Lenovo Hardware Management Pack for Microsoft System Center Operations Manager Installation and User Guide

Version 7.4.0

Note

Before using this information and the product it supports, read the information in Appendix D “Notices” on page 55.

Thirteenth Edition (May 2018)

Contents

About this publication iii
Conventions and terminology iii
Web resources iii

Chapter 1. Overview 1
Key features 1
Advantages 5
Hardware and software requirements of the management server 6
Hardware requirements 6
Software requirements 6
The Lenovo Hardware folder in Operations Manager 7
Lenovo system groups in Operations Manager 8

Chapter 2. Installing Lenovo Hardware Management Pack 9
Installing Lenovo Hardware Management Pack . . . 9
Migrating the data from the PostgreSQL database to the SQL server database 10
Viewing the database information 10
Uninstalling Lenovo Hardware Management Pack 10
Upgrading Lenovo Hardware Management Pack . . 11

Chapter 3. Managing servers through XClarity Integrator Service . . 13
Configuring XClarity Integrator Service 13
Logging in to XClarity Integrator Service . . . 13
Changing password of XClarity Integrator Service 14
Restarting XClarity Integrator Service 14
Discovering the BMC node 14
BMC node discovery and authentication . . . 14
BMC node auto-discovery and authentication. 15
Monitoring the system health 16
Obtaining the latest information for the BMC-based servers 16
Setting the power capping 17
Removing a BMC node 17

Chapter 4. Managing servers through XClarity Administrator 19
Configuring XClarity Administrator 19
Monitoring the system health 20
Obtaining the latest information for the ThinkServer servers 20
Removing a ThinkServer server. 21

Chapter 5. Managing chassis through SNMP 23
Configuring the SNMP agent 23
Configuring SNMPv1 Agent on the BladeCenter chassis 23
Configuring SNMP on the Flex System chassis 24
Discovering a chassis 25
Monitoring the chassis health 26
Monitoring the BladeCenter chassis health . . 26
Monitoring the Flex System chassis health . . 27
Obtaining the latest information for the chassis . . 28
Launching the AMM/CMM Web console 28
Starting or shutting down a blade server or a compute node 28
Removing a discovered chassis 29

Chapter 6. Managing servers through IBM Platform Agent 31
Discovering a Lenovo server 31
Monitoring the server health 32
Viewing the power data of the client System x servers 32
Setting the power capping 33
Setting the power threshold 33
Obtaining the latest information for the Lenovo servers 33

Chapter 7. Working with security certificates 35
Setting the BMC communication protocol 35
Generating and uploading the certificates. 35
Regenerating the certificates. 36
Regenerating the server certificate 36
Regenerating the root certificate 36
Downloading the certificates. 37
Downloading the server certificate. 37
Downloading the root certificate 37

Chapter 8. Log data 39
Logs for XClarity Integrator Service 39
Setting the log level 39
Collecting the log files 39
Logs for Lenovo Hardware Management Pack. . . 39
Setting the log level 39
Viewing the log in Windows Event Viewer . . . 40

Chapter 9. Troubleshooting 41

Troubleshooting by symptoms 41
Using Health Explorer to view and resolve problems 41
Using Lenovo XClarity Forum and Lenovo XClarity Ideation 42

Appendix A. Accessibility features 43

Appendix B. Best practices 45
Determining the cause of an error 45
Rediscovering all BladeCenters 47
Rediscovering a renamed server 47

Appendix C. System firewall settings. 49

Appendix D. Notices. 55
Trademarks 56
Important notes 56

About this publication

This publication provides the instructions for installing Lenovo® Hardware Management Pack for Microsoft® System Center Operations Manager (hereinafter referred to as Lenovo Hardware Management Pack) into Microsoft System Center Operations Manager (hereinafter referred to as Operations Manager) and using its integrated features to manage the systems in your environment.

Conventions and terminology

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

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

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

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

Term, Acronym, or Abbreviation	Definition
BMC	Baseboard Management Controller, which is a service processor that consolidates service processor functions and a video controller in a single chip.
CMM	Chassis Management Module, which manages the Flex System chassis.
AMM	Advanced Management Module, which manages the BladeCenter® chassis.
SNMP	Simple Network Management Protocol.
(Lenovo) XClarity® Integrator (LXCI)	A tool suite that enables IT administrators to integrate the management features of the System x with Microsoft System Center.
(Lenovo) XClarity Integrator Service	The backend component of Lenovo XClarity Integrator, which provides the functionality for Lenovo XClarity Integrator to access and manage Lenovo servers.
(Lenovo) XClarity Administrator (LXCA)	A centralized, resource-management solution that simplifies infrastructure management, speeds responses, and enhances the availability of Lenovo server systems and solutions.
Operations Manager	The Microsoft System Center Operations Manager.
Managed server or managed node	A physical machine managed by Operations Manager.

Web resources

The following Web sites provide the resources for understanding, using, and troubleshooting the BladeCenter chassis, the Flex System chassis, the ThinkServer® servers, the ThinkSystem® servers, the System x servers, and the system-management tools.

Lenovo Web site for Microsoft Systems Management Solutions for Lenovo servers

This Web site locates the latest downloads for the XClarity Integrator offerings for Microsoft System Center Management Solutions:

- Lenovo XClarity Integrator for Microsoft System 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 system management capability:

- System Management with Lenovo XClarity Solution Web site

Lenovo XClarity Forum and Ideation

The following Web sites provide the forum and ideation of all Lenovo XClarity products:

- Lenovo XClarity Forum Web site
- Lenovo XClarity Ideation Web site

Lenovo technical support portal

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

- Lenovo Support Portal Web site

Lenovo ServerProven

This Web site obtains the information about hardware compatibility with Lenovo ThinkSystem servers, System x servers, BladeCenter servers, and Flex System servers:

- Lenovo ServerProven Compatibility Web site

Microsoft System Center Operations Manager Web site

This Web site provides an overview of the Microsoft System Center Operations Manager:

- Microsoft System Center Operations Manager Web site

Chapter 1. Overview

Lenovo Hardware Management Pack manages the health state of the ThinkSystem servers, the System x servers, the ThinkServer servers, the BladeCenter chassis, and the Flex System chassis by using the enhanced features of Operations Manager. Lenovo Hardware Management Pack provides a view of your IT infrastructures and minimizes the down time caused by the hardware problems.

Key features

Lenovo Hardware Management Pack has the following key features:

- Managing the System x servers, the ThinkSystem servers, the BladeCenter servers, and the Flex System servers through XClarity Integrator Service (out-of-band mode).
- Managing the ThinkServer servers through XClarity Administrator (out-of-band mode).
- Managing the BladeCenter chassis and the Flex System chassis through SNMP.
- Managing the System x servers, the BladeCenter servers, and the Flex System servers installed with the Windows® operating systems through IBM® Platform Agent (in-band mode).

  Note: IBM Platform Agent does not support managing the ThinkSystem servers and other BMC-based servers installed with the Windows 2016 operating system. Therefore, it is not recommended to use IBM Platform Agent to manage servers.

Lenovo Hardware Management Pack contains several management packs. The following table provides the names, IDs, and the corresponding major functions of the management packs.

Table 1. Lenovo Hardware Management Pack function list

Lenovo Hardware Management Pack		**Major functions**			
Management pack name	Management pack ID	Manage System x, ThinkSystem, BladeCenter, and Flex System servers through XClarity Integrator Service (out-of-band mode)	Manage ThinkServer servers through XClarity Administrator (out-of-band mode)	Manage System x, BladeCenter, and Flex System servers through IBM Platform Agent (in-band mode)	Manage Flex System chassis and BladeCenter chassis through SNMP
Lenovo Hardware Management Pack - Common Library	Lenovo.HardwareMgmt-Pack.Common	√	√	√	√
Lenovo Hardware Management Pack - Hardware IDs Library	Lenovo.HardwareMgmt-Pack.HardwareIDs			√	

Table 1. Lenovo Hardware Management Pack function list (continued)

Lenovo Hardware Management Pack - Relation Library	Lenovo.HardwareMgmt-Pack.Relation.v2			√	√
Lenovo Hardware Management Pack - Flex Relation Library	Lenovo.HardwareMgmt-Pack.RelationCMM.v2			√	√
Lenovo Hardware Management Pack for Integrated Management Module	Lenovo.HardwareMgmt-Pack.IMM2.v2	√			
Lenovo Hardware Management Pack for Lenovo BladeCenter Chassis and Modules	Lenovo.HardwareMgmt-Pack.BladeCenter.v2				√
Lenovo Hardware Management Pack for Lenovo Flex System chassis and Modules	Lenovo.HardwareMgmt-Pack.FlexSystem.v2				√
Lenovo Hardware Management Pack for Lenovo System x and x86/x64 Blade Systems	Lenovo.HardwareMgmt-Pack.xSystems			√	
Lenovo Hardware Management Pack for ThinkServer BMC	Lenovo.ThinkServer.BMC.Module		√		

Notes:

- Lenovo Hardware Management Pack for Lenovo System x and x86/x64 Blade Systems is required for the BMC auto-discovery and authentication function.
- Lenovo Hardware Management Pack for BMC Auto Discovery Override is not included in the previous table. It will be generated in runtime.

The following table provides the supported server models and functions of Lenovo Hardware Management Pack.

Table 2. Supported server models and functions

System	Server models	Supported functions			
		Manage System x, ThinkSystem, BladeCenter, and Flex System servers through XClarity Integrator Service (out-of-band mode)	Manage ThinkServer servers through XClarity Administrator (out-of-band mode)	Manage System x, BladeCenter, and Flex System servers through IBM Platform Agent (in-band mode)	Manage Flex System chassis and BladeCenter chassis through SNMP
Lenovo ThinkSystem	• SD530 (7X20, 7X21, 7X22) • SN550 (7X16, 7X17) • SN850 (7X15) • SR530 (7X07, 7X08) • SR550 (7X03, 7X04) • SR570 (7Y02, 7Y03) • SR590 (7X98, 7X99) • SR630 (7X01, 7X02) • SR650 (7X05, 7X06) • SR850 (7X18, 7X19) • SR860 (7X69, 7X70) • SR950 (7X11, 7X12, 7X13) • ST550 (7X09, 7X10) • ST558 (7Y15, 7Y16) (China only)	√			
Lenovo System x	• x240 M5 (2591, 9532) • x3250 M6 (3633, 3943) • x3500 M5 (5464) • x3550 M4 (7914) • x3550 M5 (5463) • x3630 M4 (7158) • x3650 M4 (7915) • x3650 M5 (5462, 8871) • x3750 M4 (8753) • x3850 X6 (6241) • x3950 X6 (6241) • x440 (7167, 2590)	√		√	
Lenovo Flex System	• x280, x480, x880 X6 Compute Node (7196, 4258) • x240 Compute Node (7162, 2588)	√		√	
Lenovo NeXtScale System®	• sd350 M5 (5493) • nx360 M5 (5465) • nx360 M5 DWC (5467, 5468, 5469)	√		√	

Table 2. Supported server models and functions (continued)

Lenovo ThinkServer	• RD350 • RD450 • RD550 • RD650 • RS160 • TD350 • TS460		√		
IBM System x	• x3100 M4 (2582, 2586) • x3100 M5 (5457) • x3200 M2 (4367, 4368) • x3200 M3 (7327, 7328) • x3250 M2 (4190, 4191, 4194) • x3250 M3 (4251, 4252, 4261) • x3250 M4 (2583, 2587) • x3250 M5 (5458) • x3300 M4 (7382) • x3350 (4192, 4193) • x3400 M2 (7836, 7837) • x3400 M3 (7378, 7379) • x3450 (7948, 7949, 4197) • x3455 (7940, 7941) • x3500 M2 (7839) • x3500 M3 (7380) • x3500 M4 (7383) • x3530 M4 (7160) • x3550 (7978) • x3550 M2 (7946) • x3550 M3 (4254, 7944) • x3550 M4 (7914) • x3620 M3 (7376) • x3630 M3 (7377) • x3630 M4 (7158) • x3650 (7979) • x3650 M2 (7947) • x3650 M3 (4255, 7945) • x3650 M4 (7915) • x3650 M4 HD (5460) • x3650 T (7980, 8837) • x3655 (7985) • x3690 X5 (7147, 7148, 7149, 7192) • x3750 M4 (8722,8733) • x3755 (7163, 8877) • x3755 M3 (7164) • x3850 M2 (7141, 7144, 7233, 7234)	√		√	

Table 2. Supported server models and functions (continued)

	• x3850 X5 (7143, 7145, 7146, 7191) • x3850 MAX5 (7145, 7146) • x3950 M2 (7141, 7144, 7233, 7234) • x3950 X5 (7143, 7145, 7146) • x3950 MAX5 (7145, 7146) • x3850 X6/x3950 X6 (3837, 3839) • iDataPlex dx360 M2 (6380, 7323, 7321) • iDataPlex dx360 M3 (6391) • iDataPlex dx360 M4 (7912, 7913)				
IBM Flex System	• x240 Compute Node (7906, 2585) • x222 Compute Node (7916) • x240 Compute Node (8737, 8738, 7863) • x440 Compute Node (7917)	√		√	
IBM BladeCenter	• HS12 (8014, 8028) • HS21 (8853) • HS22 (7870, 1911) • HS22V (7871) • HS23 (7875, 1929) • HS23E (8038, 8039) • HX5 (7872) • LS21 (7971) • LS22 (7901) • LS41 (7972) • LS42 (7902)	√		√	
IBM NeXtScale	5455	√		√	
BladeCenter chassis	7967, 8677, 8852, 7989, 8886, 7779, 8720, 8730, 8740, 8750				√
Flex System chassis	7893, 8721, 8724				√

Advantages

The following are the advantages of Lenovo Hardware Management Pack.

- Easily determining the overall health status of servers through the Lenovo Windows System Group folder.
- Monitoring the overall power consumption of the System x servers, the BladeCenter servers and the Flex System servers through the Power Data Chart, and generating the alerts when power consumption exceeds predefined thresholds.
- Monitoring the chassis modules health of the BladeCenter chassis in the Windows Health Explorer view.

- Remotely starting or shutting down a blade server or a compute node.
- Remotely shutting down the Windows operating system installed on a blade server or a compute node.
- Setting the maximum power capping and power threshold.
- Launching a CMM Web console of the BladeCenter chassis and the Flex System chassis.
- Discovering and managing BMC node automatically.
- Migrating the data from the PostgreSQL database to the SQL Server database.
- Configuring XClarity Integrator Service from Operations Manager.

Hardware and software requirements of the management server

This section describes how to determine whether a server is supported by Lenovo Hardware Management Pack as a management server. The management server shall meet the following hardware and software requirements.

Hardware requirements

This topic lists the hardware requirements of the management server depending on the number of managed servers.

Up to manage 100 Lenovo servers

	Minimum	**Recommended**
Processor	4-core 2.66 GHz processor	4-core 2.66 GHz processor
Memory	16 GB	32 GB
Free disk space	20 GB	40 GB
Network card	100 MBPS	10 GBPS

Up to manage 300 Lenovo servers

	Minimum	**Recommended**
Processor	4-core 2.66 GHz processor	8-core 2.66 GHz processor
Memory	16 GB	64 GB
Free disk space	20 GB	40 GB
Network card	100 MBPS	10 GBPS

Up to manage 500 Lenovo servers

	Minimum	**Recommended**
Processor	4-core 2.66 GHz processor	8-core 2.66 GHz processor
Memory	32 GB	64 GB
Free disk space	20 GB	40 GB
Network card	100 MBPS	10 GBPS

Software requirements

This topic lists the software requirements of the management server.

- Microsoft .NET Framework v4.0 (see Microsoft .NET Framework 4 (Standalone Installer) Web site)
- PowerShell 3.0 (see Windows PowerShell 3.0 Web site)
- Internet Explorer® 10, with KB3087038 or later versions (see Cumulative Security Update for Internet Explorer 10 for Windows Server 2012 (KB3087038) Web site)
- To use the SQL server database as the database in XClarity Integrator Service, ensure that the SQL server meets the following requirements:
  - Version: SQL server 2008 R2 SP3 or later version
  - Authentication mode: SQL Server and Windows Authentication mode
  - Disk size: 10GB free size for 100 managed servers, 30GB free size for 500 managed servers
  - CPU and memory: Four-core 2.66 GHz processor and 16 GB memory are recommended

  Note: To connect to a remote SQL server, install the SQL-Client-tools-connectivity program on the XClarity Integrator Service. This program can be found in SQL server installation image.

Supported versions of Operations Manager for the management server

The following versions of Operations Manager are supported for the management server:
- Microsoft System Center Operations Manager 2016
- Microsoft System Center Operations Manager 2012
- Microsoft System Center Operations Manager 2012 R2
- Microsoft System Center Operations Manager 2012 SP1

Supported Windows operating systems for the management server

The following Windows operating systems are supported for the management server:

- Windows 2008 R2 or later
- Windows Server 2012 SP1, R2
- Windows Server 2016

The Lenovo Hardware folder in Operations Manager

Lenovo Hardware Management Pack adds the Lenovo Hardware folder to Operations Manager. This folder provides the active alerts, task status, and aggregate targets for all discovered Lenovo servers and hardware components.

The Lenovo Hardware folder contains the following views and folders:

- **Views:**
  - **Lenovo System x and ThinkSystem BMC:** This view provides the status of the BMC-based servers (excluding the ThinkServer servers).
  - **Lenovo ThinkServer BMC:** This view provides the status of the ThinkServer servers.
  - **Lenovo ThinkServer Windows Computers:** This view provides the status of the ThinkServer servers that meet the following two requirements at the same time:
    - Installed with the Windows operating system.
    - Discovered by the Microsoft System Center Operations Manager 2007 Discovery Wizard (hereinafter referred to as the discovery wizard).
  - **Lenovo Windows System Group:** This view provides the status of BMC-based servers installed with the Windows operating system.
- **Folders:**

- **Lenovo BladeCenter(s) and Modules:** This folder contains the active alerts, the task status, the status of Windows computers that manage the BladeCenter chassis, and the general status of all BladeCenter chassis. The Lenovo BladeCenter Modules subfolder under this folder includes the summary views of Blade, Chassis, Cooling Module, I/O Module, Management Module, Medi Modules, Power Modules, and Storage Modules.
- **Lenovo Flex System Chassis and Modules:** This folder contains the active alerts, the task status, the status of Windows computers that manage the Flex System chassis, and the general status of all Flex System chassis. The Lenovo Flex System Chassis and Modules subfolder under this folder includes the summary views of Compute Nodes, Cooling Modules, FanMux Modules, FSM, I/O Modules, Management Modules, Power Modules, RearLED Modules, and Storage Modules.
- **Lenovo System x and ThinkSystem BMC:** This folder contains the summary views of Active Alerts, Cooling Devices, Fibre Channel, Firmware/VPD, InfiniBand, Network Adapter, Numeric Sensors, PCI Device, Physical Memory, Processors, and RAID Controller for Lenovo BMC-based servers (excluding the ThinkServer servers).
- **Lenovo ThinkServer BMC:** This folder contains the summary views of Active Alerts, Cooling Devices, Fibre Channel, Firmware/VPD, InfiniBand, Numeric Sensors, PCI Device, Physical Memory, and Processors for the ThinkServer servers.
- **Lenovo Windows System Group:** This folder contains the summary views of the BMC-based servers installed with the Windows operating system. These servers are grouped based on the types, such as tower, rack, blade, enterprise server, and so on. The Hardware Components of Lenovo Windows System Servers subfolder under this folder includes the summary views of Cooling Fans, Management Controllers, Netword Adapters, Physical memory, Physical Processors, Power Supplies, Storage (Non-Specific), Storage (ServeRAID-8x/7x/6x), Storage (ServeRAID-BR or Integrated RAID), Storage (ServeRAID-MR or MegaRAID), Temperature Sensors, Voltage Sensors, and Unclassified Hardware.

Lenovo system groups in Operations Manager

Lenovo Hardware Management Pack defines some Lenovo system groups in Operations Manager. You can find the groups by selecting **Authoring → Groups**.

- **Lenovo Windows System Group**: This group includes the servers installed with the Windows operating system.
- **Lenovo System x and ThinkSystem Group**: This group includes the System x servers and the ThinkSystem servers.
- **Lenovo ThinkServer Group**: This group includes the ThinkServer servers.
- **Lenovo Flex System Chassis Group**: This group includes the Flex System chassis.
- **Lenovo BladeCenter Chassis Group**: This group includes the BladeCenter chassis.

Chapter 2. Installing Lenovo Hardware Management Pack

This section describes how to install, upgrade, and uninstall Lenovo Hardware Management Pack.

Installing Lenovo Hardware Management Pack

The following procedure describes how to install Lenovo Hardware Management Pack.

Before you begin

Before installing Lenovo Hardware Management Pack, ensure that:

- The server to be used and the Operations Manager console are connected to the same management server.
- Current user has administrator privilege.
- The firewall does not block the network ports of XClarity Integrator Service (default value: 9500). For more information, refer to Appendix C “System firewall settings” on page 49.

Operations Manager contains some management packs. To successfully install Lenovo Hardware Management Pack, ensure that the management packs for Operations Manager meet the version requirements listed in the following table.

Table 3. Version requirements for the management packs of Operations Manager

Management packs name	Management packs ID	Management packs
Health Library	System.Health.Library	6.0.5000.0 or above
System Library	System.Library	6.0.5000.0 or above
Performance Library	System.Performance.Library	6.0.5000.0 or above
SNMP Library	System.Snmp.Library	6.0.6278.0 or above
Data Warehouse Library	Microsoft.SystemCenter. Datawarehouse.Library	6.0.6278.0 or above
System Center Core Library	Microsoft.SystemCenter.Library	6.0.5000.0 or above
Network Device Library	System.NetworkManagement.Library	7.0.8107.0 or above
Windows Core Library	Microsoft.Windows.Library	6.0.5000.0 or above

Procedure

Step 1. Download the Lenovo Hardware Management Pack installer from the XClarity Integrator download page.

Step 2. Double-click the installer. The welcome screen is displayed.

Step 3. Read the license agreement, select the **I accept both the Lenovo and the non-Lenovo terms** check box, and click **Next**.

Step 4. Select one of the following installation modes:

- **Full Installation:** Install all hardware components, including Lenovo XClarity Integrator Service.
- **Console Only:** Only install console-related hardware components. Select this option when only the Operations Manager console is on the server.

Step 5. Install the package according to the prompts on the installation wizard.

Step 6. Install XClarity Integrator Service, and set the password, the network port (default value: 9500), and the database.

Notes:

- XClarity Integrator Service supports the PostgreSQL database and the SQL server database. If you select the PostgreSQL database, a new PostgreSQL database is installed on the server. If you select the SQL server database, you shall input the SQL server information.
- For more information, refer to Lenovo XClarity Integrator Service online documentation.
- You can migrate the data from the PostgreSQL database to the SQL server database. Refer to “Migrating the data from the PostgreSQL database to the SQL server database” on page 10.

Step 7. Import the management packs to Operations Manager based on the prompts in the installation wizard.

Notes:

- The management packs will be upgraded automatically.
- If the importing process failed, remove the old management packs from the Operation Manager and import the new management packs manually. By default, the management packs are in the folder `%Program Files%\Lenovo \Lenovo Hardware Management Pack\Management Packs`.

Step 8. Click **Finish**.

Migrating the data from the PostgreSQL database to the SQL server database

The following procedure describes how to migrate the data from the PostgreSQL database to the SQL server database.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Click **Migrate Data** on the left side of the page.

Step 3. Click **Migrate Data**.

Step 4. Click **OK**. The migration process starts.

Step 5. Click **OK** again after the migration process is finished.

Notes:

- Do not delete the data file and the configuration file on the PostgreSQL database.
- The old data in the SQL server database is overwritten with the migrated data after the migration process.

Viewing the database information

The following procedure describes how to view the database information.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. To view the database information, click the **Database Information** tab in the left navigation pane.

Uninstalling Lenovo Hardware Management Pack

The following procedure describes how to uninstall Lenovo Hardware Management Pack.

Before you begin

Before uninstalling Lenovo Hardware Management Pack from the management server, ensure that the management server installed with Lenovo Hardware Management Pack is in the maintenance mode.

Procedure

Step 1. On the Windows operating system, click **Control Panel → Uninstall a program**, the **Uninstall or change a program** page opens.

Step 2. Right-click **Lenovo Hardware Management Pack**, and click **Uninstall**.

Note: For Lenovo Hardware Management Pack v7.3.0 or earlier version, the application name is "Lenovo XClarity Integrator Unified Service".

Step 3. Right-click **PostgreSQL database**, and click **Uninstall**.

Step 4. If necessary, delete all data permanently by doing the following:

a. Delete the database files or the database named as "%hostname%LXCIDB" from the folder `%USERPROFILE%\postgresql_data for PostgreSQL`.

b. Delete the application folder `%SystemDrive%\Program Files (x86)\Lenovo\Lenovo XClarity Integrator XClarity Integrator Service`.

c. Delete the configuration files from the folder `%SystemDrive%\ ProgramData\Lenovo\LXCI\UUS`.

d. Delete Lenovo Hardware Management Pack `%SystemDrive%\Program Files\Lenovo\Lenovo Hardware Management Pack`.

e. Delete the folder `%USERPROFILE%\Lenovo\LXCI\HWMP`.

Upgrading Lenovo Hardware Management Pack

To upgrade Lenovo Hardware Management Pack, you shall uninstall it first, and then install the new version.

Before you begin

Before upgrading Lenovo Hardware Management Pack, ensure that the management server installed with Lenovo Hardware Management Pack is in the maintenance mode.

Procedure

Step 1. On the Windows operating system, click **Control Panel → Uninstall a program**, the **Uninstall or change a program** page opens.

Step 2. Right-click **Lenovo Hardware Management Pack**, and click **Uninstall**.

Step 3. Right-click **Lenovo XClarity Integrator Service**, and click **Uninstall**.

Notes:

- Do not delete the folder `%SystemDrive%\ ProgramData\Lenovo\LXCI\UUS` and the database files in this folder.
- For Lenovo Hardware Management Pack v7.3.0 or earlier versions, the application name is "Lenovo XClarity Integrator Unified Service".

Step 4. Install the new Lenovo Hardware Management Pack to the management server.

Chapter 3. Managing servers through XClarity Integrator Service

Lenovo Hardware Management Pack supports to manage the BMC-based servers through XClarity Integrator Service in out-of-band mode, including the System x servers, the ThinkSystem servers, the BladeCenter servers, and the Flex System servers.

Lenovo Hardware Management Pack provides the following functions:

- Discovering and authenticating the BMC-based servers
- Monitoring the health of the BMC-based servers and displaying the events and alerts
- Retrieving and displaying the information of the BMC-based servers
- Managing power capping
- Providing an option for deleting the BMC-based servers

Before you begin

Before you begin, ensure that:

- The target BMC node is connected to port 5988 (HTTP) or port 5989 (HTTPS) through CIM protocol.
- There are four services of Lenovo XClarity Integrator Service:
  - Lenovo XClarity Integrator Management Webservice
  - Lenovo XClarity Integrator Monitor
  - Lenovo XClarity Integrator Server
  - Lenovo XClarity Integrator Service Starter
- The firewall does not block the network port of XClarity Integrator Service (default value: 9500).

Supported server models

Refer to the “Manage System x, ThinkSystem, BladeCenter, and Flex System servers through XClarity Integrator Service (out-of-band mode)” column of Table 2 “Supported server models and functions” on page 3.

Configuring XClarity Integrator Service

To monitor the BMC-based servers, you shall configure XClarity Integrator Service first. This section describes how to configure XClarity Integrator Service. For more information, refer to Lenovo XClarity Integrator Service.

Logging in to XClarity Integrator Service

The following procedure describes how to log in to the Lenovo XClarity Integrator Service.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Windows Computers**.

Step 3. Click **(Lenovo) XClarity Integrator Management** in the **Task** pane on the right.

Step 4. Log in by using the user name and password of XClarity Integrator Service, which are generated during the installation.

Changing password of XClarity Integrator Service

The following procedure describes how to change the password of XClarity Integrator Service.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. On the **Lenovo XClarity Integrator Service** window, click **Change Password** in the bottom-right corner.

Step 3. Input the existing password and the new password.

Note: The new password must conform to the password rules.

Step 4. Click **Change**.

Restarting XClarity Integrator Service

The following procedure describes how to restart XClarity Integrator Service.

To restart Lenovo XClarity Integrator Service, restart the following four services:

- Lenovo XClarity Integrator Management Webservice
- Lenovo XClarity Integrator Monitor
- Lenovo XClarity Integrator Server
- Lenovo XClarity Integrator Service Starter

Discovering the BMC node

After configuring XClarity Integrator Service, you can discover the BMC node. This section describes how to discover the BMC node.

BMC node discovery and authentication

The following procedure describes how to discover and authenticate the BMC node from the management server.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Windows Computers**.

Step 3. Click **(Lenovo) Discover/Authenticate BMC** in the **Task** pane on the right. The **BMC Discovery** page opens.

Step 4. Log in to XClarity Integrator Service. Generally, XClarity Integrator Service and Operations Manager are installed on the same server.

Step 5. Fill in the following fields:

- **Host:** This is the address of the management server installed with Operations Manager.
- **Port:** This is the port number of Lenovo XClarity Integrator Service, which is set during the installation. The default value is 9500.
- **Password:** This is the password of Lenovo XClarity Integrator Service, which is set during the installation.

Step 6. If a certificate warning is displayed, click **Next** to trust this certificate.

Note: If you do not trust the certificate, an alert stating that there is a problem with the Web site security certificate will be displayed. Click **Continue** to skip this alert.

Step 7. From the BMC discovery list, select a BMC node to be discovered, type the address or the address range in the **IP Address** field, and click **Add → OK**.

Note: The discovery process takes several minutes.

Step 8. Select a BMC node to be authenticated, and click **Authenticate**.

Step 9. Input the user name and password in the prompt window, and click **OK**.

Note: If you input the wrong user name or password for two times, the account will be locked for a period of time.

Step 10. Click **(Lenovo) Refresh BMC** in the **Task** pane on the right, the new BMC node is displayed.

BMC node auto-discovery and authentication

Lenovo Hardware Management Pack can discover and authenticate the BMC node automatically when the target server is managed by Operations Manager.

Notes:

- BMC node auto-discovery and authentication are not accessible to the Flex System servers and the BlaceCenter servers.
- In IPv6-only environment, BMC node auto-discovery and authentication are only accessible to the ThinkSystem servers. For the supported Lenovo ThinkSystem server models, refer to Table 2 “Supported server models and functions” on page 3.

Before you begin

Before using the BMC node auto-discovery and authentication function, ensure that:

- Windows 2008 or later version, and PowerShell 3.0 or later version are installed on the target server.
- The server is managed by Operations Manager.
- The BMC node is connected.
- The local account is valid on BMC.

Enabling or disabling BMC node auto-discovery and authentication

- By default, the BMC node auto-discovery and authentication is enabled.
- To disable the BMC node auto-discovery and authentication, type `BMC_AUTO_ DISCOVERY = false` in `% SystemDrive%\ProgramData\Lenovo\LXCI\UUS\global.conf`.

Notes:

- By default, you do not need to do any configuration.
- If the network port of XClarity Integrator Service is changed, or XClarity Integrator Service is not installed in the target server, you shall change the UUSServerIP value and the UUSPort value. These values can be changed in the “Lenovo.HardwareMgmtPack.AutoOOB.Discovery” Object Discovery program in Operations Manager.
- By default, the auto-discovery and authentication interval is four hours (14400 seconds). You can change the interval if necessary.
- Do not override the UUSCert value and the UUSPbKey value.

- The BMC node auto-discovery does not work when only LDAP authentication is enabled on the target BMC node or the local account is disabled.
- In the target BMC node, if you select the **Force to change password on first access** check box, and the value in the **Minimum password change interval** field is not set to zero, the BMC node auto-discovery and authentication interval will be the same as the minimum password change interval.

Monitoring the system health

This section describes how to monitor the health of the BMC-based servers and their hardware components.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware → Lenovo System x and ThinkSystem BMC**.

Step 3. To view the overall status of the BMC-based servers, select the **Lenovo System x and ThinkSystem BMC** view.

Step 4. To view the critical or warning alerts associated with the hardware, click **Active Alerts**. To learn more about the alerts, refer to “Using Health Explorer to view and resolve problems” on page 41.

Step 5. To view the hardware components information, select the hardware component that you want to check.

Notes:

- The **Lenovo System x and ThinkSystem BMC** folder includes the views of Cooling Devices, Fibre Channel, Firmware/VPD, InfiniBand, Network Adapter, Numeric Sensors, PCI Device, Physical Memory, Processors, and RAID Controller.
- The hardware components not covered by the health monitor function are marked with “Not monitored” in the view. When the health status of the hardware components is changed, alerts will be generated.
- The following table provides the monitor information of the hardware components.

Table 4. Health monitor information for the hardware components

Components	Health monitor
Cooling Devices	**Y**
Physical Memory	**Y**
Processor	**Y**
Fibre Channel	**N**
InfiniBand	**N**
Network Adapter	**N**
Numeric Sensor	**N**
PCI Device	**N**
RAID Controller	**N**

Obtaining the latest information for the BMC-based servers

The following procedure describes how to obtain the latest information for the BMC-based servers, including the inventory and status of servers and hardware components.

Procedure

The information of the BMC-based servers will be automatically refreshed every four hours. To refresh the information manually, do one of the following:

- Click **Monitoring → Windows Computers**, and click **(Lenovo) Refresh BMC** in the **Task** pane on the right.
- Click **Monitoring → Lenovo Hardware**, select the **Lenovo System x and ThinkSystem BMC** view, and click **(Lenovo) Refresh BMC** in the **Task** pane on the right.

Setting the power capping

The following procedure describes how to set a maximum power capping value for the BMC-based servers.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**, and click the **Lenovo System x and ThinkSystem BMC** view.

Step 3. Select the server that you want to set the power capping value.

Step 4. Click **(Lenovo) Power Management** in the **Task** pane on the right. The **Power Capping Management** dialog box opens.

Step 5. Input a new power capping value, and click **OK** to save this value.

Removing a BMC node

The following procedure describes how to remove a BMC node.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**.

Step 3. Click the **Lenovo System x and ThinkSystem BMC** view, select a BMC node, and click **(Lenovo) Remove BMC** in the **Task** pane on the right.

Step 4. Click the **(Lenovo) Refresh BMC** task to refresh the BMC node. The deleted BMC node will not be displayed in XClarity Integrator Service discovery list.

Chapter 4. Managing servers through XClarity Administrator

Lenovo Hardware Management Pack supports to manage the ThinkServer servers through XClarity Administrator in out-of-band mode.

Lenovo Hardware Management Pack provides the following functions:

- Discovering the ThinkServer servers through XClarity Administrator
- Monitoring the health of the ThinkServer servers and displaying the events and alerts
- Retrieving and displaying the information of the ThinkServer servers
- Providing an option for deleting the BMC node

Before you begin

Before managing the ThinkServer servers, ensure that the target ThinkServer server is managed by XClarity Administrator.

Supported servers

Refer to the “Manage ThinkServer servers through XClarity Administrator (out-of-band mode)” column of Table 2 “Supported server models and functions” on page 3.

Configuring XClarity Administrator

To monitor the ThinkServer servers, you shall configure XClarity Administrator first. The ThinkServer servers managed by Lenovo XClarity Administrator will be automatically discovered in Operations Manager after the configuration.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Windows Computers**.

Step 3. Click **(Lenovo) XClarity Administrator** in the **Task** pane on the right. The **Rigistered Lenovo XClarity Administrator** page opens.

Step 4. Click **Register**. Input the IP address, user name, password, and port for XClarity Administrator. Then, click **OK**.

Step 5. If the **View Certificate** page is displayed, click **Trust this certificate**. The new account is created.

Notes:

- The account is used to connect XClarity Integrator Service and XClarity Administrator. Do not create the new account when you are using LDAP in XClarity Administrator and the local account is disabled.
- If you create a new account, ensure that the specified XClarity Administrator account has supervisor privilege, and the roles of “lxc-operator”, “lxc-fw-admin”, “lxc-hw-admin”, and “lxc-os-admin” are in XClarity Administrator.
- You can download XClarity Administrator certificate from XClarity Administrator, and click **Manage trusted certificates → Add** to add XClarity Administrator certificate to XClarity Integrator Service manually.

Monitoring the system health

This section describes how to monitor the health of the ThinkServer servers and their hardware components.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware → Lenovo ThinkServer BMC**.

Step 3. To view the overall status of the ThinkServer servers, select the **Lenovo ThinkServer BMC** view.

Step 4. To view the critical or warning alerts associated with your hardware, click **Active Alerts**. To learn more about the alerts, refer to "Using Health Explorer to view and resolve problems" on page 41.

Step 5. To view the hardware components information, select the hardware component that you want to check.

Notes:

- The **Lenovo ThinkServer BMC** folder includes the views of Cooling Devices, Fibre Channel, Firmware/VPD, InfiniBand, Numeric Sensors, PCI Device, Physical Memory, and Processors.
- The hardware components not covered by the health monitor function are marked with "Not monitored" in the view. When the health status of the hardware components is changed, alerts will be generated.
- The following table provides the monitor information of the hardware components.

Table 5. Health monitor information for the hardware components

Components	Health monitor
Cooling Devices	**N**
Physical Memory	**N**
Processor	**N**
Fibre Channel	**N**
InfiniBand	**N**
Numeric Sensor	**N**
PCI Device	**N**

Obtaining the latest information for the ThinkServer servers

The following procedure describes how to obtain the latest information for the ThinkServer servers, including the inventory and status of servers and hardware components.

Procedure

The information of the ThinkServer servers will be automatically refreshed every four hours. To refresh the information manually, do one of the following:

- Click **Monitoring → Windows Computers**, and click **(Lenovo) Refresh BMC** in the **Task** pane on the right.
- Click **Monitoring → Lenovo Hardware**, select the **Lenovo ThinkServer BMC** view, and click **(Lenovo) Refresh BMC** in the **Task** pane on the right.

Removing a ThinkServer server

The following procedure describes how to remove a ThinkServer server.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**.

Step 3. Click the **Lenovo ThinkServer BMC** view, select a ThinkServer server, and click **(Lenovo) Remove BMC** in the **Task** pane on the right.

Step 4. Click the **(Lenovo) Refresh BMC** task to refresh the ThinkServer servers. The deleted ThinkServer server will not be displayed in XClarity Administrator discovery list.

Chapter 5. Managing chassis through SNMP

Lenovo Hardware Management Pack supports to manage the chassis (including the BladeCenter chassis and the Flex System chassis) and chassis modules through SNMP.

Lenovo Hardware Management Pack provides the following functions:

- Discovering and authenticating the Advanced Management Module (AMM)
- Monitoring the health of the chassis and chassis modules, and displaying the events or alerts
- Retrieving and displaying information for the chassis
- Remotely starting or shutting down a blade server or a compute node
- Remotely shutting down the Windows operating system installed on a blade server or a compute node

Before you begin

Before managing the chassis, ensure that SNMP is configured correctly on the chassis.

Supported chassis

Refer to the "Manage Flex System chassis and BladeCenter chassis through SNMP" column of Table 2 "Supported server models and functions" on page 3.

Configuring the SNMP agent

To monitor the chassis and chassis modules, configure the SNMP agent first. The BladeCenter chassis support SNMPv1 Agent only, while the Flex System chassis support both SNMPv1 Agent and SNMPv3 Agent.

Note: SNMPv1 Agent does not support IPv6.

Configuring SNMPv1 Agent on the BladeCenter chassis

The following procedure describes how to configure SNMPv1 Agent on the BladeCenter chassis.

Procedure

Step 1. Log in to the AMM Web console of the BladeCenter chassis. Refer to "Launching the AMM/CMM Web console" on page 28.

Step 2. Click **MM Control → Port Assignments** to ensure that the setting of SNMP Agent is 161 and the setting of SNMP Traps is 162.

Note: Use the default SNMP ports of 161 for agent (queries/polling) and 162 for trapping. It is important for SNMP port settings to be consistent. Otherwise, Operations Manager cannot discover the BladeCenter chassis.

Step 3. Click **MM Control → Network Protocols → Simple Network Management Protocol (SNMP)**, and complete the following steps:

a. Select **Enabled for SNMP Traps**, **SNMPv1 agent**.

b. Input the following information for all Operations Managers programs that manage the BladeCenter chassis:

- In the **Community name** field, input the community name that assigned to the BladeCenter chassis through which SNMP communicates.

- From the **Fully Qualified Hostnames or IP Addresses** list, input the Operations Manager address.

c. From the **Access type** list, select **Set**. **Set** is the access type required for enabling the management tasks. A task example is remotely starting or shutting down a blade server through the Operations Manager console.

Notes:

- If you do not intend to allow this type of task through the Operations Manager console, you can lower the access type to **Get**. At a minimum, the **Get** access type must be set for the Operations Manager server to perform the SNMP queries, and receive the SNMP traps from the BladeCenter.
- Ensure that the values of SNMPv1 Agent account in the SCOM discovery wizard are consistent with those set in Operations Manager. Otherwise, Operations Manager cannot discover the BladeCenter chassis.

Step 4. Configure the SNMP event recipients and the BladeCenter chassis.

a. Click **MM Control → Alerts**. In the right pane, under **Remote Alert Recipients**, click **not used** link to configure the alert recipient.

Note: Depending on the firmware level, the menu might vary slightly.

b. In the new Remote Alert Recipient window, change the status from **Disabled** to **Enabled**.

c. In the **Name** field, input a descriptive name for the management server for Operations Manager that will be used in managing the BladeCenter chassis.

d. From the **Notification method** list, select **SNMP over LAN**.

e. Click **Save**.

Step 5. Configure the monitored alerts.

a. Click **MM Control → Alerts**.

b. From the context menu, click **Monitor Alerts**.

c. Select the alerts to be sent, and click **Save**.

Configuring SNMP on the Flex System chassis

The following procedure describes how to configure SNMP on the Flex System chassis, including SNMPv1 Agent and SNMPv3 Agent.

Procedure

Step 1. Log in to the CMM Web console. Refer to “Launching the AMM/CMM Web console” on page 28.

Step 2. Click **Mgt Module Management → Network → Port Assignments** to ensure that the setting of SNMP Agent is 161 and the setting of SNMP Traps is 162.

Note: To change the SNMP settings, select **Enable SNMPv1 Agent** or **Enable SNMPv3 Agent**. Refer to “Configuring SNMPv1 Agent” on page 25 and “Configuring SNMPv3 Agent” on page 25.

Step 3. Configure the SNMP event recipients and the Flex System chassis.

a. Click **Events → Event Recipients → Create → Create SNMP Recipient**.

b. In the **Descriptive name** field, input a name.

c. From the **Status** list, select the **Enable this recipient** check box.

d. From the **Events to receive** list, select the **Use the global settings** check box or the **Only receive critical alerts** check box, and click **OK** to return to the **Event Recipients** page.

Note: If you select the **Use the global settings** check box, you shall click **Global Settings** on the **Event Recipients** page to change the settings, and click **OK** to apply the changes.

Configuring SNMPv1 Agent

The following procedure describes how to configure SNMPv1 Agent on the Flex System chassis.

Procedure

Step 1. Click **Mgt Module Management → Network → SNMP**, and select the **Enable SNMPv1 Agent** check box.

Step 2. Click **Traps**, and select the **Enable SNMP Traps** check box.

Step 3. Select **Communities**, and input the following information:

a. In the **Community name** field, input the name that assigned to the Flex System chassis.

b. From the **Access type** list, select **Set**.

c. From the **Fully Qualified Hostnames or IP Addresses** list, select appropriate address.

Notes:

- By default, the Chassis Module Security Policies level is “Secure”. At this level, SNMPv1 Agent cannot be enabled. To enable SNMPv1 Agent, click **Mgt Module Management → Security → Security Policies → Legacy → Apply**.
- Ensure that the values of SNMPv1 Agent account in the SCOM discovery wizard are consistent with those set in Operations Manager. Otherwise, Operations Manager cannot discover the Flex System chassis.

Configuring SNMPv3 Agent

The following procedure describes how to configure SNMPv3 Agent on the Flex System chassis. You shall create a new user account before using SNMPv3 Agent or use the default user account.

Procedure

Step 1. Click **Mgt Module Management → User Accounts**, select an existing user account from the list or create a new SNMPv3 user account.

Step 2. Double-click a user name to open the **User Properties** page. Then, click the **General** tab and set a user password for the new account.

Step 3. Click **SNMPv3**, and input the following information:

a. From the **Authentication Protocol** list, select **Hash-based Message Authentication Code (HMAC) – Secure Hash Algorithm (SHA)**.

b. Select the **Use a privacy protocol** check box.

c. From the **Encryption Method** list, select **Advanced Encryption Standard (AES)**.

d. In the **Privacy password** field and the **Confirm privacy password** field, input the authentication key.

e. Change the access type to **Set**.

f. In the **IP address or host name for traps** field, input the Operations Manager IP address.

Step 4. Click **OK**.

Discovering a chassis

The following procedure describes how to discover a chassis.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Administration → Network Management → Discovery Rules → Discover Network Device** to start the **Network Device Discovery Wizard**.

Step 3. On the **General Properties** page, do the following:

a. In the **Name** field, input the name of the discovery rule.

b. Select a management or gateway server.

c. Select a resource pool.

Note: If there are several servers, ensure that all servers in the resource pool are installed with Lenovo Hardware Management Pack.

d. Click **Next**.

Step 4. On the **Discovery Method** page, select **Explicit Discovery**, and click **Next**.

Step 5. On the **Default Accounts** page, click **Next**. The **Devices** page opens.

Step 6. On the **Devices** page, click **Add**. The **Add a Device** dialog box opens.

Step 7. In the **Add a Device** dialog box, do the following:

a. In the **Name or IP address** field, input the IP address of the chassis.

b. From the **Access Mode** list, select **SNMP**.

c. Keep the port number as the default value 161.

d. Select the appropriate SNMP version.

e. Do one of the following:

- To select the existing account, click **SNMP V3 Run As account** or **SNMP V1 or V2 Run As account**.
- To add a new account, click **Add SNMP V3 Run As account** or **Add SNMP V1 or V2 Run As account**.

Note: Ensure that the values of SNMPv1 Agent account or SNMPv3 Agent account are consistent with those set in the chassis account.

f. Click **OK** to return to the **Network Device Discovery Wizard**.

Step 8. Click **Next**. Then, set the time for running the discovery rule, and click **Save**. If a window opens and prompts you to distribute the accounts, click **Yes**.

Step 9. Click **Discovery Rule → Run**.

Step 10. Wait for a while, and click **Network Management → Network Devices**. The discovered chassis is displayed.

Monitoring the chassis health

This section describes how to monitor the health of chassis and chassis modules.

Monitoring the BladeCenter chassis health

The following procedure describes how to monitor the health of the BladeCenter chassis and chassis modules.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware → Lenovo BladeCenter(s) and Modules**.

Step 3. To view the overall status of the BladeCenter chassis, select the **Lenovo BladeCenter(s)** view.

Step 4. To view the critical or warning alerts associated with the hardware, click **Active Alerts**. To learn more about the alerts, refer to “Using Health Explorer to view and resolve problems” on page 41.

Step 5. To view the chassis modules information, click **Lenovo BladeCenter Modules**, and select the chassis module that you want to check.

The views in the **Lenovo BladeCenter Modules** subfolder include:

- Lenovo BladeCenter Blades
- Lenovo BladeCenter Chassis
- Lenovo BladeCenter Cooling Modules
- Lenovo BladeCenter I/O Modules
- Lenovo BladeCenter Management Modules
- Lenovo BladeCenter Media Modules
- Lenovo BladeCenter Power Modules
- Lenovo BladeCenter Storage Modules

Monitoring the Flex System chassis health

The following procedure describes how to monitor the health of the Flex System chassis and chassis modules.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware → Lenovo Flex System Chassis and Modules**.

Step 3. To view the overall status of the Flex System chassis, select the **Lenovo Flex System chassis** view.

Step 4. To view the critical or warning alerts associated with the hardware, click **Active Alerts**. To learn more about the alerts, refer to “Using Health Explorer to view and resolve problems” on page 41.

Step 5. To view the chassis modules information, click **Lenovo Flex System chassis and Modules**, and select the chassis module that you want to check.

The views in the **Lenovo Flex System Chassis Modules** subfolder include:

- Lenovo Flex System chassis Compute Nodes
- Lenovo Flex System chassis Cooling Modules
- Lenovo Flex System chassis FanMux Modules
- Lenovo Flex System chassis FSM
- Lenovo Flex System chassis I/O Modules
- Lenovo Flex System chassis Management Modules
- Lenovo Flex System chassis Power Modules
- Lenovo Flex System chassis RearLED Modules
- Lenovo Flex System chassis Storage

Obtaining the latest information for the chassis

The following procedure describes how to obtain the latest information for the chassis, including the inventory and status of chassis and chassis modules.

The information of the chassis will be automatically refreshed every four hours. To refresh the information manually, do the following:

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**.

Step 3. Do one of the following:

- Click **Lenovo BladeCenter(s) and Modules → Lenovo BladeCenter(s)**, and select a BladeCenter chassis in the **Lenovo BladeCenter(s)** pane.
- Click **Lenovo Flex System Chassis and Modules → Lenovo Flex System Chassis**, and select a Flex System chassis in the **Lenovo Flex System Chassis** pane.

Step 4. Click **(Lenovo) Refresh this Chassis Modules** in the **Task** pane on the right. Then, the latest information for the chassis will be displayed.

Launching the AMM/CMM Web console

The Advanced Management Module (AMM) is a module that enables you to configure and manage the BladeCenter chassis, while the Chassis Management Module (CMM) is a module that you use to configure and manage the Flex System chassis. The following procedure describes how to launch the AMM/CMM Web console.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**.

Step 3. Do one of the following:

- For the BladeCenter chassis, click the **Lenovo BladeCenter(s) and Modules** folder, and select the **Lenovo BladeCenter(s)** view.
- For the Flex System chassis, click the **Lenovo Flex System Chassis and Modules** folder, and select the **Lenovo Flex System Chassis** view.

Step 4. Select a BladeCenter chassis or a Flex System chassis.

Step 5. Depending on your chassis, click **Lenovo BladeCenter Chassis Management Web Console** or **Lenovo Flex System Chassis Management Web Console** in the **Task** pane on the right.

Starting or shutting down a blade server or a compute node

The following procedure describes how to start or shut down a blade server or a compute node, and how to shut down the Windows operating system installed on a blade server or a compute node.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**.

Step 3. Do one of the following:

- For the BladeCenter chassis, click the **Lenovo BladeCenter(s) and Modules** folder, and click the **Lenovo BladeCenter Blades** view under the **Lenovo BladeCenter Modules** subfolder.
- For the Flex System chassis, click the **Lenovo Flex System Chassis and Modules** folder, and click the **Lenovo Flex System chassis Compute Nodes** view under the **Lenovo Flex System Chassis Modules** subfolder.

Step 4. Select a blade server or a compute node.

Step 5. According to your needs, click the corresponding task button.

Removing a discovered chassis

The following procedure describes how to remove a discovered chassis from the chassis list.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Administration → Network Management → Network Devices**.

Step 3. In the results pane, select a chassis to be removed.

Step 4. Click **Delete**. The chassis and its chassis modules will be removed.

Chapter 6. Managing servers through IBM Platform Agent

Lenovo Hardware Management Pack enables you to use IBM Platform Agent to manage the Lenovo servers installed with the Windows operating system in in-band mode. The Lenovo servers include the System x servers, the BladeCenter servers, and the Flex System servers.

Note: IBM Platform Agent does not support the ThinkSystem servers.

Before you begin

Before managing the Lenovo servers, ensure that:

- One of the following Windows operating systems is installed on the target server: Windows 2008, Windows 2008 R2, Windows 2012, or Windows 2012 R2.

  Note: Windows 2016 is not supported.
- The target server is managed by Operations Manager.
- IBM Platform Agent v.6.3.3 or later is installed on the target server. Refer to IBM Systems Director online documentation.
- IBM Remote Supervisor Adapter II (RSA-II Daemon) v5.4.6 or later is installed on the target server.

  Notes: The RSA-II Daemon for the Windows operating system is available at:

  – RSA-II Daemon v5.46 for Microsoft Windows IA32
  – RSA-II Daemon v5.44 for Microsoft Windows Server 2003/2008 (x64)

Supported server models

Refer to the “Manage System x, BladeCenter, and Flex System servers through IBM Platform Agent (in-band mode)” column of Table 2 “Supported server models and functions” on page 3.

Discovering a Lenovo server

The following procedure describes how to discover a Lenovo server using the **Microsoft System Center Operations Manager 2007 Discovery Wizard** (hereinafter referred to as the **Discovery Wizard**). The **Discovery Wizard** deploys Lenovo Hardware Management Pack to the discovered server.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. Click **Administration** → **Device Management** → **Agent Managed** → **Discovery Wizard**. The **Computer and Device Management Wizard** starts.

Step 3. Click **Discovery Type** → **Windows computers**, and click **Next**.

Step 4. Select the **Advanced discovery** check box.

Step 5. Select **Servers and Clients** from the **Computer and Device Classes** list, and select a Lenovo server to be added.

Step 6. Select the **Verify discovered computers can be contacted** check box, and click **Next**.

Step 7. Select the **Browse for, or type-in computer names** check box.

Step 8. Click **Browse** to detect the Lenovo server or manually type the Lenovo server name in the input box, and click **Next**.

Step 9. On the **Administrator Account** page, do one of the following:

- To select an existing server, select the **Use selected Management Server Action Account** check box, and click **Next**.
- To add a new server, select the **Other user account** check box, and type the new Lenovo server name.

Step 10. Click **Discover** to start the discovery process. When the discovery process is completed, the discovery results are displayed on the **Summary** page.

Note: The discovery time depends on the number of Lenovo servers in the network.

Step 11. On the **Summary** page, click **Finish**. The **Agent Management Task Status** page opens.

Step 12. Click **Monitoring → Task Status** to check the management task status. The Lenovo server is discovered when the status is changed from **Queued** to **Success**.

Monitoring the server health

This section describes how to monitor the health of the Lenovo servers and the hardware components, including fans, memory, management controllers, network adapters, power supplies, processors, storage, temperature sensors, and voltage sensors.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**.

Step 3. To view the overall status of the Lenovo servers, select one of the following views:

- **Lenovo Windows System Group:** This view provides the hardware status of all Lenovo servers.
- **Windows Computer on Lenovo Windows System Group:** This view lists the health indicators in the first column of the system dashboard and the hardware components dashboard.

Step 4. To view the critical or warning alerts associated with your hardware, click the **Lenovo Windows System Group** folder and click **Active Alerts**. To learn more about the alerts, refer to “Using Health Explorer to view and resolve problems” on page 41.

Step 5. To view the hardware components information, click the **Lenovo Windows System Group** folder and select the hardware component that you want to check.

Note: The undiscoverable hardware components cannot be monitored or managed.

Viewing the power data of the client System x servers

The following procedure describes how to view the power data of the client System x servers in Lenovo System x Power Data Chart. This chart is only available on the System x servers.

Before you begin

Ensure that the Windows operating system is installed on more than one managed System x servers.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware → Lenovo System x Power Data Chart**.

Step 3. Select the **Show** check box. The Power Data Chart is displayed.

Note: The power data displayed as a straight line means the power consumption is steady in a given period of time.

Setting the power capping

The following procedure describes how to set a maximum power capping value for the Lenovo servers.

Before you begin

Before setting a maximum power capping value, ensure that:

- The target server has power capping functions.
- User Access Control (UAC) is shut down on the target server.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**, and click the **Lenovo Windows System Group** view.

Step 3. Select the server that you want to set the power capping value.

Note: You can view the current power capping values of **CappingCapable**, **CappingEnabled**, **PowerMax**, **PowerMin**, and **PowerCap** of a server in **Detail View**.

Step 4. Click **(Lenovo) Set Power Capping** in the **Task** pane on the right. The **Run the task on these targets** pane is displayed.

Step 5. Input a new power capping value and click **Override**.

Step 6. Click **Run**. The task status window opens and indicates whether the value is overridden.

Setting the power threshold

The following procedure describes how to set a warning or critical power threshold for the Lenovo servers.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**, and click the **Lenovo Windows System Group** view.

Step 3. Select the server that you want to set the power threshold.

Note: You can view the current threshold values and the monitoring capacity property of the server in **Detail View**.

Step 4. Click **(Lenovo) Set/Unset Power Threshold** in the **Task** pane on the right. The **Run the task on these targets** pane is displayed.

Step 5. Input a new power threshold value, and click **Override**.

Note: If you input a blank or zero, the threshold will be reset to its default value.

Step 6. Click **Run**. The task status window opens and indicates whether the value is overridden.

Obtaining the latest information for the Lenovo servers

The following procedure describes how to obtain the latest information for the Lenovo servers, including the inventory and status of servers and hardware components.

The information of the Lenovo servers will be automatically refreshed every four hours. To refresh the information manually, do the following:

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Windows Computers**.

Step 3. Click **Refresh Lenovo Windows Computer** in the **Task** pane on the right. The latest information is displayed.

Chapter 7. Working with security certificates

XClarity Integrator Service connects to its supporting software through Secure Sockets Layer (SSL) certificates. By default, XClarity Integrator Service uses the self-generated certificates that signed and issued by an internal certificate authority (CA). This section describes how to set, generate, regenerate, and download the certificates.

Setting the BMC communication protocol

The following procedure describes how to set the BMC communication protocol.

Before you begin

Ensure that the HTTPS protocol is enabled on all BMC nodes if you only want to use the HTTPS protocol to communicate with BMC nodes.

Note: If you do not select the **Only use HTTPS protocol to communicate with BMC nodes** check box, the HTTPS protocol and the HTTP protocol will be enabled in sequece.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Click **Security Settings** in the left navigation pane. The **Security Settings** page opens.

Step 3. Click the **Security Settings** tab.

Step 4. Select the **Only use HTTPS protocol to communicate with BMC nodes** check box.

Step 5. Click **Save**.

Generating and uploading the certificates

When generating the customized server certificate in XClarity Integrator Service, you shall provide the certificate bundle that contains the entire CA signing chain.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Connect a server to XClarity Integrator Service.

Note: If the server certificate is not signed by a trusted international third party, a security message will be displayed. To avoid this security message, select the **Trust the certificate permanently** check box, and click **Next**.

Step 3. Generate the Certificate Signing Request (CSR) for XClarity Integrator Service.

a. Click **Security Settings**. The **Security Settings** page opens.

b. Click **Server Certificate**.

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

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

Note: You can allow XClarity Integrator Service to generate the common name automatically by keeping the default value **Generated by LXCI**.

e. Select the correct host name. If a wrong name is selected, the server cannot connect to XClarity Integrator Service.

f. Click **Generate CSR File**. The CSRs will be downloaded automatically.

Step 4. Send all CSRs to your trusted CA. The trusted CA will assign a certificate bundle for each CSR. The certificate bundle contains the customized certificates and the complete CA chain of trust.

Step 5. Upload the customized certificates and the generated server certificates to XClarity Integrator Service.

a. Click **Server Certificate** on the **Security Settings** page.

b. Click **Upload Certificate** to upload the certificate file (with the .cer extension).

Notes:

- The customized certificates shall contain the complete certificate chain, including the root certificates and the intermediate certificates.
- The uploading priority of the certificates is: server certificates, intermediate certificates, and root certificates.

Regenerating the certificates

If the existing certificate is invalid or the certificate version is not the latest, you can regenerate a new server certificate or a root certificate for XClarity Integrator Service to replace the old one.

Regenerating the server certificate

The following procedure describes how to regenerate the new server certificate for XClarity Integrator Service.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Click **Security Settings**. The **Security Settings** page opens.

Step 3. Click **Server Certificate**.

Step 4. Click **Regenerate Server Certificate**.

Step 5. Fill in all fields in the **Regenerate Server Certificate** page: Country, State or Province, City or Locality, Organization, Organization Unit (optional), and Common Name.

Note: You can allow XClarity Integrator Service to generate the common name automatically by keeping the default value **Generated by LXCI**.

Step 6. Select a correct host name. If a wrong name is selected, the server cannot connect to XClarity Integrator Service.

Step 7. Click **Regenerate Certificate**.

Regenerating the root certificate

The following procedure describes how to regenerate the new root certificate for XClarity Integrator Service.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Click **Security Settings**. The **Security Settings** page opens.

Step 3. Click **Certificate Authority**.

Step 4. Click **Regenerate Certificate Authority Root Certificate**.

Step 5. Read the information and click **OK**.

Notes:

- If the customized certificates are invalid, XClarity Integrator Service will generate the new certificates and replace the old certificates with these new ones automatically.
- If the customized certificates are valid, XClarity Integrator Service will only regenerate a new root certificate.

Downloading the certificates

You can download the server certificate and the root certificate.

Downloading the server certificate

The following procedure describes how to download the server certificate.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Click **Security Settings**. The **Security Settings** page opens.

Step 3. Click **Server Certificate**.

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

Step 5. Click **Download Certificate**.

Downloading the root certificate

The following procedure describes how to download a root certificate.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Click **Security Settings**. The **Security Settings** page opens.

Step 3. Click **Certificate Authority**.

Step 4. Click **Download Certificate Authority Root Certificate**.

Chapter 8. Log data

This section provides instructions on how to set the log level and how to collect or view logs.

Logs for XClarity Integrator Service

You can collect the log files and set the log level for XClarity Integrator Service.

Setting the log level

The following procedure describes how to set the log level for XClarity Integrator Service.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Click **Service Data** in the left navigation pane.

Step 3. Click the drop-down menu to set the log level:

- **Error level:** Recording error messages only.
- **Warning level:** Recording warning and error messages.
- **Information level:** Recording error, warning, and information messages.
- **Debug level:** Recording error, warning, information, and debug messages.

Collecting the log files

The following procedure describes how to collect the log files for XClarity Integrator Service.

Procedure

Step 1. Log in to XClarity Integrator Service. Refer to “Logging in to XClarity Integrator Service” on page 13.

Step 2. Click **Service Data** in the left navigation pane.

Step 3. Click **Collect Log → Download Log**. The logs for XClarity Integrator Service are downloaded.

Logs for Lenovo Hardware Management Pack

You can set the log level, and view the log of Lenovo Hardware Management Pack.

Setting the log level

The following procedure describes how to set the log level for Lenovo Hardware Management Pack.

Procedure

Step 1. On the Windows operating system, open the REG key `HKEY_LOCAL_MACHINE\SOFTWARE\Lenovo \Lenovo SCOM MP\Debug` in the **regedit.exe** program.

Step 2. In the REG key, double-click **Level**, and input one of the following values based on your needs:

- Error level: Level = 1
- Warn level: Level = 3
- Information level: Level = 5
- Debug level: Level = 7

Note: Ensure that the value type of the “Level” value is “String”.

Viewing the log in Windows Event Viewer

The following procedure describes how to view the logs for Lenovo Hardware Management Pack in Windows Event Viewer.

Procedure

Step 1. On the Windows operating system, launch Windows Event Viewer.

Step 2. Click **Applications and Services Logs → Operations Manager**. The logs of Lenovo Hardware Management Pack are displayed.

Step 3. In the **Actions** pane on the right, click **Filter Current Log**.

Step 4. Select the **Health Service Script** check box and the **Lenovo.EventLogSource**check box from the **Event sources** drop-down list. The logs of Lenovo Hardware Management Pack are displayed in the window.

Note: Only the **Lenovo.EventLogSource** check box is displayed in the **Event sources** drop-down list when there are LXCI Management Pack events.

Chapter 9. Troubleshooting

This section provides information to assist you with troubleshooting issues that you may have with Lenovo Hardware Management Pack.

Troubleshooting by symptoms

This topic provides information about basic troubleshooting and diagnostic methods to help you solve problems that might occur in the servers installed with Lenovo Hardware Management Pack. If you cannot diagnose and correct a problem by using the following information, refer to “Using Health Explorer to view and resolve problems” on page 41 or “Using Lenovo XClarity Forum and Lenovo XClarity Ideation” on page 42.

Symptom	Action
The discovered chassis installed with Windows Server 2012 is displayed in the **Network Devices Pending Management** view.	1. Start Operations Manager. 2. Start the inbound and outbound rules, and restart the discovery rule. **Note:** By default, some rules might be disabled. 3. Wait until the rules are converted to the scheduled task in the Operations Manager console.
AMM/CMM Web console cannot be opened from the Operations Manager console on a server installed with Windows Server 2012.	1. Click **Server Manager → Configure this local server**. The **Local Server Configuration** page opens. 2. Click **On** in the **Properties** pane. The **Internet Explorer Enhanced Security Configuration** dialog box opens. **Note:** If a member of the local administrator group also logs in, click **Off**. Then you can continue to use Internet Explorer Enhanced Security Configuration. 3. Click **OK** to apply the changes.
The error “Could not locate automation class named IBM.SystemsManagement.SCOMHelper. SCOMServer” is displayed.	Do one of the following: • Select a resource pool, which only includes the servers installed with Lenovo Hardware Management Pack. • Create a new resource pool, which only includes the servers installed with Lenovo Hardware Management Pack.

Using Health Explorer to view and resolve problems

The following procedure describes how to view, learn about, and resolve the alerts using Health Explorer.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**.

Step 3. Do one of the following depending on your server models:

- For the Lenovo servers, click the **Lenovo Windows System Group** view
- For the BMC-based servers, click the **Lenovo System x and ThinkSystem BMC** view
- For the ThinkServer servers, click the **Lenovo ThinkServer BMC** view

- For the BladeCenter chassis, click the **Lenovo BladeCenter(s)** view under the **Lenovo BladeCenter(s) and Modules** folder
- For the Flex System chassis, click the **Lenovo Flex System Chassis** view under the **Lenovo Flex System Chassis and Modules** folder

Note: By default, all failed monitors are displayed in an expanded view when Health Explorer opens.

Step 4. Select an alert, and double-click **State** to open Health Explorer. All basal-level health monitors that display the errors will be displayed in the **Health Explorer** page.

Step 5. Do one of the following depending on your needs:

a. To view the latest state change events, click **State Change Events**.

b. To view the explanations and solutions of the alert, click **Knowledge**. If necessary, perform the steps in the **Knowledge** page to resolve the error and reset the health sensor.

Note: You can also view the **Knowledge** page by clicking the **Active Alerts** view in the Operations Manager console or the link on the **Product Knowledge** tab.

c. To view the alert properties, double-click the alert. Alert Properties is displayed on the **General** tab.

Using Lenovo XClarity Forum and Lenovo XClarity Ideation

The following procedure describes how to post questions, suggestions or ideas using Lenovo XClarity Forum and Lenovo XClarity Ideation.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. In the left navigation pane, click **Monitoring → Lenovo Hardware**.

Step 3. Do one of the following depending on your server models:

- For the Lenovo servers, click the **Lenovo Windows System Group** view
- For the BMC-based servers, click the **Lenovo System x and ThinkSystem BMC** view
- For the ThinkServer servers, click the **Lenovo ThinkServer BMC** view
- For the BladeCenter chassis, click the **Lenovo BladeCenter(s)** view under the **Lenovo BladeCenter(s) and Modules** folder
- For the Flex System chassis, click the **Lenovo Flex System Chassis** view under the **Lenovo Flex System Chassis and Modules** folder

Step 4. Select a server or a chassis.

Step 5. To post questions, click **Lenovo XClarity Forum**; to post suggestions or ideas, click **Lenovo XClarity Forum** or **Lenovo XClarity Ideation**.

Step 6. Follow the instructions on the screen.

Appendix A. Accessibility features

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

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

Lenovo Hardware Management Pack supports the accessibility features of the integrated systems-management software. For the specific information about accessibility features and keyboard navigation, refer to your system management software documentation.

Lenovo Hardware Management Pack topic collection and its related publications are accessible for the Lenovo Home Page Reader. You can operate all features by using the keyboard instead of the mouse.

You can view the publications for Lenovo Hardware Management Pack in Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader. You can access the PDFs from Lenovo Hardware Management Pack download site.

Lenovo and accessibility

For more information about the commitment of Lenovo accessibility, refer to Lenovo Accessibility Web site.

Appendix B. Best practices

The topics in this section provide suggested methods for completing tasks.

Determining the cause of an error

Use the following diagnostic procedure to identify and solve problems that might occur in a managed environment.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. Click **Monitoring**.

Step 3. To view the status of all of your managed systems that have Windows operating systems installed, click **Lenovo Hardware → Windows Computers on Lenovo Windows Systems Group**.

Step 4. Check the health of the systems displayed in the top results pane. All newly discovered objects are in a healthy state by default. The Health check monitoring task updates the status of an object at regular intervals, according to the default interval setting. You can configure the monitoring frequency by using the **override-controlled** parameters. For more information about the **override-controlled** parameter, refer to Microsoft System Center Operations Manager documentation.

Step 5. Select a system that shows a *Critical* or *Warning* state.

Step 6. Determine whether the error is related to the hardware or software.

- **Hardware-related failures**: Check the Lenovo Hardware Components of the **System x or x86/x64 Blade Servers** pane to select the system. Scroll to the right to view all of the component status and data. You can personalize this view.

  This pane contains state views based on the class of the hardware component basis. The purpose of this view is to provide access to detailed properties of each component instance. Look for additional system information in the **Detail View** pane.

- **Software-related failures**: Check the Windows Computer in the **System x or x86/x64 Blade Servers** pane. This pane contains state views and information on a per-software-component-class basis. Select a system that has either a *Critical* or *Warning* health state.

  The purpose of these views is to provide access to detailed properties of each component instance. The **Detail View** shows all instances of the system software with a health state for each of the four health aspects.

Step 7. To obtain more information and details about a failure, access the hardware information of the desired BladeCenter module or hardware system component by clicking **Lenovo BladeCenter Modules**.

Step 8. If you already know that a power supply component failed, for example, select the related view, **Lenovo BladeCenter Power Modules**, to determine the problem with the power supply.

Step 9. Click a **Critical** power module and review its related data.

Step 10. Review the information and data presented in the **Detail View** pane. Check all instances of the module type and each of its four health aspects.

Step 11. Right-click the selected module, and click **open → Health Explorer**.

Step 12. Select the alert, and look at the information on the **State Change Events** page.

Step 13. Depending on the type of alert you have, you can click **View Alert** for more information.

Step 14. Click the **Knowledge** tab to read the **Knowledge** page and one or more Knowledge Articles that relate to your alert.

Important: In addition to the health information available for each object, related information might be available from other objects that are health-related from different perspectives. For example, a blade server that is monitored in-band through its platform agent shows a health state, but the BladeCenter chassis management module also shows a health state for the blade server.

Other BladeCenter chassis modules might affect the blade server health, such as a power supply that provides power to the blade server. Similarly, the health of a blade server from the management module perspective might include the health and other information about the operating system running on the blade server.

For instance, the following BladeCenter simple network management protocol (SNMP) alert has an event description field of *1.3.6.1.4.1.2.6.158.3.1.1.8* and an event ID of *1.3.6.1.4.1.2.6.158.3.1.1.14*. Convert the decimal event ID value to a hexadecimal number to look up the message in the *Advanced Management Module Message Guide*.

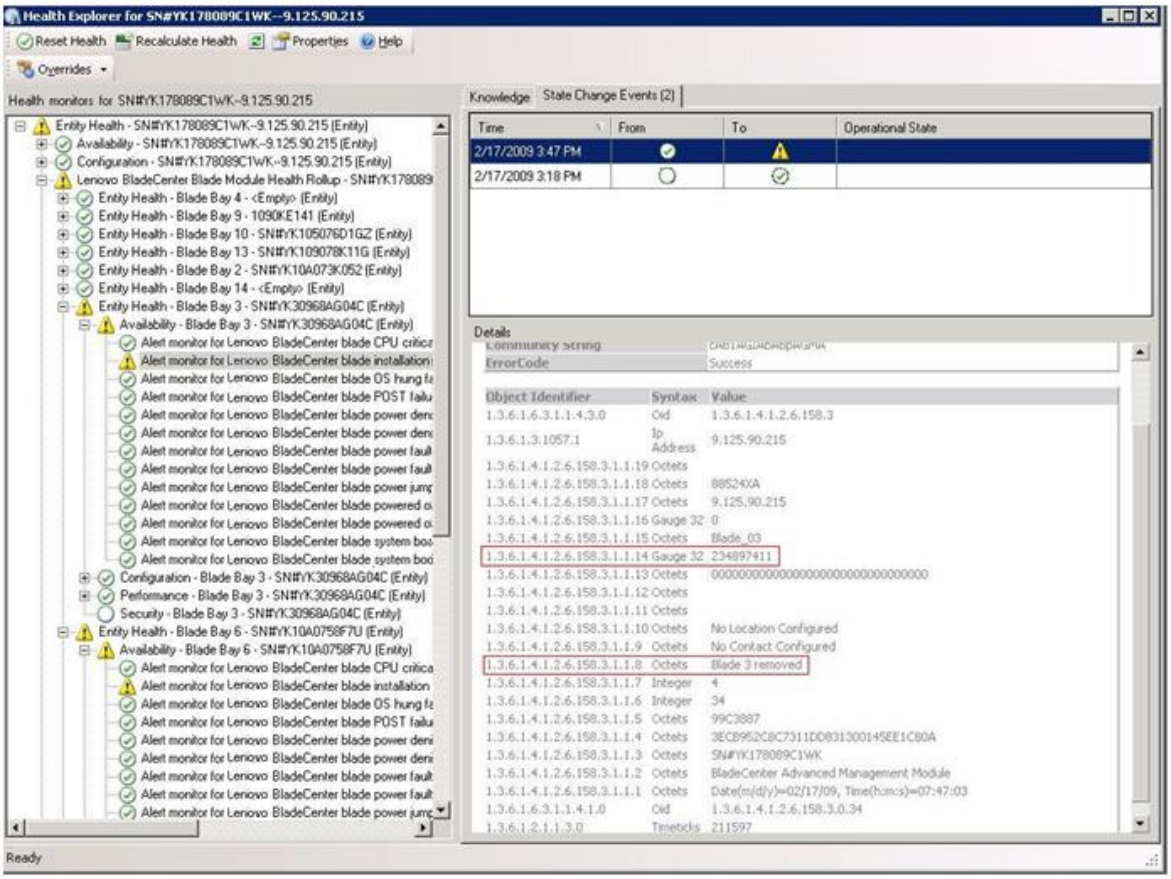

Figure 1. System x Windows Management Instrumentation (WMI) event

For a System x WMI event, the **Details** pane includes the event ID and a description.

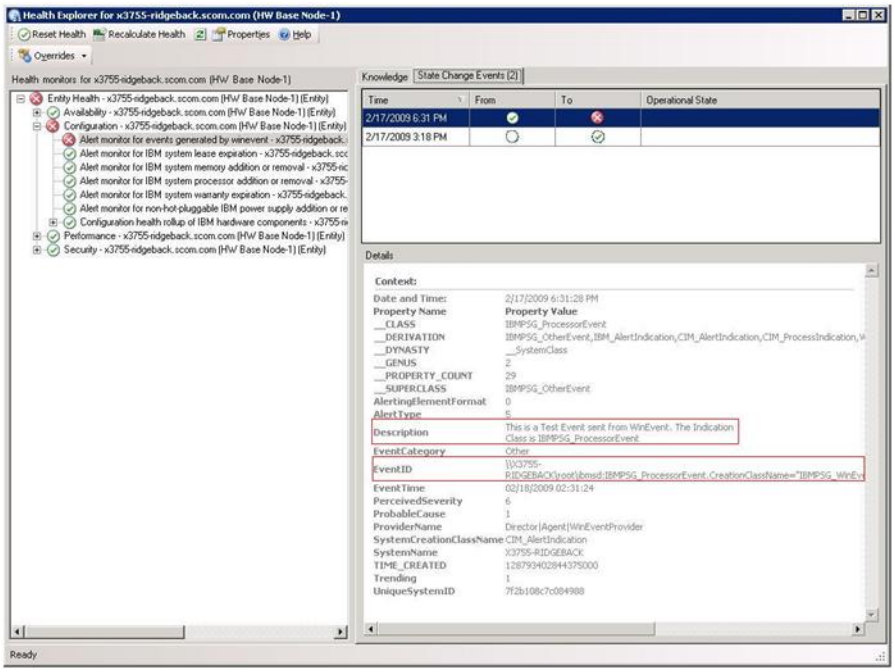

Figure 2. Example of the State Change Events tab detail information

Rediscovering all BladeCenters

The BladeCenter monitor stalls when the same version of Lenovo Hardware Management Pack is deleted and re-imported.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. Click **Administration → Device Management → Network Devices**.

Step 3. Note the IP addresses listed in the **Network Devices** view of the results pane. You will need this information for the discovery network device information later.

Step 4. Select the **IP Address** of the BladeCenter you want to rediscover, and in the **Actions** pane, select **Delete**.

Step 5. Use the noted IP address to limit the scope of Network Devices and rediscover the BladeCenter.

Rediscovering a renamed server

When a Windows server is renamed, the Windows server instance entry monitored by the Operations Manager becomes grayed out. This is an indication that the Windows server is no longer being monitored by the Operations Manager.

To rediscover and monitor a renamed server, first delete the original server name from the **Operations Manager Agent Managed server** list, and then rediscover the renamed server by using the following procedure.

Procedure

Step 1. Log in to the Operations Manager console.

Step 2. Click **Administration → Device Management → Agent Managed**.

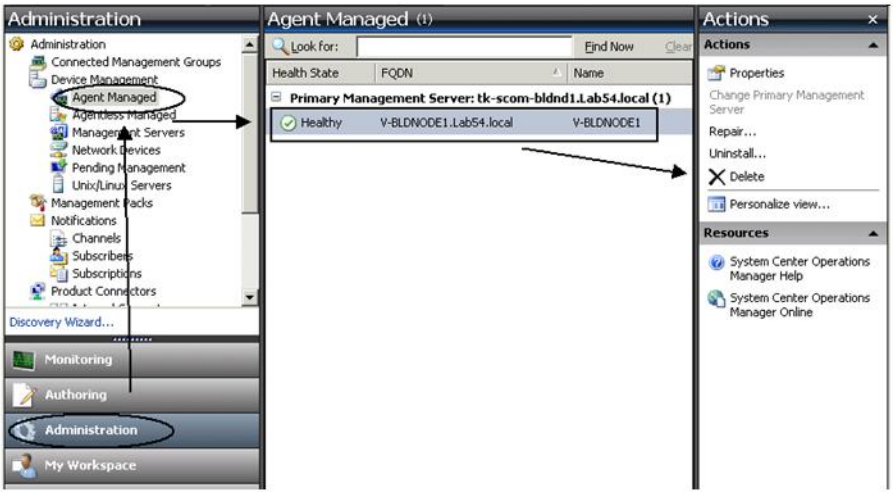

Figure 3. Deleting a renamed server

Step 3. Select the original name listed in the **Agent Managed** view of the results pane. This entry has the original name before it was renamed.

Step 4. Click **Delete** in the **Actions** pane located on the right side of the Operations Manager console. This action removes the renamed server from the view.

Step 5. Add the new server name.

Appendix C. System firewall settings

This section describes how to set firewall exceptions.

This table is a reference for determining the ports that are used for the specified Lenovo XClarity Integrator products.

Table 6. Ports used by **Lenovo XClarity Integrator** *products.*

Project	Source			Target			Protocol	Notes
	Port	Location	Component	Port	Location	Component		
SCVMM Add-in	not specified	management server	SCVMM Add-in console (localhost/ 127.0.0.1)	TCP 9500*	management server	Lenovo XClarity Integrator XClarity Integrator Service	HTTPS	You can change the target port when Lenovo XClarity Integrator is installed.
		managed server	Hyper-V/Windows clients managed with SCVMM					
	not specified	management server	Lenovo XClarity Integrator UXClarity Integrator Service (localhost/127.0.0.1)	TCP 9501*	management server	PostgreSQL	n/a	You can change the target port when Lenovo XClarity Integrator is installed.
	not specified	management server	Lenovo XClarity Integrator XClarity Integrator Service	TCP 5988	managed server	BMC	HTTP, CIM, SLP	You can change the BMC HTTP/HTTPS ports in BMC portal.
				TCP 5989			HTTPS, CIM, SLP	
	not specified	management server	Lenovo XClarity Integrator XClarity Integrator Service	TCP 80	external resource	IBM/Lenovo Web site	HTTP	You can download firmware from IBM/ Lenovo Web site through HTTP proxy.
				TCP 443			HTTPS	
	not specified	management server	Lenovo XClarity Integrator XClarity Integrator Service	TCP 443	external resource	Lenovo XClarity Administrator	HTTPS	The port depends on Lenovo XClarity Administrator configuration. You must input the correct port when registering theLenovo XClarity Administrator in Lenovo XClarity Integrator.
	not specified	management server	Lenovo XClarity Integrator XClarity Integrator Service	TCP 135	managed server	Host OS - WMI Server	CIM	n/a
	not specified	management server	Lenovo XClarity Integrator XClarity Integrator Service	UDP 137	managed server	Host OS - Samba Server	NetBIOS name service (NMBD)	n/a

Table 6. Ports used by Lenovo XClarity Integrator *products. (continued)*

Project	Source			Target			Protocol	Notes
	Port	Location	Component	Port	Location	Component		
				UDP 138			SMB	
				TCP 139				
				TCP 389			LDAP	
				TCP 445			NetBIOS	
				TCP 901			SWAT	
	not specified	managed server	Hyper-V/Windows clients managed with SCVMM	UDP 137	management server	OS - Samba Server	NetBIOS name service (NMBD)	n/a
				UDP 138			SMB	
				TCP 139				
				TCP 389			LDAP	
				TCP 445			NetBIOS	
				TCP 901			SWAT	
SCOM HWMP	not specified	management server	SCOM Hardware MP console (localhost/127.0.0.1)	TCP 9500*	management server	management server - (Lenovo XClarity Integrator) XClarity Integrator Service	HTTPS	You can change the target port when you install Lenovo XClarity Integrator.
	not specified	management server	Lenovo XClarity Integrator XClarity Integrator Service (localhost/127.0.0.1)	TCP 9501*	management server	PostgreSQL	n/a	The target port can be changed when Lenovo XClarity Integrator is installed.
	not specified	management server	Lenovo XClarity Integrator XClarity Integrator Service	TCP 5988	managed server	BMC	HTTP, CIM, SLP	The BMC HTTP/ HTTPS ports are changeable in BMC portal.
				TCP 5989			HTTPS, CIM, SLP	
	not specified	management server	SCOM Hardware MP	TCP 161	managed server	CMM or AMM	SNMP	The ports are changeable in CMM portal.
				TCP 162			SNMP Traps	

Table 6. Ports used by Lenovo XClarity Integrator *products. (continued)*

Project	Source			Target			Protocol	Notes
	Port	Location	Component	Port	Location	Component		
SCCM OSD	not specified	management server	SCCM OSD console	UDP 137	managed server	Preboot OS & Host OS - Samba Server	NetBIOS name service (NMBD)	n/a
				UDP 138			SMB	
				TCP 139				
				TCP 389			LDAP	
				TCP 445			NetBIOS	
				TCP 901			SWAT	
	not specified	managed server	PXE client	UDP 67	management server	DHCP Server	DHCP	n/a
				UDP 68				
				UDP 69		TFTP Server	TFTP	
SCCM Update	not specified	management server	SCCM Update Tool	TCP 80	external resource	WSUS Server	HTTP	n/a
				TCP 443			HTTPS	
				TCP 8530	external resource	WSUS Server (Windows Server 2012 and later version)	HTTP	n/a
				TCP 8531			HTTPS	
				UDP 137	managed server	Host OS - Samba Server	NetBIOS name service (NMBD)	n/a
				UDP 138			SMB	
				TCP 139				
				TCP 389			LDAP	
				TCP 445			NetBIOS	
				TCP 901			SWAT	

Table 6. Ports used by Lenovo XClarity Integrator *products. (continued)*

Project	Source			Target			Protocol	Notes
	Port	Location	Component	Port	Location	Component		
SCCM Inventory	not specified	management server	SCCM Inventory Tool	TCP 5988	managed server	BMC	HTTP, CIM, SLP	The BMC HTTP/ HTTPS ports are changeable in BMC portal.
				TCP 5989			HTTPS, CIM, SLP	
SCCM Configuration	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
*The ports marked with an asterisk are registered by Lenovo XClarity Integrator. The others are only used to access specific services in Lenovo XClarity Integrator.								

Appendix D. Notices

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

Lenovo might have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

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

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might 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 might make improvements or changes in the product(s) 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 might 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 might vary.

Lenovo might 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 might vary significantly. Some measurements might 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 might have been estimated through extrapolation. Actual results might vary. Users of this document shall verify the applicable data for their specific environment.

Trademarks

BladeCenter, Lenovo, the Lenovo logo, NeXtScale System, System x, ThinkServer, ThinkSystem, and XClarity are trademarks of Lenovo in the United States, other countries, or both.

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

IBM is the trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

Other company, product, or service names might 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.