Lenovo WDAC policy**, and save the policy file in `c:\wdac`.

b. Open Windows PowerShell, run `Add-ASWDACSupplementalPolicy -Path c:\wdac\Contoso-policy.xml` to deploy the policy, and run `Get-ASLocalWDACPolicyInfo` to check the status of the new policy. For more information, see Step 4-5 in Create a WDAC supplemental policy.

c. Go back to the server page, click **Take Me There** again, and flash the webpage.

Step 4. After the initialization, the Summary page of the managed server is automatically displayed.

Step 5. The **Data Source** field under the server name is displayed as **Native OS Management**. Users can click the **Switch to Lenovo XClarity Administrator** link to return to the server home page and then add a Lenovo XClarity Administrator to manage this server.

Notes:

- The views for native OS management are the same as those for LXCA-managed servers, while some detailed information might not be available, such as alert details. For the information not available, consider using Lenovo XClarity Administrator.
- Native OS management is inapplicable to ThinkServer and ThinkSystem SR635/SR655 servers. For servers enabled with Storage Spaces Direct, native OS management is disabled by default. To enable native OS management for servers enabled with Storage Spaces Direct, refer to “Configuring native OS management” on page 12.

Viewing the details of a managed server

After connecting to Lenovo XClarity Integrator in Server Manager, users can view the details of a managed server. For more information, refer to “Managing a server” on page 20.

Updating firmware/drivers for a server

The **Updates** pane displays the best recipes, latest updates, and update logs of firmware and drivers.

The following features are supported in the **Updates** pane:

- **Best Recipes (Recommended)**

  Best recipe is also a compliance policy, but includes firmware and driver updates. This method does not allow users to select part of components from the recipe for update. All components in the recipe will be updated for all servers in a cluster.

  This feature is supported only by specific server models. Refer to Features supported by specific server models.

  For details about the best recipe, see ThinkAgile MX Certified Node Best Recipe.
- **Compliance Policies**

  If a compliance policy is used, users can still determine components in the policy to be updated for a specific server or all servers in a cluster. It is only available when the server is managed by Lenovo XClarity Administrator.
- **Latest Updates**

  This method does not use any policy, and users need to select a target version for each component to be updated. The target version must be later than the current installed version.
- **Update Logs**

  The **Update Logs** pane supports to delete, cancel, or retry the update jobs of current cluster nodes or servers.

Procedure

Step 1. Connect to Lenovo XClarity Integrator in Server Manager. Refer to “Connecting to Lenovo XClarity Integrator in Server Manager” on page 31.

Step 2. Do one of the following:

- Ensure that the target server is managed. In the **Menu** pane of the Lenovo Server page, click **Updates**.

  Notes:

  - Users can refer to “Managing a server with Lenovo XClarity Administrator” on page 31 or “Managing a server without Lenovo XClarity Administrator” on page 32.
  - The **Compliance Policies** feature is only supported when managing a server with Lenovo XClarity Administrator.
- In the left navigation pane of the server page, click **Lenovo XClarity Integrator — Compliance and Updates** or XC.

Step 3. In the **Updates** pane, select one of the following update methods:

- To assign a best recipe for firmware/driver updates:
  1. Click **Best Recipes (Recommended)**.
  2. Select the best recipe from the drop-down list, and do one of the following:
     - To view firmware/driver updates in the best recipe, click **Show Best Recipe Definition**.
     - To refresh the recipe, click **Refresh Best Recipe**.
     - To view the applicable firmware/driver updates, click > in front of a device.

       Notes:
       - If **Compliance** is **Compliant** for a component, the installed version is already the same as or even higher than the target update version in the policy. Therefore, components with **Compliance** being **Not Compliant** are recommended to be updated.
       - The table only shows the components defined in the best recipe.
  3. Click **Install Updates**.
- To assign a compliance policy for firmware updates:
  1. Click **Compliance Policies**.
  2. Select a policy from the drop-down list.

     Notes:
     - Users can click **Show Compliance Policy Definition** to view firmware updates in the policy.
     - Users can click > in front of the device to view firmware updates applicable to it in the policy. If **Compliance** is **Compliant** for a component, the installed version is already the same as or even higher than the target update version in the policy. Therefore, components with **Compliance** being **Not Compliant** are recommended to be updated.
  3. Click **Install Updates**.
- To select a target version for each component to be updated:
  1. Click **Latest Updates**.
  2. Do one of the following:
     - To view the latest firmware and driver updates, click **Reload local repository**.
     - To perform firmware and driver updates, select a target catalog or a target update package, and click **Install Updates**.
     - To manage local repository, click **Manage local repository**, and do one of the following:
       - To refresh catalog, select one or more target catalogs, and click **Refresh Catalog**.
       - To download the update packages, select one or more target catalogs or update packages, and click **Download**.
       - To delete the update packages, select one or more target machine types or update packages, and click **Delete**.
       - To filter out firmware updates or driver updates only, click **Firmware & Driver**, and select **Firmware** or **Driver**.
       - To filter out updates for Windows or Linux only, click **Windows & Linux**, and select **Windows** or **Linux**.
- To delete, cancel, or retry the update jobs of current cluster nodes or servers:
  1. Click **Update Logs**.
  2. Do one of the following:
     - To delete the update job, select one or more update jobs, and click **Delete**.

  - To cancel the update job, select one or more scheduled update jobs, and click **Cancel**.
  - To retry the update job, select an update job in **Failed**, **Stopped**, or **Cancelled** status, and click **Retry**.

Step 4. On the **Update Selection** tab, select or deselect components to be updated.

a. Select or deselect components to be updated in the **Select Items** pane.

Notes:

- Users can click ‹ at the upper right corner of the **Select Items** pane to expand the **Preview** pane, or click × to remove a component.
- Operations on the **Select Items** and **Preview** panes are synchronized in real time.

b. (Optional) To update firmware/drivers on the selected components even if the installed version is already up to date or later than the target version for update, enable **Forced update**.

Notes:

- It's not allowed to apply firmware or drivers of earlier versions to device options, adapters, or disk drives.
- Forced update is available only when **Compliance Policy** is used.

c. Click **Next**.

Step 5. On the **Update Download** tab, download or import update packages as required, and then click **Next**.

Step 6. On the **Clustered Roles Migration** tab, click **Next**.

Attention: The cluster roles cannot be migrated when the cluster consists only one server node; otherwise, all running clustered roles, including clustered and non-clustered virtual machines, will be disrupted after the server node is restarted.

Note: Clustered roles migration is automatically enabled on all servers in the cluster.

Clustered Roles Migration performs the following tasks:

1. Puts one cluster node into maintenance mode, and moves the clustered roles off the node.
2. Install system updates.
3. Performs a restart.
4. Brings the node out of maintenance mode, and restores the clustered roles on the node.
5. Moves to the next cluster node.

Step 7. On the **OS Credential** tab, click **Credential Needed** to input the account, user name, and password of a Windows administrator account, and then click **Next**.

Notes:

- For the cluster node, the account should be the Active Directory domain account included in the local Administrators group.
- For the non-cluster server, the account should be the Active Directory domain account included in the local Administrators group or the built-in administrator account.
- OS credentials are required if one or more of the following operations are required:
  - Firmware/driver update in native OS management mode
  - Clustered roles migration

Step 8. On the **BitLocker** tab, set the BitLocker following the message, and click **Next**.

Step 9. On the **Options** tab, name and schedule the update job. Then, click **Next**.

Step 10. On the **Summary** tab, check the information about the update job, including the components to be updated, job name, schedule, and assigned policy if any.

Step 11. Click **Submit**.

The system then navigates to the Persistent Job page, and users can check the status of the update job.

Notes:

- If the Persistent Job page or the update wizard is closed, the system will then navigate back to the page before the update wizard is opened.
- To view the update history from any extension, refer to "Viewing the persistent jobs" on page 25.

Managing the system updates repository

This section describes how to manage the system updates repository for the target servers.

To download, back up, or restore system updates, refer to Chapter 8 "Managing the system updates repository" on page 61.

Chapter 6. Managing servers through Cluster Manager

Users can use Lenovo XClarity Integrator with the Cluster Manager solution. This chapter describes how to manage the server through Lenovo XClarity Integrator in Cluster Manager.

Notes:

- For Windows Admin Center 1904.1, Lenovo XClarity Integrator supports both Hyper-Converged Cluster Manager and Failover Cluster Manager.
- For Windows Admin Center 1910, Lenovo XClarity Integrator supports Cluster Manager since Hyper-Converged Cluster Manager and Failover Cluster Manager are combined, but with slight function differences depending on whether Storage Spaces Direct is enabled on a cluster.

Connecting to Lenovo XClarity Integrator in Cluster Manager

Before managing the server in Cluster Manager, users should connect to Lenovo XClarity Integrator in Cluster Manager.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. In the top left corner, click the drop-down list arrow ⌄ on the right of **Windows Admin Center**

Step 3. Click **Cluster Manager**.
The Cluster connections page is displayed.

Step 4. On the Cluster connections page:

a. Select a cluster.

b. When the **Specify your credentials** pane is displayed, select an existing account or input a new account.

c. Click **Continue**. The cluster page is displayed.

Step 5. In the left navigation pane of the cluster page, click **Lenovo XClarity Integrator** or XC.

Notes:

- If all cluster nodes are detected to be managed by connected Lenovo XClarity Administrators, the Lenovo XClarity Integrator dashboard will be displayed.
- If any cluster nodes are detected to be not managed by any connected Lenovo XClarity Administrator, Lenovo XClarity Integrator will prompt users to choose a management approach, either through Lenovo XClarity Administrator (see “Managing cluster nodes with Lenovo XClarity Administrator” on page 37) or native OS management (see “Managing cluster nodes without Lenovo XClarity Administrator” on page 38).

Managing cluster nodes with Lenovo XClarity Administrator

After entering into the Lenovo XClarity Integrator page in Cluster Manager, a message indicating that one or more servers are currently not managed by a management server might be displayed. This section describes how to manage cluster nodes with Lenovo XClarity Administrator in Cluster Manager.

Note: If all Lenovo XClarity Administrators that manage these servers are connected, this page will not be displayed.

Procedure

Step 1. Connect to Lenovo XClarity Integrator in Cluster Manager. Refer to "Connecting to Lenovo XClarity Integrator in Cluster Manager" on page 37.

Step 2. Select **Lenovo XClarity Administrator**.

Step 3. Users can do one or more of the following:

- To connect to a current registered Lenovo XClarity Administrator:
  1. Select **Connect to a registered XClarity Administrator management server**.
  2. Select the IP address of a registered Lenovo XClarity Administrator from the drop-down list.
  3. Click **Connect**.

     The **Connect to Lenovo XClarity Administrator** pane will be displayed on the right.
  4. Input the user name and password. Ensure that the user provided meets the user privilege and role requirements and has enough permissions to perform desired operations.
  5. Click **Submit**.

  Note: If one or more Lenovo XClarity Administrators are connected, users can select one Lenovo XClarity Administrator to manage the server.
- To manage the nodes with a connected Lenovo XClarity Administrator:
  1. Select **Add nodes to a connected XClarity Administrator management server**.
  2. Select the IP address of a connected Lenovo XClarity Administrator from the drop-down list.
  3. Click **Add to**.

     The **Manage Lenovo Rack or Tower Servers** pane will be displayed on the right.
  4. Input a BMC IP address, click the add icon +, and input another BMC IP address. Repeat this step until all rack or tower servers are added. Then input the user name and password.

     Note: It is recommended to manage all the cluster nodes with the same Lenovo XClarity Administrator.
  5. Click **Manage**.
- To connect to a new Lenovo XClarity Administrator:
  1. Select **Connect to a new XClarity Administrator management server**.
  2. Click **Add**.

     The **Connect to Lenovo XClarity Administrator** pane will be displayed on the right.
  3. Input the IP address, user name, and password. Ensure that the user provided meets the user privilege and role requirements and has enough permissions to perform desired operations.
  4. Click **Submit**.
- To disconnect a connected Lenovo XClarity Administrator:
  1. Select **Disconnect a connected XClarity Administrator management server**.
  2. Select the IP address of a registered Lenovo XClarity Administrator from the drop-down list.
  3. Click **Disconnect**.

     A warning window will be displayed for users to confirm your operation.
  4. Click **Yes**.

Managing cluster nodes without Lenovo XClarity Administrator

After entering into the Lenovo XClarity Integrator page in Cluster Manager, a message indicating that one or more servers are currently not managed by a management server might be displayed. This section describes how to manage cluster nodes without Lenovo XClarity Administrator, that is, through native OS management in Cluster Manager.

Native OS management is a way to manage the hardware when no Lenovo XClarity Administrator is available. To use this function, log in to the XCC Web GUI and enable IPMI over KCS Access, Ethernet Over USB, and REST/CIM Over HTTPS.

Note: If all Lenovo XClarity Administrators that manage these servers are connected, this page will not be displayed.

Procedure

Step 1. Connect to Lenovo XClarity Integrator in Cluster Manager. Refer to "Connecting to Lenovo XClarity Integrator in Cluster Manager" on page 37.

Step 2. Select **Native OS Management**.

Step 3. Click **Take Me There**. If the **Native OS Management** window pops up, do the following:

a. Click **Lenovo WDAC policy**, and save the policy file in `c:\wdac`.

b. Open Windows PowerShell, run `Add-ASWDACSupplementalPolicy -Path c:\wdac\Contoso-policy.xml` to deploy the policy, and run `Get-ASLocalWDACPolicyInfo` to check the status of the new policy. For more information, see Step 4-5 in Create a WDAC supplemental policy.

c. Go back to the server page, click **Take Me There** again, and flash the webpage.

Step 4. After the initialization, the Dashboard page of the managed server is automatically displayed.

Notes:

- The views for native OS management are the same as those for LXCA-managed servers, while some detailed information might not be available, such as alert details. For the information not available, consider using Lenovo XClarity Administrator.
- Native OS management is inapplicable to ThinkServer and ThinkSystem SR635/SR655 servers. For servers enabled with Storage Spaces Direct, native OS management is disabled by default. To enable native OS management for servers enabled with Storage Spaces Direct, refer to "Configuring native OS management" on page 12.

Managing drives used by cluster nodes in Disk Manager

This section describes how to manage drives used by cluster nodes in Disk Manager. This feature is supported only by specific server models. Refer to Features supported by specific server models.

In this section, do one or more of the following:

- View the overall information of pools, drives, and servers of a cluster. Refer to "Viewing the overall information of pools, drives, and servers of a cluster" on page 40.
- Turn on or off the location LED of a server. Refer to "Turning on or off the location LED of a server" on page 40.
- Turn on or off the location LED of a drive. Refer to "Turning on or off the location LED of a drive" on page 41.
- Replace a drive in a storage pool. Refer to "Replacing a drive in a storage pool" on page 41.
- Remove a drive from a server. Refer to "Removing a drive from a server" on page 42.
- Add a non-pooled drive to a storage pool. Refer to "Adding a drive to a storage pool" on page 42.

Logging in to the Disk Manager page

Before managing drives used by servers in a cluster, users should log in to the Disk Manager page first. This section describes how to log in to the Disk Server page of a cluster.

Procedure

Step 1. Connect to Lenovo XClarity Integrator in Cluster Manager. Refer to "Connecting to Lenovo XClarity Integrator in Cluster Manager" on page 37.

Step 2. Connect to Lenovo XClarity Administrator in Cluster Manager. Refer to "Managing cluster nodes with Lenovo XClarity Administrator" on page 37.

Step 3. Click **Disk Manager** from the menu.
The Disk Manager page is displayed.

The Disk Manager page consists of three main panels:

- Disk list: lists all drives used by servers in the cluster, which are classified by storage pool. Server name, media type, bus type, status, and capacity of a drive can be queried from the list.
- Information panel: displays details about a selected drive, server, or pool. Operations on drives or servers are supported from the information panel, such as **Light On**, **Light Off**, **Replace**, **Remove**, and **Add to Pool**.
- Graphical View: displays the front and rear views of servers in the cluster.

Viewing the overall information of pools, drives, and servers of a cluster

This section describes how to view the overall information of pools, drives, and servers of a cluster on the Disk Manager page.

Procedure

Step 1. Log in to the Disk Manager page. Refer to "Logging in to the Disk Manager page" on page 39.

Step 2. On the Disk Manager page, users can do one or more of the following:

- To view the information of a storage pool, click the name of the pool. The pool details will be displayed in the lower left panel.

  Note: No information will be displayed for clicking **Non-pooled Drives**.
- To view the information of a drive, click its name. The drive details will be displayed in the lower left panel, and the selected drive will also be highlighted in the **Graphical View** panel to indicate its actual location on the server to which it belongs.

  Note: Clicking a specific drive slot in the **Graphical View** panel can also help users locate the drive in the disk list, with drive details displayed in the lower left panel at the same time.
- To view the information of a server, click the left or right latch or an empty slot of the server in the **Graphical View** panel. The server details will be displayed in the lower left panel.
- To toggle between the front and rear views of a server, click ⇄ in the upper right corner of its graphical view.

Turning on or off the location LED of a server

This section describes how to turn on or off the location LED of a server on the Disk Manager page so as to visually locate the server.

Procedure

Step 1. Log in to the Disk Manager page. Refer to "Logging in to the Disk Manager page" on page 39.

Step 2. In the **Graphical View** panel, click the left or right latch or an empty slot of the target server.
The sever details are displayed in the lower left panel.

Step 3. In the lower left panel, click **Light On** or **Light Off** to turn on or off the location LED in the upper right corner of the server.

- If users click **Light On**, the location LED of the server turns blue in real time in the **Graphical View** panel.
- If users click **Light Off**, the location LED of the server turns unlit in real time in the **Graphical View** panel.
- Any status change of the location LED is synchronized to the physical server in real time, which helps to visually locate the server.

Turning on or off the location LED of a drive

This section describes how to turn on or off the location LED of a drive on the Disk Manager page so as to visually locate the drive.

Procedure

Step 1. Log in to the Disk Manager page. Refer to "Logging in to the Disk Manager page" on page 39.

Step 2. In the disk list on the left, click the name of the target drive.
The drive details are displayed in the lower left panel.

Step 3. In the lower left panel, click **Light On** or **Light Off** to change the status of the location LED in the lower left corner of the drive.

- If users click **Light On**, the location LED of the drive blinks yellow in real time in the **Graphical View** panel.
- If users click **Light Off**, the location LED of the drive turns unlit in real time in the **Graphical View** panel.
- Any status change of the location LED is synchronized to the physical drive in real time, which helps to visually locate the drive.
- Currently, NVMe drives do not support the status toggle of the location LED through Disk Manager.

Replacing a drive in a storage pool

This section describes how to replace a drive in a storage pool on the Disk Manager page.

Procedure

Step 1. Log in to the Disk Manager page. Refer to "Logging in to the Disk Manager page" on page 39.

Step 2. In the disk list on the left, click the name of the drive to be replaced under a storage pool.
The drive details are displayed in the lower left panel.

Step 3. In the lower left panel, click **Replace**.
The Replace Drive wizard is displayed.

Step 4. Retire the drive to be replaced from the storage pool.

a. On the **Retire from Storage Pool** tab, click **Yes** in the confirmation dialog below the graphical view.
The drive will be retired and then removed from the pool, which may take some time to complete.

b. Click **Next** if a message is displayed to indicate that the drive has been successfully removed from the storage pool.

Step 5. Pull out the drive to be replaced and insert a new one.

a. (Optional) On the **Pull Out and Insert** tab, click ● to turn on the server or disk location LED so as to visually locate the drive to be replaced.

b. Remove the drive to be replaced from the server and insert a new one.

c. Return to the **Pull Out and Insert** tab, and click **Yes** in the confirmation dialog below **Server Location LED** and **Disk Location LED**.

Note: It may take some time for the process to complete. Information about the new drive will be displayed if the drive replacement is successful.

d. Click **Next** if a message is displayed to indicate that the drive has been successfully replaced.

The new drive is added to the storage pool automatically.

Step 6. On the **More Operations** tab, click ● to start rebalancing the pool immediately if needed. Then, click **Next**.

Step 7. On the **Summary** tab, view the operation result. If desired operations are completed, click **Finish**.

The drive is successfully replaced with a new one.

Removing a drive from a server

This section describes how to remove a drive from a server on the Disk Manager page.

Procedure

Step 1. Log in to the Disk Manager page. Refer to "Logging in to the Disk Manager page" on page 39.

Step 2. In the disk list on the left, click the name of the drive to be removed.
The drive details are displayed in the lower left panel.

Step 3. In the lower left panel, click **Remove**.
The Remove Drive wizard is displayed.

Step 4. Do either of the following:

- If the drive to be removed is not in a storage pool, directly click **Next** and go to Step 5 on page 42.
- If the drive to be removed is in a storage pool, continue the following steps.

a. On the **Retire from Storage Pool** tab, click **Yes** in the confirmation dialog below the graphical view.
The drive will be retired and then removed from the pool, which may take some time to complete.

b. Click **Next** if a message is displayed to indicate that the drive has been successfully removed from the storage pool.

Step 5. Pull out the drive from the server.

a. (Optional) On the **Pull Out** tab, click ● to turn on the server or disk location LED so as to visually locate the drive to be removed.

b. Remove the drive from the server.

c. Return to the **Pull Out** tab, and click **Next**.

Step 6. On the **Summary** tab, view the operation result. If desired operations are completed, click **Finish**.

The drive is successfully removed from the server.

Adding a drive to a storage pool

This section describes how to add a non-pooled drive to a storage pool on the Disk Manager page.

Procedure

Step 1. Log in to the Disk Manager page. Refer to "Logging in to the Disk Manager page" on page 39.

Step 2. In the disk list on the left, click the name of the drive to be added to a storage pool.
The drive details are displayed in the lower left panel.

Step 3. In the lower left panel, click **Add to Pool**.
The Add Drive to Pool wizard is displayed.

Step 4. Select a target pool.

a. Select a target pool from the **Select a pool** drop-down list, and then click **Add**.

b. Click **Next** if a message is displayed to indicate that the drive has been successfully added to the storage pool.

Step 5. On the **More operation** tab, click ● to start rebalancing the pool immediately if needed. Then, click **Next**.

Step 6. On the **Summary** tab, view the operation result. If desired operations are completed, click **Finish**.

The drive is successfully added to the storage pool.

Working with Lenovo Cluster Dashboard

After connecting to Lenovo XClarity Integrator, users can view the status of all managed Lenovo servers, their power supplies, fans, firmware consistency, the latest active alerts, and the power consumption and temperature of the cluster nodes through Lenovo Cluster Dashboard.

The following areas are displayed on the Dashboard page:

- **Servers**: Refer to "Managing cluster nodes" on page 43.
- **Alerts**: Refer to "Managing alerts" on page 43.
- **Firmware Consistency**: Refer to "Managing firmware consistency" on page 44.
- **Cluster Power Consumption**: Refer to "Managing the cluster power consumption" on page 44.
- **System Temperature (Inlet)**: Refer to "Managing the system temperature" on page 44.
- **Power Supplies**: Refer to "Managing power supplies" on page 44.
- **Processor Cores**: Refer to "Managing processor cores" on page 56.
- **Fans**: Refer to "Managing fans" on page 45.

Managing cluster nodes

The **Servers** area displays the overall status of all cluster nodes.

Users can do one or more of the following:

- To view the cluster node with the "Critical", "Warning", "Normal", or "Unknown" status, click the number in the Status column.
- To view the overall status of all cluster nodes, or manage the cluster nodes:
  1. Click **VIEW ALL**. The Servers page will be displayed.
  2. On the Servers page, users can do one or more of the following:
     - To launch the remote control of a cluster node, select a cluster node, and click **Launch Remote Control**.

       Note: This action is not supported in native OS management mode.
     - To view the alerts of a cluster node, click the health status of this cluster node.
     - To view the overall information of a cluster node, click the BMC host name of this cluster node.
     - To view more information of the cluster nodes, click **Customize Columns** on the Servers page, select one or more target columns, and return to the Servers page.

Managing alerts

The **Alerts** area displays the latest three alerts of all cluster nodes.

Users can do one or more of the following:

- To view the latest alerts, click the link of Event ID (Message ID).
- To view all alerts of the cluster nodes:
  1. Click **VIEW ALL**. The Alerts page will be displayed.
  2. On the Alerts page, users can do one or more of the following:
     - To view the details of an alert, click this alert.
     - To export the alerts information as a CSV file, click **Export**.

– To view more information of the alerts, click **Customize Columns** on the Alerts page, select one or more target columns, and return to the Alerts page.

Managing firmware consistency

The **Firmware Consistency** area indicates whether the versions of the cluster nodes firmware are the same.

To view the firmware consistency report, click **VIEW DETAILS**.

Notes:

- It is recommended that all cluster nodes use the firmware of the same version in the same hardware component controllers.
- Firmware Consistency Report displays the BMC, UEFI, HBA, and Storage NIC firmware versions, which are the consistency indicators for Hyper-Converged Cluster. The BMC and UEFI firmware versions are the consistency indicators for Failover Cluster. If BMC, UEFI, HBA and Storage NIC are not configured in the target cluster nodes, or the firmware versions are N/A or not available, the firmware versions are not consistent across cluster nodes.
- For each hardware component controller, the default baseline firmware version is the one that counts the most. Users could select either as a baseline.

To update firmware for cluster nodes, refer to “Updating firmware/drivers for cluster nodes” on page 45.

Managing the cluster power consumption

The **Cluster Power Consumption** area displays the average power consumption of the cluster nodes.

Users can click the **Cluster Power Consumption** tab to view the average power consumption of the cluster nodes.

Managing the system temperature

The **System Temperature (Inlet)** area displays the average temperature of the cluster nodes.

Users can do one or more of the following:

- To view the average temperature of the cluster nodes, click the **System Temperature (Inlet)** tab.
- To switch between Celsius and Fahrenheit, click the **System Temperature (Inlet)** tab, and click the temperature button ⬤ °C or ○ °F in the top right corner.

Managing power supplies

The **Power Supplies** area displays the overall status of power supplies of all cluster nodes.

Users can do one or more of the following:

- To view the power supplies in the “Critical”, “Warning”, “Normal”, or “Unknown” status, click the number in the Status column.
- To view the overall status of power supplies of all cluster nodes:
  1. Click **VIEW ALL**. The Power Supplies page will be displayed.
  2. On the Power Supplies page, users can do one or more of the following:
     – To view the overall information of a cluster node, click the BMC host name of this cluster node.
     – To view the health status of the power supply of a cluster node, click the status of this cluster node.
     – To view more information of the power supplies, click **Customize Columns** on the Power Supplies page, select one or more target columns, and return to the Power Supplies page.

Managing fans

The **Fans** area displays the overall status of all fans of the cluster nodes.

Users can do one or more of the following:

- To view the fans in the “Critical”, “Warning”, “Normal”, or “Unknown” status, click the number in the Status column.
- To view the overall status of fans of all cluster nodes:
  1. Click **VIEW ALL**. The Fans page will be displayed.
  2. On the Fans page, users can do one or more of the following:
     - To view the overall information of a cluster node, click the BMC host name of this cluster node.
     - To view the health status of the fan of a cluster node, click the status of this cluster node.
     - To view more information of fans, click **Customize Columns** on the Fans page, select one or more target columns, and return to the Fans page.

Updating firmware/drivers for cluster nodes

For Windows Admin Center 1910, Hyper-Converged Cluster Manager and Failover Cluster Manager are combined into the Cluster Manager solution. This section describes how to perform a firmware/driver update job on cluster nodes in Cluster Manager, using **Best Recipes (Recommended)**, **Compliance Policies**, or **Latest Updates**. The **Updates** pane displays the best recipes, latest updates, cluster consistency, and update logs of firmware and drivers.

The following features are supported in the **Updates** pane:

- **Best Recipes (Recommended)**

  Best recipe is also a compliance policy, but includes firmware and driver updates. This method does not allow users to select part of components from the recipe for update. All components in the recipe will be updated for all servers in a cluster.

  This feature is supported only by specific server models. Refer to Features supported by specific server models.

  For details about the best recipe, see ThinkAgile MX Certified Node Best Recipe.
- **Compliance Policies**

  If a compliance policy is used, users can still determine components in the policy to be updated for a specific server or all servers in a cluster. It is only available when the server is managed by Lenovo XClarity Administrator.
- **Latest Updates**

  This method does not use any policy, and users need to select a target version for each component to be updated. The target version must be later than the current installed version.
- **Cluster Consistency**

  The **Cluster Consistency** pane supports to check the consistency of firmware versions across cluster nodes.
- **Update Logs**

  The **Update Logs** pane supports to delete, cancel, or retry the update jobs of current cluster nodes or servers.

Procedure

Step 1. Connect to Lenovo XClarity Integrator in Cluster Manager. Refer to “Connecting to Lenovo XClarity Integrator in Cluster Manager” on page 37.

Step 2. Do one of the following:

- Ensure that the target server is managed. In the **Menu** pane of the Lenovo Server page, click **Updates**.

  Notes:
  - Users can refer to "Managing cluster nodes with Lenovo XClarity Administrator" on page 37 and "Managing cluster nodes without Lenovo XClarity Administrator" on page 38.
  - The **Compliance Policies** feature is only supported when managing a server with Lenovo XClarity Administrator.
- In the left navigation pane of the server page, click **Lenovo XClarity Integrator — Compliance and Updates** or XC.

Step 3. In the **Updates** pane, select one of the following update methods:

- To assign a best recipe for firmware/driver updates:
  1. Click **Best Recipes (Recommended)**.
  2. Select the best recipe from the drop-down list, and do one of the following:
     - To view firmware/driver updates in the best recipe, click **Show Best Recipe Definition**.
     - To refresh the recipe, click **Refresh Best Recipe**.
     - To view the applicable firmware/driver updates, click › in front of a device.

       Notes:
       - If **Compliance** is **Compliant** for a component, the installed version is already the same as or even higher than the target update version in the policy. Therefore, components with **Compliance** being **Not Compliant** are recommended to be updated.
       - The table only shows the components defined in the best recipe.
  3. Click **Install Updates**.
- To assign a compliance policy for firmware updates:
  1. Click **Compliance Policies**.
  2. Select a policy from the drop-down list.

     Notes:
     - Users can click **Show Compliance Policy Definition** to view firmware updates in the policy.
     - Users can click › in front of the device to view firmware updates applicable to it in the policy. If **Compliance** is **Compliant** for a component, the installed version is already the same as or even higher than the target update version in the policy. Therefore, components with **Compliance** being **Not Compliant** are recommended to be updated.
  3. Click **Install Updates**.
- To select a target version for each component to be updated:
  1. Click **Latest Updates**.
  2. Do one of the following:
     - To view the latest firmware and driver updates, click **Reload local repository**.
     - To perform firmware and driver updates, select a target catalog or a target update package, and click **Install Updates**.
     - To manage local repository, click **Manage local repository**, and do one of the following:
       - To refresh catalog, select one or more target catalogs, and click **Refresh Catalog**.
       - To download the update packages, select one or more target catalogs or update packages, and click **Download**.
       - To delete the update packages, select one or more target machine types or update packages, and click **Delete**.
       - To filter out firmware updates or driver updates only, click **Firmware & Driver**, and select **Firmware** or **Driver**.
       - To filter out updates for Windows or Linux only, click **Windows & Linux**, and select **Windows** or **Linux**.
- To check the consistency of firmware versions across cluster nodes, click **Cluster Consistency**, and select a base for BMC and UEFI to check the firmware version consistency.
- To delete, cancel, or retry the update jobs of current cluster nodes or servers:

1. Click **Update Logs**.
2. Do one of the following:
   - To delete the update job, select one or more update jobs, and click **Delete**.
   - To cancel the update job, select one or more scheduled update jobs, and click **Cancel**.
   - To retry the update job, select an update job in **Failed**, **Stopped**, or **Cancelled** status, and click **Retry**.

Step 4. On the **Update Selection** tab, select or deselect components to be updated.

a. Select or deselect components to be updated in the **Select Items** pane.

Notes:

- Users can click < at the upper right corner of the **Select Items** pane to expand the **Preview** pane, or click × to remove a component.
- Operations on the **Select Items** and **Preview** panes are synchronized in real time.

b. (Optional) To update firmware/drivers on the selected components even if the installed version is already up to date or later than the target version for update, enable **Forced update**.

Notes:

- It's not allowed to apply firmware or drivers of earlier versions to device options, adapters, or disk drives.
- Forced update is available only when **Compliance Policy** is used.

c. Click **Next**.

Step 5. On the **Update Download** tab, download or import update packages as required, and then click **Next**.

Step 6. On the **Clustered Roles Migration** tab, click **Next**.

Attention: The cluster roles cannot be migrated when the cluster consists only one server node; otherwise, all running clustered roles, including clustered and non-clustered virtual machines, will be disrupted after the server node is restarted.

Note: Clustered roles migration is automatically enabled on all servers in the cluster.

Clustered Roles Migration performs the following tasks:

1. Puts one cluster node into maintenance mode, and moves the clustered roles off the node.
2. Install system updates.
3. Performs a restart.
4. Brings the node out of maintenance mode, and restores the clustered roles on the node.
5. Moves to the next cluster node.

Step 7. On the **OS Credential** tab, click **Credential Needed** to input the account, user name, and password of a Windows administrator account, and then click **Next**.

Notes:

- For the cluster node, the account should be the Active Directory domain account included in the local Administrators group.
- For the non-cluster server, the account should be the Active Directory domain account included in the local Administrators group or the built-in administrator account.
- OS credentials are required if one or more of the following operations are required:
  - Firmware/driver update in native OS management mode
  - Clustered roles migration

Step 8. On the **BitLocker** tab, set the BitLocker following the message, and click **Next**.

Step 9. On the **Options** tab, name and schedule the update job. Then, click **Next**.

Step 10. On the **Summary** tab, check the information about the update job, including the components to be updated, job name, schedule, and assigned policy if any.

Step 11. Click **Submit**.

The system then navigates to the Persistent Job page, and users can check the status of the update job.

Notes:

- If the Persistent Job page or the update wizard is closed, the system will then navigate back to the page before the update wizard is opened.
- To view the update history from any extension, refer to "Viewing the persistent jobs" on page 25.

Updating firmware/drivers when creating an Azure Stack HCI cluster

Lenovo XClarity Integrator is integrated into Microsoft's Azure Stack HCI solution to provide a snap-in for driver and firmware updates. When creating an Azure Stack HCI cluster in Windows Admin center, users can update firmware and drivers for the cluster nodes.

To update the firmware/drivers for Azure Stack HCI cluster nodes, do the following:

1. Log in to the Install hardware updates page provided by Lenovo. Refer to "Logging in to the Install hardware updates page" on page 48.
2. Select a management method if required. Refer to "Managing Azure Stack HCI cluster nodes with Lenovo XClarity Administrator" on page 48 or "Managing Azure Stack HCI cluster nodes without Lenovo XClarity Administrator" on page 50.
3. Perform firmware/driver updates on the cluster nodes. Refer to "Updating firmware/drivers for Azure Stack HCI cluster nodes" on page 50.

Logging in to the Install hardware updates page

To update firmware and drivers for the cluster nodes when creating an Azure Stack HCI cluster in Windows Admin center, log in to the Install hardware updates page first.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. On the All Connections page, click **Add**.
The Add or create resources page is displayed.

Step 3. In the **Sever clusters** pane, click **Create new**.

Step 4. Click **Azure Stack HCI**.
The Deploy an Azure Stack HCI cluster page is displayed.

Step 5. Complete operations on the **1.1 Check the prerequisites**, **1.2 Add servers**, **1.3 Join a domain**, **1.4 Install features**, and **1.5 Install updates** tabs as required.
The **1.6 Install hardware updates** tab is displayed.

Step 6. On the **1.6 Install hardware updates** tab, click **Get updates**.

Users can select a required management method or perform firmware/driver updates on the cluster nodes. Refer to "Managing Azure Stack HCI cluster nodes with Lenovo XClarity Administrator" on page 48 or "Managing Azure Stack HCI cluster nodes without Lenovo XClarity Administrator" on page 50.

Managing Azure Stack HCI cluster nodes with Lenovo XClarity Administrator

After entering into the Solution updates page in Windows Admin Center, a message indicating that one or more servers are currently not managed by a management server might be displayed. This section describes how to manage Azure Stack HCI cluster nodes with Lenovo XClarity Administrator when creating an Azure Stack HCI cluster.

If all Lenovo XClarity Administrators that manage these servers are connected, this page will not be displayed.

Procedure

Step 1. Log in to the Solution updates page. Refer to "Logging in to the Install hardware updates page" on page 48.

Step 2. Select **Lenovo XClarity Administrator**.

Step 3. Users can do one or more of the following:

- To connect to a current registered Lenovo XClarity Administrator:
  1. Select **Connect to a registered XClarity Administrator management server**.
  2. Select the IP address of a registered Lenovo XClarity Administrator from the drop-down list.
  3. Click **Connect**.

     The **Connect to Lenovo XClarity Administrator** pane will be displayed on the right.
  4. Input the user name and password. Ensure that the user provided meets the user privilege and role requirements and has enough permissions to perform desired operations.
  5. Click **Submit**.

  Note: If one or more Lenovo XClarity Administrators are connected, users can select one Lenovo XClarity Administrator to manage the server.
- To manage the nodes with a connected Lenovo XClarity Administrator:
  1. Select **Add nodes to a connected XClarity Administrator management server**.
  2. Select the IP address of a connected Lenovo XClarity Administrator from the drop-down list.
  3. Click **Add to**.

     The **Manage Lenovo Rack or Tower Servers** pane will be displayed on the right.
  4. Input a BMC IP address, click the add icon +, and input another BMC IP address. Repeat this step until all rack or tower servers are added. Then input the user name and password.

     Note: It is recommended to manage all the cluster nodes with the same Lenovo XClarity Administrator.
  5. Click **Manage**.
- To connect to a new Lenovo XClarity Administrator:
  1. Select **Connect to a new XClarity Administrator management server**.
  2. Click **Add**.

     The **Connect to Lenovo XClarity Administrator** pane will be displayed on the right.
  3. Input the IP address, user name, and password. Ensure that the user provided meets the user privilege and role requirements and has enough permissions to perform desired operations.
  4. Click **Submit**.
- To disconnect a connected Lenovo XClarity Administrator:
  1. Select **Disconnect a connected XClarity Administrator management server**.
  2. Select the IP address of a registered Lenovo XClarity Administrator from the drop-down list.
  3. Click **Disconnect**.

     A warning window will be displayed for users to confirm your operation.
  4. Click **Yes**.

Managing Azure Stack HCI cluster nodes without Lenovo XClarity Administrator

After entering into the Solution updates page in Windows Admin Center, a message indicating that one or more servers are currently not managed by a management server might be displayed. This section describes how to manage Azure Stack HCI cluster nodes without Lenovo XClarity Administrator, that is, through native OS management, when creating an Azure Stack HCI cluster.

Native OS management is a way to manage the hardware when no Lenovo XClarity Administrator is available. To use this function, log in to the XCC Web GUI and enable IPMI over KCS Access, Ethernet Over USB, and REST/CIM Over HTTPS.

Note: If all Lenovo XClarity Administrators that manage these servers are connected, this page will not be displayed.

Procedure

Step 1. Log in to the Solution updates page. Refer to "Logging in to the Install hardware updates page" on page 48.

Step 2. Select **Native OS Management**.

Step 3. Click **Take Me There**. If the **Native OS Management** window pops up, do the following:

a. Click **Lenovo WDAC policy**, and save the policy file in `c:\wdac`.

b. Open Windows PowerShell, run `Add-ASWDACSupplementalPolicy -Path c:\wdac\Contoso-policy.xml` to deploy the policy, and run `Get-ASLocalWDACPolicyInfo` to check the status of the new policy. For more information, see Step 4-5 in Create a WDAC supplemental policy.

c. Go back to the server page, click **Take Me There** again, and flash the webpage.

Step 4. After the initialization, the System Update page is displayed for users to perform firmware/driver updates for the cluster nodes.

Note: Native OS management is inapplicable to ThinkServer and ThinkSystem SR635/SR655 servers. For servers enabled with Storage Spaces Direct, native OS management is disabled by default. To enable native OS management for servers enabled with Storage Spaces Direct, refer to "Configuring native OS management" on page 12.

Updating firmware/drivers for Azure Stack HCI cluster nodes

When creating an Azure Stack HCI cluster in Windows Admin Center, users can update firmware and drivers for the cluster nodes using **Best Recipes (Recommended)**, **Compliance Policies**, or **Latest Updates**.

The following features are supported in the **Updates** pane:

- **Best Recipes (Recommended)**

  Best recipe is also a compliance policy, but includes firmware and driver updates. This method does not allow users to select part of components from the recipe for update. All components in the recipe will be updated for all servers in a cluster.

  This feature is supported only by specific server models. Refer to Features supported by specific server models.

  For details about the best recipe, see ThinkAgile MX Certified Node Best Recipe.

- **Compliance Policies**

  If a compliance policy is used, users can still determine components in the policy to be updated for a specific server or all servers in a cluster. It is only available when the server is managed by Lenovo XClarity Administrator.

- **Latest Updates**

This method does not use any policy, and users need to select a target version for each component to be updated. The target version must be later than the current installed version.

- **Update Logs**

  The **Update Logs** pane supports to delete, cancel, or retry the update jobs of current cluster nodes or servers.

Procedure

Step 1. Log in to the Solution updates page. Refer to "Logging in to the Install hardware updates page" on page 48.

Step 2. Ensure that all the cluster nodes are managed. Refer to "Managing Azure Stack HCI cluster nodes with Lenovo XClarity Administrator" on page 48 or "Managing Azure Stack HCI cluster nodes without Lenovo XClarity Administrator" on page 50.
The system update wizard is displayed.

Note: In the system update wizard, users can sync the inventory by clicking ⟳ in the upper right corner to sync the inventory. This function is the same as "Syncing the inventory of a server" on page 21.

Step 3. Select any of the following update methods:

- To assign a best recipe for firmware/driver updates:
  1. Click **Best Recipes (Recommended)**.
  2. Select the best recipe from the drop-down list, and do one of the following:
     - To view firmware/driver updates in the best recipe, click **Show Best Recipe Definition**.
     - To refresh the recipe, click **Refresh Best Recipe**.
     - To view the applicable firmware/driver updates, click > in front of a device.

       Notes:
       - If **Compliance** is **Compliant** for a component, the installed version is already the same as or even higher than the target update version in the policy. Therefore, components with **Compliance** being **Not Compliant** are recommended to be updated.
       - The table only shows the components defined in the best recipe.
  3. Click **Install Updates**.
- To assign a compliance policy for firmware updates:
  1. Click **Compliance Policies**.
  2. Select a policy from the drop-down list.

     Notes:
     - Users can click **Show Compliance Policy Definition** to view firmware updates in the policy.
     - Users can click > in front of the device to view firmware updates applicable to it in the policy. If **Compliance** is **Compliant** for a component, the installed version is already the same as or even higher than the target update version in the policy. Therefore, components with **Compliance** being **Not Compliant** are recommended to be updated.
  3. Click **Install Updates**.
- To select a target version for each component to be updated:
  1. Click **Latest Updates**.
  2. Do one of the following:
     - To view the latest firmware and driver updates, click **Reload local repository**.
     - To perform firmware and driver updates, select a target catalog or a target update package, and click **Install Updates**.
     - To manage local repository, click **Manage local repository**, and do one of the following:

- To refresh catalog, select one or more target catalogs, and click **Refresh Catalog**.
- To download the update packages, select one or more target catalogs or update packages, and click **Download**.
- To delete the update packages, select one or more target machine types or update packages, and click **Delete**.
- To filter out firmware updates or driver updates only, click **Firmware & Driver**, and select **Firmware** or **Driver**.
- To filter out updates for Windows or Linux only, click **Windows & Linux**, and select **Windows** or **Linux**.

Step 4. On the **Update Selection** tab, select or deselect components to be updated.

a. Select or deselect components to be updated in the **Select Items** pane.

Notes:

- Users can click < at the upper right corner of the **Select Items** pane to expand the **Preview** pane, or click × to remove a component.
- Operations on the **Select Items** and **Preview** panes are synchronized in real time.

b. (Optional) To update firmware/drivers on the selected components even if the installed version is already up to date or later than the target version for update, enable **Forced update**.

Notes:

- It's not allowed to apply firmware or drivers of earlier versions to device options, adapters, or disk drives.
- Forced update is available only when **Compliance Policy** is used.

c. Click **Next**.

Step 5. On the **Update Download** tab, download or import update packages as required, and then click **Next**.

Step 6. On the **Clustered Roles Migration** tab, click **Next**.

Attention: The cluster roles cannot be migrated when the cluster consists only one server node; otherwise, all running clustered roles, including clustered and non-clustered virtual machines, will be disrupted after the server node is restarted.

Note: Clustered roles migration is automatically enabled on all servers in the cluster.

Clustered Roles Migration performs the following tasks:

1. Puts one cluster node into maintenance mode, and moves the clustered roles off the node.
2. Install system updates.
3. Performs a restart.
4. Brings the node out of maintenance mode, and restores the clustered roles on the node.
5. Moves to the next cluster node.

Step 7. On the **OS Credential** tab, click **Credential Needed** to input the account, user name, and password of a Windows administrator account, and then click **Next**.

Notes:

- For the cluster node, the account should be the Active Directory domain account included in the local Administrators group.
- For the non-cluster server, the account should be the Active Directory domain account included in the local Administrators group or the built-in administrator account.
- OS credentials are required if one or more of the following operations are required:
  - Firmware/driver update in native OS management mode
  - Clustered roles migration

Step 8. On the **BitLocker** tab, set the BitLocker following the message, and click **Next**.

Step 9. On the **Summary** tab, check the information about the update job, including the components to be updated, job name, schedule, and assigned policy if any.

Step 10. Click **Submit**.

Users may continue to complete creating the Azure Stack HCI cluster as prompted on Windows Admin Center.

Updating firmware/drivers with the Cluster-Aware Updating tool in Cluster Manager

Lenovo XClarity Integrator is integrated into Microsoft's Cluster-Aware Updating (CAU) tool to provide a snap-in for driver and firmware updates. Using this snap-in, users can update firmware and drivers for cluster nodes when using the CAU tool in Cluster Manager. This method of updating firmware/drives with CAU is available only for Azure Stack HCI on SE350, SR630 V2, SR650, and SR650 V2 servers. For other servers, the Lenovo XClarity Integrator snap-in is not available in the CAU tool.

Note: CAU is a feature that automates the software updating process on clustered servers while maintaining availability.

To update the firmware/drivers with the Cluster-Aware Updating tool in Cluster Manager, do the following:

1. Log in to the Hardware updates page in the CAU tool. Refer to "Logging in to the Hardware updates page" on page 53.
2. Select a management method if required. Refer to "Managing cluster nodes with Lenovo XClarity Administrator" on page 37 or "Managing cluster nodes without Lenovo XClarity Administrator" on page 38.

   Note: By default, native OS management is disabled for ThinkAgile MX servers with Microsoft Storage Spaces Direct enabled. To enable this function, click the link provided. Refer to "Configuring native OS management" on page 12.
3. Perform firmware/driver updates on the cluster nodes. Refer to "Updating firmware/drivers for cluster nodes with the Cluster-Aware Updating tool" on page 54.

Logging in to the Hardware updates page

To update the firmware/drivers with the CAU tool in Cluster Manager, log in to the Hardware updates page first.

Procedure

Step 1. Log in to Windows Admin Center.

Step 2. On the All Connections page, click the name of a connected cluster to enter its cluster page in Cluster Manager.

Note: If no cluster is available, click **Add**, locate the **Sever clusters** pane, and then click **Add**. Then enter the cluster name and specify the user credentials to add the cluster.

Step 3. In the left navigation pane of the cluster page, click **Updates**.

Step 4. In the Updates page, select one or more target quality updates and click **Install**.

Note: If there is no available quality updates, hardware updates cannot be installed in CAU tool.

Step 5. Select **Hardware Updates** and click **Get Updates**.

Notes:

- If all cluster nodes are detected to be managed by connected Lenovo XClarity Administrators, the Lenovo XClarity Integrator dashboard will be displayed.

- If any cluster nodes are detected to be not managed by any connected Lenovo XClarity Administrator, Lenovo XClarity Integrator will prompt users to choose a management approach, either through Lenovo XClarity Administrator (see "Managing cluster nodes with Lenovo XClarity Administrator" on page 37) or native OS management (see "Managing cluster nodes without Lenovo XClarity Administrator" on page 38).
- It may take some time to check updates and load the Updates page.

Updating firmware/drivers for cluster nodes with the Cluster-Aware Updating tool

When using the CAU tool in Cluster Manager, users can update firmware and drivers for the cluster nodes using **Best Recipes (Recommended)**, **Compliance Policies**, or **Latest Updates**.

The following features are supported in the **Updates** pane:

- **Best Recipes (Recommended)**

  Best recipe is also a compliance policy, but includes firmware and driver updates. This method does not allow users to select part of components from the recipe for update. All components in the recipe will be updated for all servers in a cluster.

  This feature is supported only by specific server models. Refer to Features supported by specific server models.

  For details about the best recipe, see ThinkAgile MX Certified Node Best Recipe.
- **Compliance Policies**

  If a compliance policy is used, users can still determine components in the policy to be updated for a specific server or all servers in a cluster. It is only available when the server is managed by Lenovo XClarity Administrator.
- **Latest Updates**

  This method does not use any policy, and users need to select a target version for each component to be updated. The target version must be later than the current installed version.

Procedure

Step 1. Log in to the Hardware updates page. Refer to "Logging in to the Hardware updates page" on page 53.

Step 2. Ensure that all the cluster nodes are managed. Refer to "Managing cluster nodes with Lenovo XClarity Administrator" on page 37 or "Managing cluster nodes without Lenovo XClarity Administrator" on page 38.
The system update wizard is displayed.

Note: In the system update wizard, users can sync the inventory by clicking ⟳ in the upper right corner to sync the inventory. This function is the same as "Syncing the inventory of a server" on page 21.

Step 3. Select any of the following update methods:

- **Best Recipes (Recommended)**

  Best recipe is also a compliance policy, but includes firmware and driver updates. This method does not allow users to select part of components from the recipe for update. All components in the recipe will be updated for all servers in a cluster.

  This feature is supported only by specific server models. Refer to Features supported by specific server models.

  For details about the best recipe, see ThinkAgile MX Certified Node Best Recipe.

- **Compliance Policies**

  If a compliance policy is used, users can still determine components in the policy to be updated for a specific server or all servers in a cluster. It is only available when the server is managed by Lenovo XClarity Administrator.
- **Latest Updates**

  This method does not use any policy, and users need to select a target version for each component to be updated. The target version must be later than the current installed version.

Step 4. On the **Update Selection** tab, select or deselect components to be updated.

a. Select or deselect components to be updated in the **Select Items** pane.

   Notes:

   - Users can click < at the upper right corner of the **Select Items** pane to expand the **Preview** pane, or click × to remove a component.
   - Operations on the **Select Items** and **Preview** panes are synchronized in real time.

b. (Optional) To update firmware/drivers on the selected components even if the installed version is already up to date or later than the target version for update, enable **Forced update**.

   Notes:
   - It's not allowed to apply firmware or drivers of earlier versions to device options, adapters, or disk drives.
   - Forced update is available only when **Compliance Policy** is used.

c. Click **Next**.

Step 5. On the **Update Download** tab, download or import update packages as required, and then click **Next**.

Step 6. On the **Update Storage** tab, select any of the following methods to store the updates.
- **Copy to cluster nodes**: Copy the selected updates and prerequisites to all the cluster nodes.
- **Specify a predefined share folder**: Transfer the selected updates and prerequisites to the specified share folder. A share server in the same domain as the cluster nodes is recommended.

  Note: Ensure that the CAU clustered roles and Windows account used have adequate permissions.
- **Create a share folder automatically**: Create a share folder automatically on the system running the Windows Admin Center service.

Step 7. On the **OS Credential** tab, click **Credential Needed** to input the account, user name, and password of a Windows administrator account, and then click **Next**.

Notes:
- The account should be the Active Directory domain account included in the local Administrators group.
- OS credentials are required if one or more of the following operations are required:
  - Firmware/driver update in native OS management mode
  - Clustered roles migration

Step 8. On the **BitLocker** tab, set the BitLocker following the message, and click **Next**.

Step 9. On the **Summary** tab, check the information about the update job, including the components to be updated, job name, schedule, and assigned policy if any.

Step 10. Click **Submit**.

Note: To modify the selected update options, click **Back**. After the modification, click **Resubmit** to resubmit the updates.

Step 11. Click **Next: Install**.

An overview of selected updates is displayed, with the **Type** being **Solution updates**. Users may continue to complete installing the updates as prompted on Windows Admin Center.

Managing the system updates repository

This section describes how to manage the system updates repository for the target servers.

To download, back up, or restore system updates, refer to Chapter 8 “Managing the system updates repository” on page 61.

Managing processor cores

On the **Processor Cores** page, users can view the overall information of processor cores or set the enabled processor cores for one or more servers under the target cluster.

Note: This feature is only supported in native OS management mode.

Procedure

Step 1. Connect to Lenovo XClarity Integrator in Cluster Manager. Refer to “Connecting to Lenovo XClarity Integrator in Cluster Manager” on page 37.

Step 2. In the left navigation pane of the server page, click **Processor Cores**.

Step 3. Do one of the following:

- View the number of cores, processors and servers, the number and percentage of enabled and standby cores, and the list of processor cores enabled per server.
- In the “Processor cores enabled per server” area, do one of the following:
  - To enable maximum cores for all servers in the list, click **Enable All**.
  - To enable the same number of cores for all servers in the list, click **Select Enabled Cores**, select the number from the drop-down list.
  - To change the enabled processor cores for the target server, find the target server, click the edit icon ✎ in the **Enabled Cores per Processor** column, input the number of cores, or select the number of cores from the drop-down list.

    Note: To cancel the changes, click the cancel icon ✕.

Step 4. Do one of the following:

- To cancel the changes, click **Reset**.
- To apply changes, click **Apply Changes** to enter into the Set Processor Cores page.

  Notes:
  - This feature is only applicable to the ThinkAgile MX appliances and certified nodes installed with Azure Satck HCI or Windows Server cluster.
  - If the feature is not supported, the version of XCC and UEFI firmware might be outdated and the number of cores might be incorrect. Users should install the latest XCC and UEFI firmware to view accurate processor information or to set the number of enabled processor cores. For more information, refer to “Updating firmware/drivers for cluster nodes” on page 45.

a. On the **Clustered Roles Migration** tab, click **Next**.

Attention: The cluster roles cannot be migrated when the cluster consists only one server node; otherwise, all running clustered roles, including clustered and non-clustered virtual machines, will be disrupted after the server node is restarted.

Note: Clustered roles migration is automatically enabled on all servers in the cluster.

Clustered Roles Migration performs the following tasks:

1. Puts one cluster node into maintenance mode, and moves the clustered roles off the node.
2. Set enabled processor cores.
3. Performs a restart.
4. Brings the node out of maintenance mode, and restores the clustered roles on the node.
5. Moves to the next cluster node.

b. On the **OS Credential** tab, click **Credential Needed** to input the account, user name, and password of a Windows administrator account, and then click **Next**.

Notes:

- The account should be the Active Directory domain account included in the local Administrators group.
- OS credentials are required if one or more of the following operations are required:
  - Clustered roles migration
  - Set enabled processors cores

c. On the **Options** tab, name and schedule the update job. Then, click **Next**.

d. On the **Summary** tab, check the information about the update job, including the components to be updated, job name, schedule, and assigned policy if any.

e. Click **Submit**.

The system then navigates to the Persistent Job page, and users can check the status of the update job.

Notes:

- If the Persistent Job page or the update wizard is closed, the system will then navigate back to the page before the update wizard is opened.
- To view the update history from any extension, refer to "Viewing the persistent jobs" on page 25.

Chapter 7. Updating firmware/drivers for Lenovo servers

This section illustrates all methods to update firmware/drivers for Lenovo servers through different interfaces, tools, and extensions. Users can select one or more of the following methods based on the actual scenarios.

Managing servers and chassis through Lenovo XClarity Integrator

If the target server is installed without any OS, it is recommended to manage the server through Lenovo XClarity Integrator. Do one or more of the following:

- To update firmware for a server, refer to "Updating firmware for a server" on page 21.
- To update firmware for multiple servers, refer to "Updating firmware for multiple servers" on page 23.
- To manage the system updates repository through Lenovo XClarity Integrator, refer to Chapter 8 "Managing the system updates repository" on page 61.

Managing servers through Server Manager

If the target server is installed with OS, and is not a cluster node, it is recommended to manage the server through Server Manager. Do one or more of the following:

- To update firmware/drivers for a server through Server Manager, refer to "Updating firmware/drivers for a server" on page 33.
- To manage the system updates repository through Server Manager, refer to "Managing the system updates repository" on page 36.

Managing servers through Cluster Manager

If the target server is installed with OS, and is a cluster node, it is recommended to manage the server through Cluster Manager. Do one or more of the following based on your needs:

- To update firmware/ drivers for cluster nodes through Cluster Manager, refer to "Updating firmware/ drivers for cluster nodes" on page 45.
- To update firmware/drivers when creating an Azure Stack HCI cluster, refer to "Updating firmware/drivers when creating an Azure Stack HCI cluster" on page 48.
- To update firmware/drivers with the Cluster-Aware Updating tool in Cluster Manager, refer to "Updating firmware/drivers with the Cluster-Aware Updating tool in Cluster Manager" on page 53.
- To manage the system updates repository through Cluster Manager, refer to "Managing the system updates repository" on page 56.

Chapter 8. Managing the system updates repository

This chapter describes how to manage the system updates repository for the target servers.

In this chapter, do one or more of the following:

- "Downloading system updates" on page 61
- "Backing up system updates" on page 62
- "Restoring system updates" on page 62
- "Deleting system updates" on page 63
- "Filtering system updates" on page 63

Opening the system updates repository

Before managing the system updates repository for the target servers, users should open the repository first. This section describes how to open the system updates repository.

Procedure

Step 1. In any of Lenovo extensions, click the repository icon in the top right corner. Alternatively, click the more icon ··· in the top right corner and then click **System Updates Repository** from the menu.
The System Updates Repository page is displayed.

The System Updates Repository page consists of the following information:

- **Current repository path**: describes the directory where the firmware/driver update packages are stored. To change the path, choose **...(More icon) → Set Path** from the action bar, and designate a path that meets the conditions described.
- **Repository Usage**: describes the total space and occupied space of the update repository.
- **Product Catalog**: lists all the machine types of servers currently managed and their available firmware and driver updates. To view specific firmware or driver updates, users can do one or more of the following:
  - **Firmware & Driver**: filters out firmware updates or driver updates only.
  - **Any OS**: filters out updates for any OS, Windows, or Linux.
  - **Any time**: filters out updates released at any time, within 6 months, within 1 year, within 2 years, or within any custom period set by users.
  - **All Type**: filters out individual updates, best recipes, and UXSP updates.
  - **Select Machine Types**: enables users to select any required machine type to check its firmware and driver updates available.
- Search box: enables users to search for a specify machine type and its available firmware and driver updates by using a keyword.

Downloading system updates

This section describes how to download specific firmware and driver updates.

Procedure

Step 1. Open the System Updates Repository page. Refer to "Opening the system updates repository" on page 61.

Step 2. Select the target machine type, and click **Refresh Catalog** above the product catalog to obtain the latest updates for the machine type.

Step 3. Click > in front of any desired machine type and desired component to select the target firmware and driver updates.

Note: For more specific selection, use filters **Firmware & Driver**, **Windows & Linux**, and **All time** above the product catalog to filter out the target updates.

Step 4. Click **Download**.

Backing up system updates

This section describes how to back up specific firmware and driver updates or all updates for all machine types.

Procedure

Step 1. Open the System Updates Repository page. Refer to "Opening the system updates repository" on page 61.

Step 2. On the System Updates Repository page, do either of the following:

- To back up all firmware and driver updates available:
  1. Choose **...(More icon) → Backup → Backup All**.

     The Backup Updates page is displayed.
  2. Specify the path for backup, user name, and password.
  3. Click **Backup**.
- To back up selected firmware and driver updates:
  1. Click > in front of the target machine type and component to select the target firmware and driver updates.

     Note: For more specific selection, use filters **Firmware & Driver**, **Windows & Linux**, and **All time** above the product catalog to filter out the target updates.
  2. Choose **...(More icon) → Backup → Backup Selection**.

     The Backup Updates page is displayed.
  3. Specify the path for backup, user name, and password.
  4. Click **Backup**.

Restoring system updates

This section describes how to restore specific firmware and driver updates or all updates for all machine types.

Procedure

Step 1. Open the System Updates Repository page. Refer to "Opening the system updates repository" on page 61.

Step 2. On the System Updates Repository page, do either of the following:

- To restore all firmware and driver updates available:
  1. Choose **...(More icon) → Restore → Restore All**.

     The Restore Updates page is displayed.
  2. Specify the path for restoration, user name, and password.
  3. Click **Restore**.
- To restore selected firmware and driver updates:
  1. Click > in front of the target machine type and component to select the target firmware and driver updates.

Note: For more specific selection, use filters **Firmware & Driver**, **Windows&Linux**, and **All time** above the product catalog to filter out the target updates.

2. Choose **...(More icon) → Restore → Restore Selection**.

   The Restore Updates page is displayed.
3. Specify the path for restoration, user name, and password.
4. Click **Restore**.

Deleting system updates

This section describes how to delete specific firmware and driver updates.

Procedure

Step 1. Open the System Updates Repository page. Refer to "Opening the system updates repository" on page 61.

Step 2. Do one or more of the following:

- To delete all firmware/driver updates of the machine type, select one or more target machine types, and click **Delete**.
- To delete one or more firmware/driver updates of the machine type, click > in front of the target machine type, select one or more target firmware/driver updates, and click **Delete**.
- To delete the update package which is prerequisite of other update packages, enable **Force Delete** and click **Delete**.

Filtering system updates

This section describes how to filter specific firmware and driver updates.

Procedure

Step 1. Open the System Updates Repository page. Refer to "Opening the system updates repository" on page 61.

Step 2. Do one or more of the following:

- To filter out firmware updates or driver updates only, click the **Firmware & Driver** drop-down list, and select **Firmware** or **Driver**.
- To filter out updates for Windows or Linux only, click the **Windows & Linux** drop-down list, and select **Windows** or **Linux**.

Chapter 9. Reporting problems to Lenovo

This chapter describes how to report problem to Lenovo, manage the call home contact and service tickets.

In this chapter, do one or more of the following:

- “Managing call home contact” on page 65
- “Reporting problem” on page 65
- “Managing service tickets” on page 67
- “Setting automatic problem reporting” on page 68

Managing call home contact

This section describes how to add, delete, and edit the contact, set the primary contact, and check the detail information of a contact.

Procedure

Step 1. In any of Lenovo extensions, do one of the following to enter into the Call Home Contact page:

- Click the more icon ··· on the top right corner, and then click **Call Home → Contacts** from the menu.
- Click the report problem icon ☎ on the top right corner, and then click **Contacts** from the menu.

Step 2. On the Call Home Contact page, do one or more of the following:

- To add a contact:
  1. Click **Add**.
  2. On the Add Call Home Contact page, input the effective information, and click **Apply**.
- To delete one or more contacts, select one or more target contacts and click **Delete**.
- To edit the contact information:
  1. Select the target contact and click **Edit**.
  2. On the Edit Call Home Contact page, edit the information, and click **Apply**.
- To set the primary contact, select the target contact, and click **Set Primary**.
- To check the details of a contact, click the target contact from the list.

  Note: To hide the Details area, click the collapse icon ⌄ on the top-right corner of the Details area.
- To sort the list by alphabet or number, click the target column name.

Reporting problem

This section describes how to report problem to Lenovo.

Notes:

- This feature is only supported when connecting servers or clusters through native OS management mode or LXCA.
- LXCI automatically collects the required logs and data, and uploads them to Lenovo, including Server Service Data, Cluster Diagnostic Data, Windows Admin Center Log, and Lenovo XClarity Integrator Log. LXCI will automatically retry if any log or data collection is failed.

Procedure

Step 1. Do one of the following to enter into the Report Problem page:

- In Cluster Manager or Server Manager extensions:

  - Click the report problem icon ☎ on the top right corner.
  - Click the more icon ··· on the top right corner, and then click **Call Home → Report Problem** from the menu.
- In any of Lenovo extensions, click **Report Problem** in the alert bar.

  Note: The alert will only be displayed after the automatic problem reporting function is enabled. For more information, refer to "Setting automatic problem reporting" on page 68.

Step 2. On the **Call Home User Agreement** window, click **Accept**.

Note: Users can also click **Decline** to skip to the Service Tickets page.

Step 3. On the Report Problem page, input the required information.

Notes:

- For the servers except for the ThinkAgile MX series, the customer number (XClarity Pro license key) is required when **Lenovo XClarity Integrator features** is selected. Users can select the existing customer number from the drop-down list or add a new one.
- In the **Functional Area** field, if the option excepting for **Cluster — Storage**, **Cluster — Performance**, or **Cluster — Network** is selected, the cluster diagnostic data will not be uploaded. Users can manually upload the data after receiving the notification from Lenovo Support. For more information, refer to "Managing service tickets" on page 67.
- The text in the **Title** field must be no more than 128 characters.
- The text in both the **Description** and **Reproduction Steps** fields must be no more than 4096 characters.
- To change the default primary contact, select another target primary contact from the drop-down list.
- The primary and secondary contacts manually added in this page will also be added to the contact list on the Call Home Contact page, but will not be automatically set as the primary contact in that page.

Step 4. In the Upload File field, do one of the following to upload the file:

Note: The size of file to be uploaded must be less than or equal to 10MB.

- Click **Select a file**, select and upload the target file.
- Drag the target file to the Upload File field.

Step 5. In OS Credential field, authorize Lenovo to retrieve the data and logs:

a. Click **Credential Needed**.

b. On the Specify your credentials page, do one of the following:

- To use a new credential, select **Use manually entered credentials** and input account and password.

  Notes:

  - For the cluster node, the account should be the Active Directory domain account included in the local Administrators group.
  - For the non-cluster server, the account should be the Active Directory domain account included in the local Administrators group or the built-in administrator account.
  - This credential will not be saved in the **Credential** drop-down list.

- To use an existing credential, select **Use stored credentials** and select the target credential from the drop-down list.

  Note: To add, edit, or delete a credential, click **Open credential manager**. For more information, refer to "Managing credentials" on page 12.

c. Click **Continue** to go back to the Report Problem page.

Step 6. On the Report Problem page, click **Submit**.

Managing service tickets

This section describes how to delete, export, refresh, and search tickets, attach file and notes, customize columns of the ticket list, and check details of tickets.

Procedure

Step 1. In any of Lenovo extensions, do one of the following to enter into the Service Tickets page:

- Click the report problem icon ☎ on the top right corner, and click **Service Tickets** from the menu.
- Click the more icon ··· on the top right corner, and then click **Call Home → Service Tickets** from the menu.

Step 2. On the Service Tickets page, do one of the following:

- To delete tickets:
  1. Select one or more target tickets, click **Delete**.

     A pop-up dialog will be displayed for users to confirm whether to delete the ticket.
  2. Click **OK**.

     Note: Only the tickets in the status of **Resolved**, **Cancelled**, **Unknown**, **Error**, **Duplicate**, or **Rejected** can be deleted.
- To attach the file for the target ticket:
  1. Select the target ticket, and click **Attach File**.
  2. On the Attach File page, upload the file, and click **Apply**.
- To attach the note for the target ticket:
  1. Select the target ticket, and click **Attach Notes**.
  2. On the Attach Notes page, fill in the title and description, and click **Apply**.

     The information in the Notes area of the target ticket will be updated.
- To manually upload the data or log failed to be uploaded in the past 30 days, select the target ticket, and click **Retry**.
- To export the ticket list, click **Export**.

  The ticket list will be exported as a CSV file.
- To customize the columns of the ticket list:
  1. Click the more icon ···, and select **Customize Columns**.
  2. On the Customize Ticket Columns page, select the columns to be displayed on the Service Tickets page, and click **Apply**.

     The target columns will be displayed in the ticket list.
- To refresh the ticket list and details, click the refresh icon ↻ on the top right corner.
- To search the specific ticket, input the ticket number, status, or title of the target ticket in search field. The target tickets will be displayed.
- To check the details of a ticket, click the target ticket from the list. The Details area will be displayed.

  Notes:
  - To download the data or log to local, click the ZIP/EVTX file of the target data or log.
  - If the option excepting for **Cluster — Storage**, **Cluster — Performance**, or **Cluster — Network** is selected on the Report Problem page, the cluster diagnostic data will not be uploaded. Users can click **Upload** to manually upload the data after receiving the notification from Lenovo Support.

  - To hide the Details area, click the collapse icon ⌄ on the top-right corner of the Details area.
- To sort the ticket list by alphabet or number, click the **Ticket Number**, **Status**, or **Title** column.

Setting automatic problem reporting

This section describes how to enable or disable automatic problem reporting function, add, edit, or remove endpoints, and manage the rules for reporting problem automatically.

Note: After the functions in this page are enabled, the alerts associated with the enabled rules will be displayed once the problems are detected in the target endpoints, and the corresponding tickets will be automatically generated. Users can click **Report Problem** in the alert bar to report problem. For more information, refer to "Reporting problem" on page 65.

Procedure

Step 1. In any of Lenovo extensions, do one of the following to go to the Settings page:

- Click the report problem icon ☎ on the top right corner, and click **Settings** from the menu.
- Click the more icon ⋯ on the top right corner, and then click **Call Home** from the menu.

Step 2. On the Settings page, do one or more of the following:

- To enable or disable the automatic reporting function, click ● or ○ in the **Automatically report to Lenovo Support** field to toggle between **Enable** or **Disable**.
- To add a host or cluster to be monitored:
  1. In the **Managed Endpoints** area, click **Add**. The Add Host or Cluster page is displayed.
  2. Input the host name.
  3. Do one of the following:
     - To use a new credential, select **Use manually entered credentials** and input account and password.

       Notes:
       - For the cluster node, the account should be the Active Directory domain account included in the local Administrators group.
       - For the non-cluster server, the account should be the Active Directory domain account included in the local Administrators group or the built-in administrator account.
       - This credential will not be saved in the **Credential** drop-down list.
     - To use an existing credential, select **Use stored credentials** and select the target credential from the drop-down list.

       Note: To add, edit, or delete a credential, click **Open credential manager**. For more information, refer to "Managing credentials" on page 12.
  4. Click **Apply**.

     Note: When a host belonging to a cluster is added, the corresponding cluster will also be added.
- To edit a host to be monitored:
  1. In the **Managed Endpoints** area, select the target host, and click **Edit**. The Edit Cluster page is displayed.
  2. On the Edit Cluster page, do one of the following:
     - To use a new credential, select **Use manually entered credentials** and input account and password.

       Notes:
       - For the cluster node, the account should be the Active Directory domain account included in the local Administrators group.

        - For the non-cluster server, the account should be the Active Directory domain account included in the local Administrators group or the built-in administrator account.
        - This credential will not be saved in the **Credential** drop-down list.
      - To use an existing credential, select **Use stored credentials** and select the target credential from the drop-down list.

        Note: To add, edit, or delete a credential, click **Open credential manager**. For more information, refer to "Managing credentials" on page 12.
   3. Click **Apply**.
- To remove the host or cluster to be monitored:
   1. In the **Managed Endpoints** area, select one or more target hosts or clusters.
   2. Click **Remove**. The **Remove Endpoints** window is displayed.
   3. In the **Remove Endpoints** window, click **OK**.
- To test the accessibility between the host or cluster and the credential:
   1. In the **Managed Endpoints** area, select one or more target hosts or clusters.
   2. Click **Test Accessibility**.
- To enable or disable one or more rules for automatic problem reporting, click ● or ○ in the **Rules** area to toggle between **Enable** or **Disable** for the target rules.

Step 3. Click **Close** to save the settings.

Appendix A. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

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

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

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, Flex System, System x, and NeXtScale System are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Storage Spaces Direct, Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

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

Important notes

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

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