



Lenovo XClarity Integrator for VMware vCenter Installation and User's Guide

Version 4.1



Lenovo XClarity Integrator for VMware vCenter Installation and User's Guide

Version 4.1

Note

Before using this information and the product it supports, there is some important prerequisite information to read.

This information can be found in “Notices” on page 81.

Edition notice

This edition applies to version 4.1 of Lenovo XClarity Integrator for VMware vCenter and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright Lenovo 2014, 2016.

Portions © Copyright IBM Corporation 2012, 2014.

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

© Lenovo 2014, 2016

Contents

Figures	v	Managing Rolling System Update tasks	18
Tables	vii	Working with the Rolling System Reboot function	24
About this publication	ix	Managing Rolling System Reboot tasks	25
Conventions and terminology	ix	Working with Predictive Failure Management	28
Information resources	xi	Setting a new policy	29
PDF files	xi	Viewing predictive failure alert events and the Action History table	30
World Wide Web resources	xi	Managing hardware events	31
Chapter 1. Lenovo XClarity Integrator for VMware vCenter	1	Alarms	32
Dashboard	1	Chapter 5. Managing servers	33
Dynamic System Analysis	1	System function	33
Firmware Updates	1	Chassis Map function	34
Power Metric	1	System Overview	34
Advanced Settings Utility	2	Launching the System Diagnostic Collection function	34
Predictive failure management	2	Viewing the categorized analysis results for vSphere Web Client.	35
Chapter 2. Installing Lenovo XClarity Integrator for VMware vCenter	3	Working with Alerts and Events	35
System requirements for Lenovo XClarity Integrator for VMware vCenter.	3	Working with Firmware Updates	36
Supported versions of VMware vCenter Server ..	3	Prerequisites for updating firmware	36
Supported operating systems	3	Selecting an update preference	36
Supported ESXi version.	3	Firmware Updates scenarios.	37
Supported hardware.	4	Working with Power and Cooling	40
Hardware requirements.	6	Power Metric page	40
Port requirements.	6	Set Power Capping on vSphere Web Client.	41
Installing Lenovo XClarity Integrator for VMware vCenter	7	Set Power Throttling on vSphere Web Client ..	41
Installing the Lenovo License Tool and activating the premium features.	9	Viewing the Power Usage History, Thermal Usage History, and Fan Usage History for vSphere Web Client.	42
Configuring Lenovo XClarity Integrator	9	Working with configuration	44
Configuring access control.	9	Deploying a configuration pattern on a server ..	44
Configuring Lenovo XClarity Administrator	9	Viewing advanced system settings.	45
Chapter 3. Lenovo XClarity Integrator for VMware vCenter with vSphere Web Client	11	Changing advanced system settings	47
Chapter 4. Managing clusters	13	Chapter 6. Managing Lenovo infrastructure	51
Working with the Cluster Overview function	13	Working with the Lenovo Infrastructure view	51
Requesting host access.	14	Working with the Chassis Map function.	53
Requesting IMM access using the Cluster Overview function	15	Viewing the details of a managed chassis	56
Working with the IMM Discovery function.	15	Launching an Integrated Management Module Interface	56
Requesting IMM access using the IMM Discovery function	16	Launching Remote Control	57
Working with the Rolling System Update function	16	Working with configuration patterns	57
Configuring the Rolling System Update preferences	17	Working with firmware compliance	58
		Assigning compliance policies	58
		Applying and activating firmware updates	59
		Identifying endpoints that are not compliant ..	61
		Chapter 7. Using Lenovo XClarity Integrator for VMware vCenter with vSphere Client	63
		The Dashboard	63
		System Information Summary	63

System Health, Power Throttling, and Predictive Failure Alert summaries	63
Working with Dynamic System Analysis.	64
Firmware updates	65
Prerequisites	65
Firmware update scenarios	65
Working with Power Metric	69
Viewing power usage, thermal history, and fan summary information	70
Power Capping	72
Power Throttling	72
Working with Advanced System Settings	73
Viewing Advanced System Settings	73
Changing Advanced System Settings	74
Appendix A. Troubleshooting	77
Help information	77

Finding the vCenter plug-in version	77
Installed version field shows Undetected in firmware updates	77
IMM Discovery failure.	77
Cannot display a chassis map or a configuration pattern page because of a certificate issue	77

Appendix B. Accessibility features. 79

Notices	81
Trademarks	82
Important notes	82

Index 83

Figures

1. VMware vCenter server configuration	8	26. Viewing IMM Alerts	48
2. Lenovo XClarity Integrator Administration window.	10	27. Setting change success symbol	48
3. Cluster Overview	14	28. Setting change not success symbol	48
4. Requesting IMM access on the IMM Discovery page	16	29. LXCA domains Actions list	51
5. Task Manager page	19	30. Managed Chassis and Racks table	52
6. Select hosts and firmware page	20	31. Chassis view	52
7. Select options and schedules page	21	32. Chassis view	53
8. Summary page	22	33. LXCA Configuration Pattern dialog box	57
9. Set Policy	29	34. Workflow for updating firmware on managed endpoints	58
10. Viewing Predictive Failures	31	35. System Health Summary Dashboard view	64
11. System Overview page.	34	36. Updates page	66
12. Viewing Alerts and Events	35	37. Update Recommendation example	67
13. Update Preferences page	37	38. Acquire Updates	67
14. Recommended Updates wizard - Check Compliance dialog box.	38	39. Update Authentication page	68
15. Check Compliance complete	39	40. Update execution page.	68
16. Recommended Updates wizard - updating firmware	39	41. All updates successfully applied	69
17. Power Metric page	41	42. Enabling Power Metric.	70
18. Setting Power Capping on vSphere Web Client	41	43. Power Usage Chart	71
19. Setting Power Throttling on vSphere Web Client	42	44. Thermal History chart	71
20. Power Usage History for vSphere Web Client	43	45. Fan History chart	72
21. Thermal Usage History for vSphere Web Client	43	46. Set Power Capping	72
22. Fan Usage History for vSphere Web Client	44	47. Set Power Throttling	73
23. Deploy Pattern	45	48. Power Throttling Indications.	73
24. Viewing IMM Port Assignments	46	49. Viewing Advanced System Settings	74
25. Viewing Boot Order.	47	50. Setting not supported symbol	74
		51. Setting change is successful symbol	75
		52. Setting change is not successful symbol	75
		53. Changing Advanced System Settings	75

Tables

1. Frequently used terms and acronyms	ix	7. Rolling System Update task status	24
2. Supported Lenovo hardware	4	8. Rolling System Reboot task functions	25
3. Supported IBM hardware	4	9. Rolling System Reboot task status	28
4. Hardware requirements	6	10. Predictive Failure Alert Event categories	30
5. Port requirements	6	11. Hardware map overlays	54
6. Rolling System Update task functions	19		

About this publication

This book provides instructions for installing and using Lenovo XClarity Integrator for VMware vCenter v4.1.

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

Conventions and terminology

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

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

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

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

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

Table 1. Frequently used terms and acronyms

Term/Acronym	Definition
ASU	Lenovo Advanced Settings Utility
DSA	Lenovo Dynamic System Analysis
IMM	Integrated Management Module
LXCA	Lenovo XClarity Administrator
LXCI	Lenovo XClarity Integrator
PFA	predictive failure alert
UXSP	UpdateXpress System Packs
UXSPi	UpdateXpress System Pack Installer

Information resources

You can find additional information about Lenovo XClarity Integrator for VMware vCenter, Version 4.1 in the product documentation and on the World Wide Web.

PDF files

You can view or print documentation that is available in Portable Document Format (PDF).

Downloading Adobe Acrobat Reader

You need Adobe Acrobat Reader to view or print PDF files. You can download a copy from the Adobe website.

Viewing and printing PDF files

You can view or print PDF files that can be found on the web pages listed in “World Wide Web resources.”

Saving PDF files

To save a PDF file, complete the following steps:

1. Right-click the link to the PDF in your browser.
2. Perform one of the following tasks.

Web browser	Command
For Internet Explorer	Click Save Target As .
For Netscape Navigator or Mozilla	Click Save Link As .

3. Navigate to the directory into which you want to save the PDF file.
4. Click **Save**.

World Wide Web resources

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

Lenovo XClarity Integrator for VMware vCenter site

Locate the latest downloads for the Lenovo XClarity Integrator for VMware vCenter:

Lenovo XClarity Integrator for VMware vCenter site

Technical support portal

This website can assist you in locating support for hardware and software:

Lenovo Systems Technical Support

System Management with Lenovo XClarity Solution

This website provides an overview of the Lenovo XClarity solution which integrates System x M5 and M6, as well as Flex System to provide system management capability:

System Management with Lenovo XClarity Solution site

ServerProven websites

The following websites provide an overview of hardware compatibility for BladeCenter, Flex System[™], System x and xSeries[®] hardware:

- Lenovo ServerProven: Compatibility for BladeCenter products
- Lenovo ServerProven: Compatability for Flex System Chassis
- Lenovo ServerProven: Compatability for System x hardware, applications, and middleware

VMware vCenter Product Family site

This website can assist you in locating VMware products:

VMware vCenter Products

Chapter 1. Lenovo XClarity Integrator for VMware vCenter

The topics in this section provide information about Lenovo XClarity Integrator for VMware vCenter.

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

- Dashboard
- Dynamic System Analysis
- Firmware Updates
- Power Metric
- Advanced System Settings
- Predictive Failure Management

Dashboard

The Dashboard provides an overview of a selected host or cluster and displays summary information including overall resource utilization, host health messages and connection status. The Dashboard also displays IMM information for each host and allows you to launch the IMM console directly.

Dynamic System Analysis

Dynamic System Analysis is a tool that collects and analyzes system information to aid in diagnosing system problems.

Firmware Updates

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

Power Metric

To aid in balancing workloads on hosts, the Power Metric feature monitors power usage, thermal, and fan speed values of the ESXi host and graphically displays this information.

Power Metric provides Power Capping and Power Throttling features. Power Capping allows you to allocate less power and cooling to a system. Power Throttling allows you to receive an alert after power consumption exceeds the set values.

Advanced Settings Utility

Advanced Settings Utility provides a management interface for viewing and configuring frequently changed system settings on a managed endpoint, such as IMM, uEFI, and boot order. To change unsupported settings in Lenovo XClarity Integrator for VMware vCenter, use the IMM and uEFI interfaces.

Predictive failure management

The Predictive Failure Management feature monitors server hardware status and automatically evacuates virtual machines in response to predictive failure alerts to protect your workloads.

Predictive Failure Analysis refers to computer mechanisms that analyze trends in corrected errors to predict future failures of hardware components and proactively enable mechanisms to avoid them.

Chapter 2. Installing Lenovo XClarity Integrator for VMware vCenter

The topics in this section provide information about installing Lenovo XClarity Integrator for VMware vCenter.

System requirements for Lenovo XClarity Integrator for VMware vCenter

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

Supported versions of VMware vCenter Server

The Lenovo XClarity Integrator for VMware vCenter plug-in is an extension to VMware vCenter Server.

The Lenovo XClarity Integrator for VMware vCenter plug-in supports the following versions of VMware vCenter Server:

- 6.0
- 5.5
- 5.1
- 5.0
- 4.1

Note: Only 5.1 and later versions of the VMware vCenter Server Appliance are supported.

Supported operating systems

Lenovo XClarity Integrator for VMware vCenter can be installed on the following operating systems.

- Microsoft Windows Server 2008 (x64)
- Microsoft Windows Server 2008 R2 (x64)
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Note:

- Microsoft .NET Framework Version 2.0 or later is required. You can launch the Add Features wizard of the Windows Server Manager to install .NET.
- If you install LXCI on a separate Windows operating system without VMware vCenter, Java 8 (64-bit) is required.

Supported ESXi version

Lenovo XClarity Integrator for VMware vCenter supports the following Lenovo customized ESXi images:

- 6.0
- 5.5
- 5.1

- 5.0
- 4.1

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

For generic VMware ESXi, you need to download and install IBM Customization for ESXi offline bundles on Fix Central to enable all management functions. Without the offline bundles being installed, Lenovo XClarity Integrator for VMware vCenter provides limited management functionality. It is recommended that you update to the latest patch version on each managed ESXi host at your earliest convenience. You can find VMware vCenter ESXi with Lenovo Customization offline bundles and patches at Fix Central.

Supported hardware

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

The XClarity Integrator plug-in has no hardware limitations. However, the hardware that the plug-in manages is limited to the Lenovo and IBM hardware listed in the following tables.

Table 2. Supported Lenovo hardware

System	Server number
System x server	NeXtScale nx360 M5 (5465)
	NeXtScale nx360 M5 DWC (5467, 5468, 5469)
	x3500 M5 (5464)
	x3550 M4 (7914)
	x3550 M5 (5463)
	x3630 M4 (7158)
	x3650 M4 (7915)
	x3650 M5 (5462)
	x3750 M4 (8753)
	x3850 X6 / x3950 X6 (6241)
Flex Compute Node	Flex System x240 Compute Node (7162, 2588)
	Flex System x240 M5 Compute Node (2591, 9532)
	Flex System x280, x480, x880 X6 Compute Node (7196, 4258)
	Flex System x440 Compute Node (7167, 2590)

Table 3. Supported IBM hardware

System	Server number
System x server	dx360 M2 (7321, 7323)
	dx360 M3 (6391)
	dx360 M4 (7912, 7913, 7918, 7919)
	nx360 M4 (5455)

Table 3. Supported IBM hardware (continued)

System	Server number
	Smart Analytics System (7949)
	x3100 M4 (2582, 2586)
	x3100 M5 (5457)
	x3200 M2 (4367, 4368)
	x3200 M3 (7327, 7328)
	x3250 M2 (7657, 4190, 4191, 4194)
	x3250 M3 (4251,4252,4261)
	x3250 M4 (2583) *
	x3250 M5 (5458)
	x3300 M4 (7382)
	x3400 M2 (7836, 7837)
	x3400 M3 (7378, 7379)
	x3500 M2 (7839)
	x3500 M3 (7380)
	x3500 M4 (7383)
	x3530 M4 (7160)
	x3550 M2 (7946, 4198)
	x3550 M3 (7944, 4254)
	x3550 M4 (7914)
	x3620 M3 (7376)
	x3630 M3 (7377)
	x3630 M4 (7158, 7518, 7519)
	x3650 M2 (7947, 4199)
	x3650 M3 (7944, 7945, 4254, 4255, 5454)
	x3650 M4 (7915)
	x3650 M4 HD (5460)
	x3650 M4 BD (5466)
	x3750 M4 (8722, 8733)
	x3755 M4 (7164)
	x3690 X5 (7148, 7149, 7147, 7192)
	x3850 X5/X3950 X5 (7145, 7146, 7143, 7191)
	x3850 X6/x3950 X6 (3837, 3839)
Flex Compute Node	Flex System x220 Compute Node (7906, 2585)
	Flex System x222 Compute Node (7916)
	Flex System x240 Compute Node (8737, 8738, 7863)
	Flex System x280 X6 Compute Node / x480 X6 Compute Node / x880 Compute Node X6 (4259, 7903)
	Flex System x440 Compute Node (7917)
Blade server	HS22 (7870, 7809, 1911, 1936)
	HS22V (7871, 1949)

Table 3. Supported IBM hardware (continued)

System	Server number
	HS23 (7875, 1882, 1929)
	HS23E (8038, 8039)
	HX5 (7872, 7873, 1909, 1910)

* Note the following:

- x3250 M4 2583 supports only partial functions in the Dashboard and Lenovo Dynamic System Analysis. Update, power, and system configuration functions are not supported.
- The power and cooling function and the remote control function support only IMM2 systems.
- The predictive failure alert (PFA) function supports only systems that provide out-of-band IMM access.

Hardware requirements

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

Table 4. Hardware requirements

Component	Minimum	Recommended
Memory	4 GB RAM	8 GB RAM
Disk space	20 GB of free hard disk space	40 GB of free hard disk space
Processor	1 processor	2 processors

Port requirements

The following table lists ports used by Lenovo XClarity Integrator for VMware vCenter.

Table 5. Port requirements

Port	Default port	Notes
LXCI Unified Service port	https 9500	Can be changed when you install LXCI
LXCI database port	TCP 9501	Can be changed when you install LXCI
ESXi CIMOM port	https 5989	Communicates with remote ESXi via the port
IMM port	https 5989 http 5988 UDP 427	Communicates with IMM via the port
Firmware download	http 80 https 443	Download firmware from Lenovo site via the port
LXCA	https 443	Communicates with LXCA via the port

Installing Lenovo XClarity Integrator for VMware vCenter

Lenovo XClarity Integrator for VMware vCenter must be installed on a standalone physical server set up exclusively for Lenovo XClarity Integrator for VMware vCenter, a virtual machine, or the same server as VMware vCenter Server. Note that for VMware vCenter Virtual Appliance, Lenovo XClarity Integrator for VMware vCenter must be installed outside the vCenter server.

Before you begin

Administrator privileges are required to install Lenovo XClarity Integrator for VMware vCenter.

About this task

Lenovo XClarity Integrator for VMware vCenter can be accessed with either vSphere Client or vSphere Web Client, depending on the VMware vCenter version.

- For VMware vCenter 5.0 and the previous version, you can only access the plug-in with vSphere Client. For more information, see Chapter 7, “Using Lenovo XClarity Integrator for VMware vCenter with vSphere Client,” on page 63.
- For VMware vCenter 5.1 and later versions, you can only access the plug-in with vSphere Web client. For more information, see Chapter 3, “Lenovo XClarity Integrator for VMware vCenter with vSphere Web Client,” on page 11.

Procedure

1. Download and extract the Lenovo XClarity Integrator for VMware vCenter installation package files.
2. Double-click **lnvgy_sw_vmuim_x.x_windows_64.exe** to launch the installer. Where *x.x* represents the version of the Lenovo XClarity Integrator for VMware vCenter package you are installing.
3. Click **Next** on the startup page of the installer.
4. Read and agree to the Lenovo XClarity Integrator for VMware vCenter license.
5. Select the destination folder for installing Lenovo XClarity Integrator for VMware vCenter, then click **Next**.
6. Input your **user** and **company** information.
7. Click **Confirm** to install. The installation process begins.

During the installation process, Lenovo XClarity Integrator Unified Service is launched and installed. For more information, refer to the *Lenovo XClarity Integrator Unified Service User's Guide*.

After the installation is complete, the configuration starts.
8. Enter the VMware vCenter server information and connection information for the product.

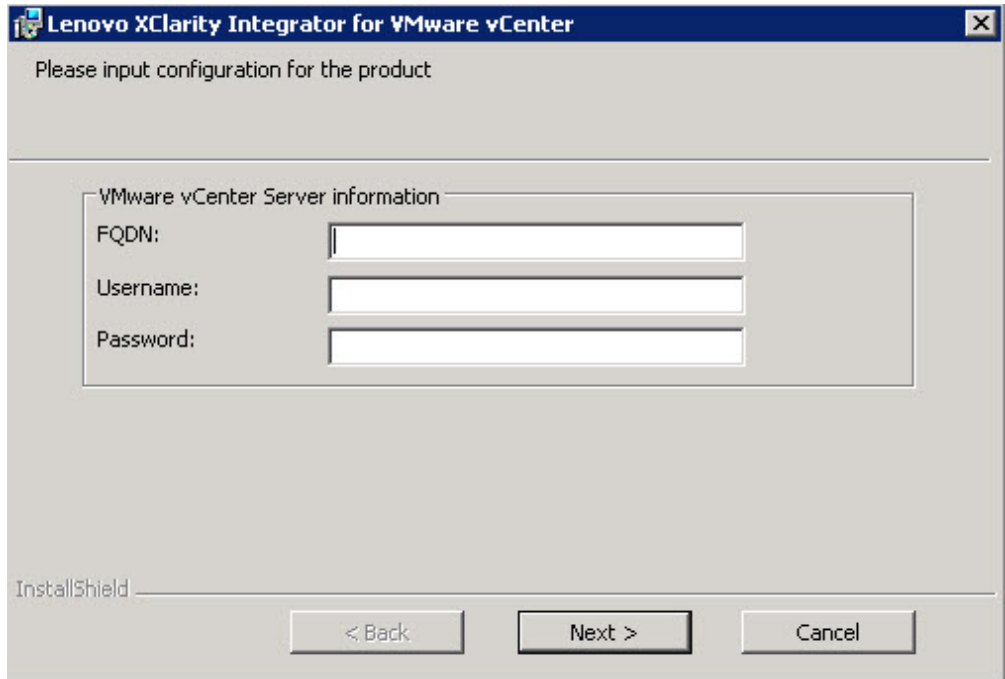


Figure 1. VMware vCenter server configuration

- In the **FQDN** field, enter the FQDN or IP address of the management network (used to connect to the vCenter Server).
 - In the **Username** and **Password** fields, provide a user name and password that has administrative credentials to manage the vCenter Server.
9. Click **Next** to start the configuration.
 10. Click **Finish**. Lenovo XClarity Integrator for VMware vCenter is successfully installed.

Notes:

- a. For VMware vCenters in a Linked Mode group, you can only install Lenovo XClarity Integrator for VMware vCenter on one of the vCenters, and manage hosts in that vCenter only. If there are additional vCenters in the Linked Mode group, they are not supported.
- b. When you launch the installation package, if an earlier version of Lenovo XClarity Integrator for VMware vCenter is detected, an upgrade dialog box is displayed. Click **Upgrade** to upgrade the product. The installer will remove the old version and install the new version. After the product has been successfully upgraded, it is recommended that you remove the directory with the prefix "com.ibm.ivp-" listed under C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity or /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity on the host where vSphere Web Client is installed, and restart the vSphere Web Client service to force plug-in redeployment.

Note: The directory name might vary depending on the vCenter version.

- c. If you want to fully uninstall the product from the control panel, you must remove Lenovo XClarity Integrator for VMware vCenter first, then remove Lenovo XClarity Integrator Unified Service. If you choose to uninstall the product with the installer, both of items are automatically removed.

Installing the Lenovo License Tool and activating the premium features

Lenovo XClarity Integrator for VMware vCenter provides a 90-day trial license by default. When the license expires after 90 days, all of the premium features are disabled. It is suggested that you install the Lenovo XClarity Integrator for VMware vCenter License Tool to activate the product license. Activation licenses can be purchased by contacting either your Lenovo representative or a Lenovo Business Partner.

After you purchase the Lenovo XClarity Integrator for VMware vCenter product license, you are only required to activate the license on the vCenter Server that is running Lenovo XClarity Integrator for VMware vCenter. It is not necessary to activate the license on each managed ESXi host. The license token is automatically delivered to the ESXi host when it is managed by vCenter Server. For more information about activating the premium features, refer to the *Lenovo XClarity Integrator for VMware vCenter License Installer Guide*.

Configuring Lenovo XClarity Integrator

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

Configuring access control

Lenovo XClarity Integrator is fully accessible by the Administrator role automatically.

Lenovo XClarity Integrator is controlled by two privileges:

LenovoXClarityIntegrator.AccessLenovoESXiHost

This privilege allows access to all of the features listed under the Lenovo XClarity Integrator tabs, beneath the Manage tab for the DataCenter, Cluster, and Host items. These features include: monitoring, inventory, firmware updates, system configuration, and predictive failure management.

This privilege allows you to use Lenovo XClarity Integrator Administration for registering, editing, and unregistering a Lenovo XClarity Administrator.

LenovoXClarityIntegrator.AccessLenovoInfrastructure

This privilege allows access to all of the features of the vCenter Lenovo Infrastructure, where you can view all of the infrastructures for the Lenovo XClarity Administrator domains.

The System Administrator should assign one or all privileges to a role as appropriate for working with Lenovo XClarity Integrator for VMware vCenter with vSphere Web Client.

Configuring Lenovo XClarity Administrator

Lenovo XClarity Integrator provides an integrated method for managing your servers with Lenovo XClarity Administrator using vSphere Web Client. Use the register function to integrate Lenovo XClarity Administrator with vSphere Web Client. Once registered, you can manage servers in vSphere Web Client using the Lenovo XClarity Administrator features.

Before you begin

Before you can work with Lenovo XClarity Administrator, ensure the following:

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

About this task

This task is performed on the **vSphere Web Client Home** page.

Procedure

1. Click **Administration**. The Lenovo XClarity Integrator Administration page is displayed.

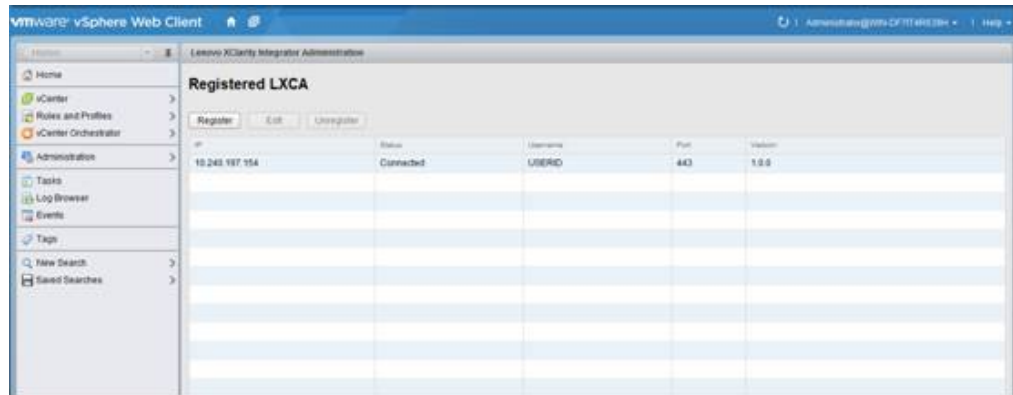


Figure 2. Lenovo XClarity Integrator Administration window

2. Click **Register** and enter the information required by the Lenovo XClarity Administrator function.
3. Click **OK** and wait for the registration to complete.

What to do next

After completing the registration, you can perform these actions:

- Edit Lenovo XClarity Administrator by clicking **Edit** and making any necessary changes.
- Unregister Lenovo XClarity Administrator by clicking **Unregister**.

Chapter 3. Lenovo XClarity Integrator for VMware vCenter with vSphere Web Client

You can use the Lenovo XClarity Integrator for VMware vCenter software with vSphere Web Client. Lenovo XClarity Integrator is a platform management tool integrated into vCenter and provides a single, heterogeneous view of all host systems within your managed environment.

After installation, the Lenovo XClarity Integrator tabs are available in vSphere Web Client providing both host and cluster level management functionality that includes:

- Monitoring
- Inventory
- Firmware updates
- System configuration
- Predictive failure management

Chapter 4. Managing clusters

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

About this task

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

Procedure

1. Select a cluster from the inventory tree.
2. Click the **Manage** tab.
3. Click the **Lenovo XClarity Integrator** tab. The following cluster management functions are available:
 - Cluster Overview
 - IMM Discovery
 - Rolling System Update
 - Rolling Reboot
 - Predictive Failure

Working with the Cluster Overview function

The Cluster Overview function collects and analyzes cluster inventory information and health status to assist with the operation and management of hosts and clusters.

The Cluster Health section provides a snapshot view of the following aspects of a system:

- The total number of hosts, which includes:
 - IBM hosts
 - Lenovo hosts
 - Other hosts
- The overall health status of a host and any current alerts.
- A summary of usage information indicating the space used for the cluster disk, memory, and CPU.

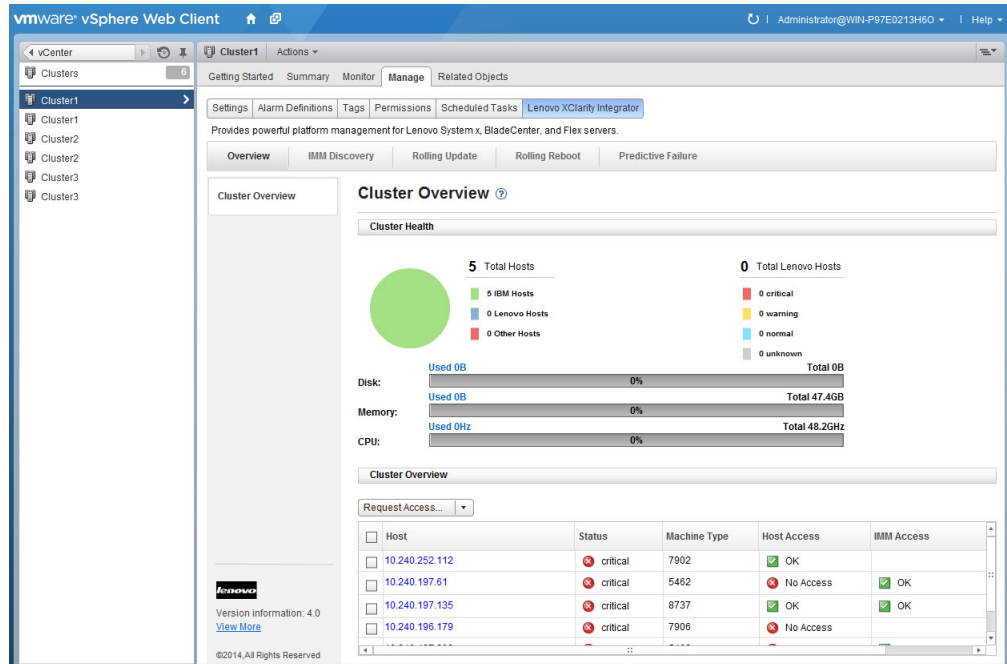


Figure 3. Cluster Overview

The Cluster Overview section provides the following host information:

- Host IP address
- Status
- Machine Type
- Host Access
- IMM Access

The **Request Access** list has the following options:

- Request host access
- Request IMM access

Requesting host access

This topic explains how to request host access.

Before you begin

Add hosts to a cluster in vSphere Web Client.

About this task

This task is performed on the Cluster Overview page.

Procedure

1. Click **Lenovo XClarity Integrator > Overview**.
2. In the Cluster Overview section, select the hosts for which you want to request host access.
3. From the **Request Access** list, select **Request Host Access**.
4. In the Request Host Access dialog box, enter the following information for the host(s) you selected, then click **OK**.

- User Name
- Password

If any of the hosts selected have the same account information, they are also enabled.

Requesting IMM access using the Cluster Overview function

This topic explains how to request IMM access from the Cluster Overview page.

Before you begin

To request IMM access, the selected hosts must have been previously discovered using the IMM Discovery page. For more information, see “Working with the IMM Discovery function.”

About this task

This task is performed on the Cluster Overview page.

Procedure

1. Click **Lenovo XClarity Integrator > Overview**.
2. In the Cluster Overview section, select the hosts for which you want to request IMM access.
3. From the **Request Access** list, select **Request IMM Access**. In the Request IMM Access dialog box, enter the following information for the IMM you selected, then click **OK**.
 - User Name
 - Password
4. Select the IP address link to launch the IMM web console.
 - User Name
 - Password

Results

The IMM web console is displayed.

Working with the IMM Discovery function

The IMM Discovery function provides out-of-band (OOB) management for your servers using IMM2 or IMM on vSphere Web Client. This functionality can assist you with managing your host and lower the risk cluster hardware problems by monitoring hardware events using IMM or setting predictive failure policies. The IMM Discovery function discovers the IMM for your host in the cluster.

About this task

This task is performed on the IMM Discovery page.

Procedure

1. Click **Lenovo XClarity Integrator > IMM Discovery**.
2. From the **select a discovery option** dual-list, select a discovery option.
3. Enter a range of IP addresses or a single IP address.

4. Click **Add** to add the discovery items to the Discovery Item dual-list. If there are any discovery items added, that you do not want to discover, you can select **Delete** to remove them from the Discovery Item list.
5. After adding all of the discovery items, click **Discover Now** to start the discovery process.

Note: You cannot stop the discovery operation after it has started.
When the discovery operation has finished, the discovered IMM is listed in the Discovered IMM table.

Requesting IMM access using the IMM Discovery function

This topic explains how to request IMM access from the IMM Discovery page.

About this task

This task is performed on **Lenovo XClarity Integrator > IMM Discovery** page.

Procedure

1. From the Discovery IMM table, select one or multiple IMM IP addresses that will use the same credentials for IMM access.

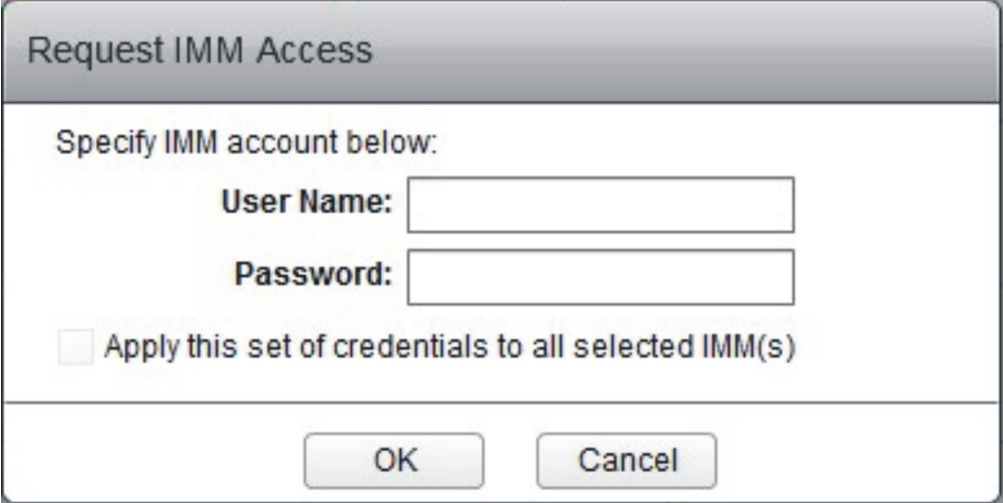
A screenshot of a 'Request IMM Access' dialog box. The title bar is grey with the text 'Request IMM Access'. The main area is white and contains the text 'Specify IMM account below:'. Below this text are two input fields: 'User Name:' followed by a text box, and 'Password:' followed by a text box. Below the password field is a checkbox with the label 'Apply this set of credentials to all selected IMM(s)'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Figure 4. Requesting IMM access on the IMM Discovery page

2. In the Request IMM Access dialog box, enter the IMM credentials and then click **OK**. If the user name and password are valid, the IMM Access displays a status of OK.

If any IMM fails the authentication process, the following warning message is displayed: One or more IMM fails the authentication with the given user name and password; close this window to see the result.

Working with the Rolling System Update function

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

any workload interruption. The RSU function updates firmware in a single batch while the system continues running without interruption to application services on a server host.

Before you begin

The following prerequisites are necessary for using the Rolling System Update function:

Lenovo customized ESXi image, version 5.0 and later:

For more information, see “Supported ESXi version” on page 3.

VMware vCenter Enterprise or Enterprise Plus Edition with DRS:

DRS is enabled and running in fully automated mode.

Host access has been granted:

For more information, see the “Working with the Cluster Overview function” on page 13.

Configuring the Rolling System Update preferences

The Preferences page allows you to configure the update repository for the Rolling System Update function.

Specify the update repository location

Select the update repository location where the Rolling System Update function should look for updates.

Procedure

1. Click **Lenovo XClarity Integrator > Rolling System Update**.
2. In the navigation pane, click **Preferences**.
3. On the Preferences page, specify the update location by selecting one of the following options:

Check the Lenovo website:

Download the appropriate updates automatically from the Lenovo website during the rolling update.

You can configure a proxy if the vCenter Server cannot access the website directly, but completing these steps:

- a. Select **Check the Lenovo website** and click **Require a proxy server for Internet connection**.
- b. Enter proxy configuration and click **Save**. please provide specifics for the proxy configuration.

Look in a directory on vCenter Server:

For vCenter, locate updates in a local directory: InstallFolder\webroot\bin\data\repository.

The directory cannot be changed for Rolling System Update.

Checking for updates automatically

If you selected the **Check the Lenovo website** option, you can have XClarity Integrator automatically download the latest firmware for all managed servers from the Lenovo website.

Procedure

1. Click **Check available updates periodically**.

2. Configure the check cycle based on how frequently you want to check and download updates.
3. Click **Save**.

Checking for updates manually

Complete the following steps to manually check for updates.

Procedure

1. Click **Check Now**. A dialog box opens.
2. In the dialog box, click **OK** to begin checking for updates. The results are listed on the vCenter event monitor.
3. In the left pane of the vSphere Web Client, click **vCenter node**, select **monitor**, and then **Events**. When the checking operation has finished, the checking updates results indicate an update event.

What to do next

It is recommended that you download the latest updates on a regular basis.

Managing Rolling System Update tasks

The Rolling System Update (RSU) Task Manager can assist you with creating and managing rolling update tasks. An RSU task contains all of the information and options required for a rolling update.

Procedure

1. Click **Lenovo XClarity Integrator > Rolling System Update**.
2. In the navigation pane, click **Task Manager**. The Task Manager page is displayed.

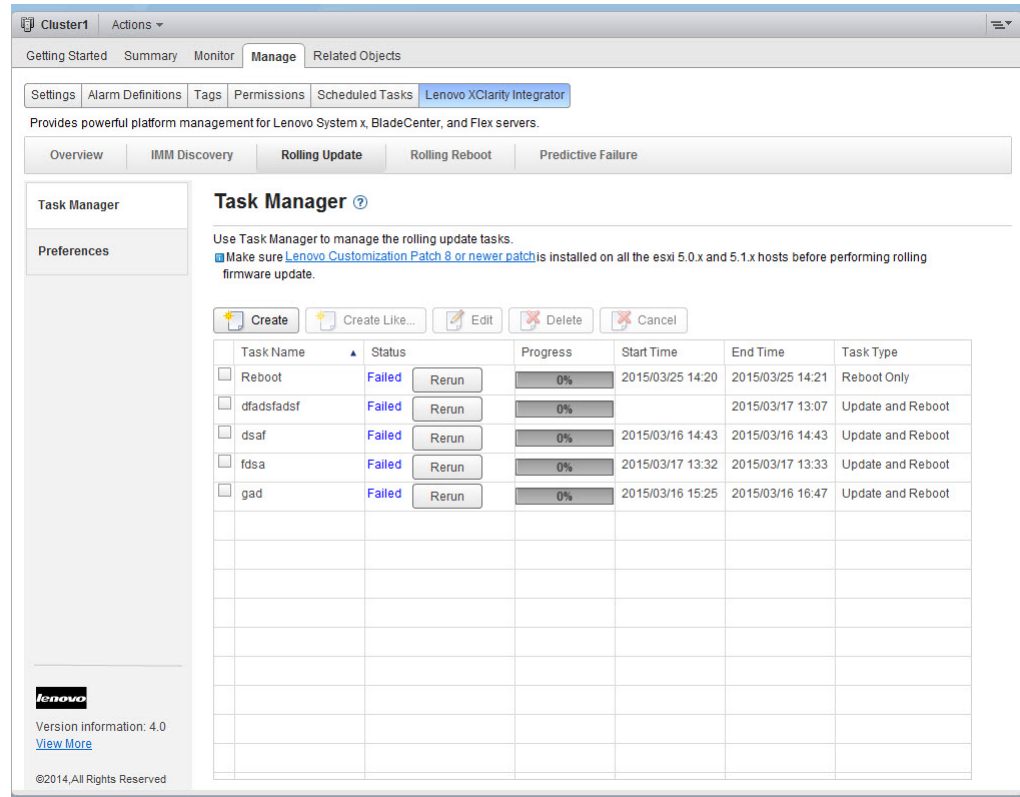


Figure 5. Task Manager page

The Task Manager table provides the following detailed information about RSU tasks:

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

3. Use the Task Manager to perform these task functions:

Table 6. Rolling System Update task functions

Task function	Description
Create	Create a new RSU task.
Create Like	Create a new RSU task from an existing RSU task.
Edit	Edit an RSU task that has not been started.
Delete	Remove an RSU task from the task list.
Cancel	Stop a running RSU task.
Rerun	Rerun a failed RSU task.

Creating a task

Use the **Create** option to create a new Rolling System Update (RSU) task. Each cluster can have only one active RSU task if the task type is *Update Only* or *Update and Reboot*.

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Update > Task Manager** page.

Procedure

1. Click **Create** to open the Rolling System Update wizard. The **Create** button is enabled only if a task has a status of *Finished*, *Canceled*, or *Failed* in the task list. The Name and Type page is displayed.
2. Enter a name for the task you are creating in the **Task Name** field.
3. Select a **Task Type**:

Update and Reboot:

The server is placed in maintenance mode for updating, and the hosts are rebooted after the update has successfully completed.

Update Only:

The server is placed in maintenance mode for updating, and the hosts are not rebooted following update completion.

4. Click **Next**. The Select hosts and firmware page is displayed.

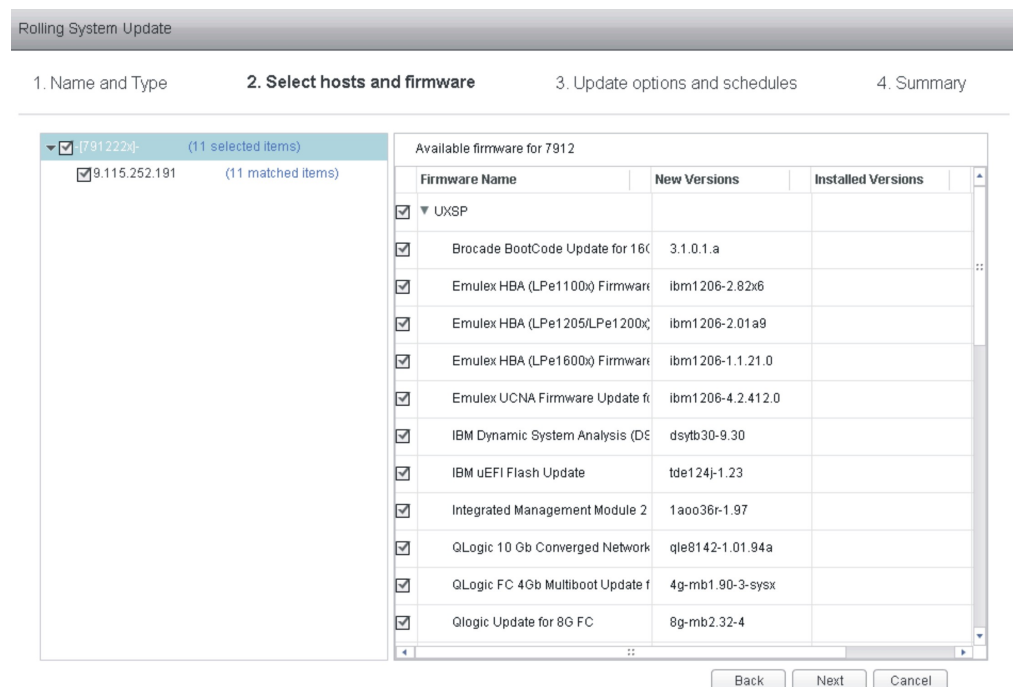


Figure 6. Select hosts and firmware page

All of the hosts in the current cluster display on the left and are organized by machine type. The available and installed firmware versions for each machine type and host are listed on the right.

5. Select a host to view the available firmware from the right and choose the updates you want to apply.

If a machine type is selected, the selection of firmware is applied to all of the hosts that have this machine type. If a host check box is not selectable, there are no available updates in the repository.

If inventory information has not been collected for a host, RSU displays the firmware for the machine type of this host. In this case, you can still select

firmware for this host to update. RSU will try to collect host inventory information when updating and install the selected firmware. If the selected firmware is not available for the host, the update is skipped.

6. Click **Next**. The update options and schedules screen is displayed.

Rolling System Update

1. Name and Type 2. Select hosts and firmware **3. Update options and schedules** 4. Summary

☒ Update Parallelization

Scale: Make sure the value is set according to the current available system resources of the cluster.

☐ Force downgrade

☒ Schedule

☐ Now

☒ Schedule

Back Next Cancel

Figure 7. Select options and schedules page

The following options are displayed on this page:

Update Parallelization:

The default is 1.

Specifies the number of hosts that can be updated concurrently.

Updating multiple hosts concurrently requires more system resources.

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

Force downgrade:

Specifies whether to update firmware if the installed version is newer than the one you selected.

Schedule:

Specifies a time to initiate the task.

7. Click **Next**. The Summary page is displayed.

Rolling System Update

1. Name and Type2. Select hosts and firmware3. Update options and schedules4. Summary

You have made the following selections:

Task Name: task example -2

Task Type: Update and Reboot

Update Option: Update Parallelization :2

Schedule: 2014/04/28 21:56

Selected hosts and firmwares:

9.115.253.74

QLLogic 10 GbE Converged Network Adapter MultiFlash Update for System x - sysx-2.20.04

Online Broadcom NetXtreme and NetXtreme II Firmware Utility for VMware - 2.2.1b

QLLogic FC 8 Gb Multiboot Update for BladeCenter - 8g-f70100-b214-e251

Brocade BootCode Update for 16G FC, 10G CNA and 4/8G FC HBA - 3.2.3.0

QLLogic 10 Gb Converged Network Adapter MultiBoot Update for BladeCenter - qmi8142-2.05.06

Emulex HBA (LPe1205/LPe1200x) Firmware Update for VMware - ibm1212-2.01a11-12

Emulex UCNA Firmware Update for VMware - ibm1212-4.6.281.21-1

BackFinishCancel

Figure 8. Summary page

8. Click **Finish** to save the task. RSU initiates the task according to the schedule.

Editing a not-started RSU task

Use the **Edit Rolling System Update (RSU)** option to make changes to a task that has not started and has a task type of *Update Only* or *Update and Reboot*.

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Update > Task Manager** page.

Procedure

1. Select a not-started RSU task from the list and click **Edit**. The Rolling System Update wizard opens. The current machine type and hosts are listed on the left and the available firmware are on the right.
2. Edit the task and then click **Finish** to save the changes.

Deleting an RSU task

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Update > Task Manager** page.

Procedure

1. Select one or more RSU tasks, that are not currently running, from the list.
2. Click **Delete**. The selected tasks are removed from the task list.

Canceling a running RSU task

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Update > Task Manager** page.

Procedure

1. Select a running RSU task in the list.
2. Click **Cancel**. RSU finishes updating the host that is currently running the task being canceled and cancels the task on the other hosts. This task may take several minutes to complete.

Rerunning a failed RSU task

Use the **Rerun** option to restart a Rolling System Update (RSU) task if the task has failed or if it has been canceled. The **Rerun** button is only available in these two situations.

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Update > Task Manager** page.

Procedure

Click **Rerun** in the status column. RSU restarts the task and shows the current status.

Cloning a completed RSU task

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Update > Task Manager** page.

Procedure

1. Select a finished, failed or canceled RSU task from the list.
2. Click **Create Like...** to open the Rolling System Update Wizard.
3. Edit the original selection and click **Finish** to save the new task.

Viewing the RSU task report

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Update > Task Manager** page.

Procedure

In the Status column, click a status link to open the Rolling System Update Report view. The table below lists the status for tasks, hosts, and firmware. For detailed information about the Rolling System Update tasks, please refer to “Working with the Rolling System Update function” on page 16.

Table 7. Rolling System Update task status

Target	Status	Description
Rolling Update Task	Not Started	The task has not started.
	Running	The task is running.
	Canceled	The task is canceled.
	Failed	Causes of task failure: <ul style="list-style-type: none">• Downloading firmware package failed.• Rebooting ESXi host failed.• VM migration failed.• Firmware update failed
	Finished	The task has completed. If firmware is failing to update, the task is also marked as Finished.
Host	Not Started	The update for the host has not started.
	Migrating	The host is entering maintenance mode.
	Maintenance	The host is in maintenance mode.
	Updating	The firmware of the host is updating.
	Reboot	The host is rebooting after updating completes.
	Exit Maintenance	The host is exiting maintenance mode.
	Success	The firmware update succeeded.
	Failed	The causes of host failure: <ul style="list-style-type: none">• Cannot enter maintenance mode.• Cannot get the update package.• Cannot update the firmware.• Cannot reboot the host.• Cannot exit maintenance mode.
Firmware	Not Started	The firmware update has not started.
	Running	The firmware update is running.
	Success	The firmware update succeeded.
	Failed	The firmware update failed.

Working with the Rolling System Reboot function

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

Before you begin

The following prerequisites are necessary for using the Rolling System Reboot function:

VMware vCenter Enterprise or Enterprise Plus Edition with DRS:

Is enabled and running in fully automated mode.

Host access has been granted:

For more information, see the “Working with the Cluster Overview function” on page 13.

Managing Rolling System Reboot tasks

The Rolling System Reboot (RSR) Task Manager can assist you with creating and managing rolling reboot tasks. An RSR task contains all of the information and options required for a rolling reboot.

Procedure

1. Click **Lenovo XClarity Integrator > Rolling System Reboot**.
2. In the navigation pane, click **Task Manager**. The Task Manager page is displayed.

The Task Manager table provides the following detailed information about RSR tasks:

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

3. Use the Task Manager to perform the following task functions.

Table 8. Rolling System Reboot task functions

Task function	Description
Create	Creates a new RSR task.
Create Like	Creates a new RSR task from an existing RSR task.
Edit	Allows you to edit an RSR task that has not been started.
Delete	Removes an RSR task from the task list.
Cancel	Stops a running RSR task.
Rerun	Allows you to rerun a failed RSR task.

Creating an RSR task

Use the **Create** option to create a new Rolling System Reboot (RSR) task. Each cluster can have only one active RSR task if the task type is *Update Only*, *Update and Reboot*, or *Reboot Only*.

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Reboot > Task Manager** page.

Procedure

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

2. Enter a name for the task you are creating in the **Task Name** field and select the hosts you want to reboot.
3. Click **Next**. The reboot options and schedules screen is displayed.

Reboot Parallelization

The default is 1.

Specifies the number of hosts that can be rebooted concurrently.

Rebooting multiple hosts concurrently requires more system resources.

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

Schedule

Specifies a time to initiate the task.

4. Click **Next**. The Summary page is displayed.
5. Click **Finish** to save the task. RSR initiates the task according to the schedule.

Editing a not-started RSR task

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Reboot > Task Manager** page.

Procedure

1. Select a not-started RSR task in the list and click **Edit**. The Rolling System Reboot wizard opens. The machine type and hosts are listed.
2. Edit the task and then click **Finish** to save changes.

Deleting an RSR task

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Reboot > Task Manager** page.

Procedure

1. Select one or more RSR tasks, that are not currently running, from the list.
2. Click **Delete**. The selected tasks are removed from the task list.

Canceling a running RSR task

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Reboot > Task Manager** page.

Procedure

1. Select a running RSR task from the list.
2. Click **Cancel**. RSR completes updating the host that has started and only cancels the others. This task may take several minutes to complete.

Rerunning a failed RSR task

Use the **Rerun** option to restart a Rolling System Reboot (RSR) task that has failed or if it has been canceled. The **Rerun** button is only available in these two situations.

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Reboot > Task Manager** page.

Procedure

Click **Rerun** in the status column. RSR restarts this task and shows its current status.

Cloning a completed RSR task

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Reboot > Task Manager** page.

Procedure

1. Select a finished, failed or canceled RSR task from the list.
2. Click **Create Like...** to open the Rolling System Reboot wizard.
3. Edit the original selection and click **Finish** to save the new task.

Viewing the RSR task report

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

About this task

This task is performed from the **Lenovo XClarity Integrator > Rolling System Reboot > Task Manager** page.

Procedure

In the Status column, click a status link to open the Rolling System Reboot Report view. The table below lists the status for tasks and hosts. For detailed information about the Rolling System Reboot tasks, refer to “Working with the Rolling System Reboot function” on page 24.

Table 9. Rolling System Reboot task status

Target	Status	Description
Rolling Reboot Task	Not Started	The task has not started.
	Running	The task is running.
	Canceled	The task is canceled.
	Failed	Causes of task failure: <ul style="list-style-type: none"> • Downloading firmware package failed. • Rebooting ESXi host failed. • VM migration failed. • Firmware update failed
	Finished	The task has completed.
Host	Not Started	The update for the host has not started.
	Migrating	The host is entering maintenance mode.
	Maintenance	The host is in maintenance mode.
	Reboot	The host is rebooting after updating completes.
	Exit Maintenance	The host is exiting maintenance mode.
	Success	The firmware update succeeded.
	Failed	The causes of host failure: <ul style="list-style-type: none"> • Cannot enter maintenance mode. • Cannot reboot the host. • Cannot exit maintenance mode.

Working with Predictive Failure Management

The topics in this section describe how to use Predictive Failure Management on vSphere Web Client to protect your running workload. Use the Policy and Rules page to set management policies for a server based on a hardware predictive failure alert. Based on a defined policy, Lenovo XClarity Integrator for VMware vCenter evacuates VMs from a server to other hosts in the cluster in response to predictive failure alerts that have occurred. Use the Predictive Failures page to view predictive failure alerts from the server and the triggered policy history.

Before you begin

Before using Predictive Failure Management, verify the following prerequisites are met:

- Discover the IMMs and request access to the IMMs before setting the predictive failure management policy.
- Proper configuration of the network management policy on the vCenter Server server is required to enable TCP on the https port that you selected when installing Lenovo XClarity Integrator. The default port is 9500. Lenovo XClarity Integrator for VMware vCenter listens on this port for incoming indications.
- A host must be put in a properly configured cluster. A host with vMotion enabled must be available within this cluster. Lenovo XClarity Integrator for VMware vCenter evacuates VMs to other hosts in the cluster, and then puts the host in maintenance mode.

Setting a new policy

A policy defines the hardware event categories you want to monitor and the corresponding action if an event occurs. You can set an RAS policy for each of the supported servers in a cluster.

About this task

This task is performed from the **Lenovo XClarity Integrator > Predictive Failure > Policy and rules** page.

Procedure

1. Click **Set policy**. The Set Policy dialog box is displayed.

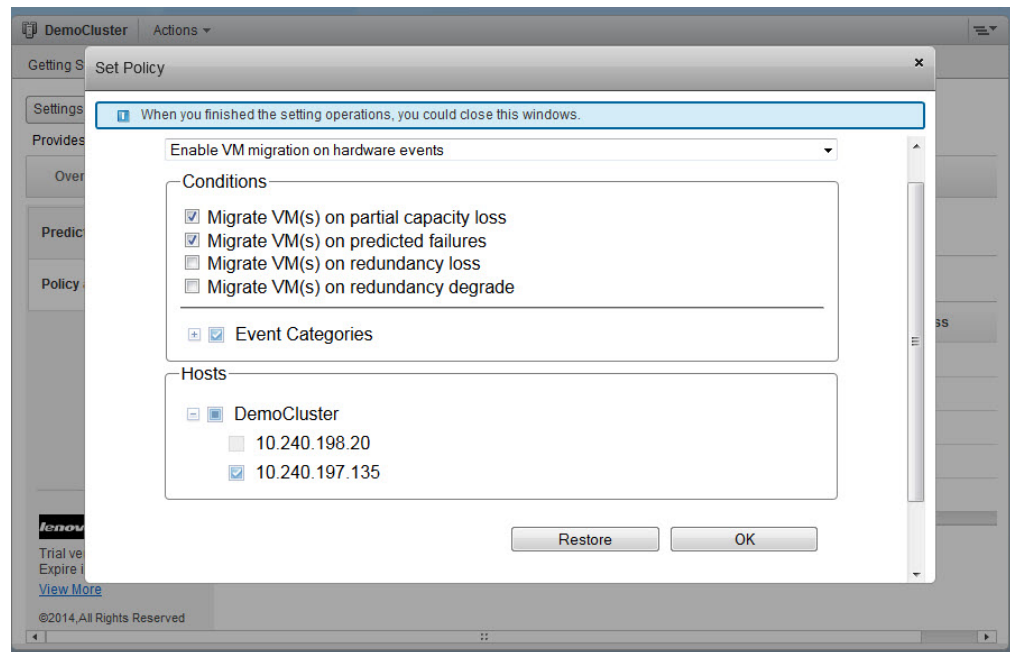


Figure 9. Set Policy

Note: The Conditions and Event Categories might be different for each server, depending on the server's firmware version.

2. To create a new policy, select **Enable VM migration on hardware events** from the list.
3. Select your preferred Conditions and Hosts and click **OK**.
4. To disable a policy, select **Disable VM migration on hardware events** from the list.
5. Select the hosts, and click **OK**.
6. Close the Set Policy dialog by clicking the close button at the top right.

The Conditions will show as one or more of the following:

- Migrate VM(s) on partial capacity loss
- Migrate VM(s) on predicted failures
- Migrate VM(s) on redundancy loss
- Migrate VM(s) on redundancy degrade

You can select one or more of the supported condition actions.

Event categories

This topic describes predictive failure alert event categories as shown on the Set Policy page.

The following table contains the predictive failure alert event categories used on the Set Policy page.

Table 10. Predictive Failure Alert Event categories

PFA Event	Description
Processor subsystem	Processor subsystem includes the CPU, its internal circuits like cache, the bus controller, and external interface.
Memory subsystem	Memory subsystem includes the memory controller, memory buffer, memory bus interface, memory card, and DIMM.
I/O subsystem	I/O subsystem includes: I/O Hub, I/O bridge, I/O bus, I/O processor, I/O adapters for various I/O protocols, such as PCI and InfiniBand.
Power	Power includes the power supply and power control hardware.
Cooling	All thermal-related events.
Fans	Includes the fan and blower.
Storage	Includes the storage enclosure, storage controller, raid controller, and media (disk, flash).
Platform firmware	Platform firmware includes IMM and uEFI.
Software	Operating system software and application software.
External environment	All events of an external-related environment including: AC power source, room ambient temperature, and user error.

Condition Action: The Virtual Machine Migration action evacuates all of the VMs from the server and puts the server in maintenance mode.

Viewing predictive failure alert events and the Action History table

Lenovo XClarity Integrator for VMware vCenter with vSphere Client monitors predictive failure alerts (PFAs) from an IMM. All predictive failure events are listed in the Event Log table. When the conditions of a rule are met, the defined action of the rule is launched on the managed endpoint. All of the triggered rules and action results are listed in the Action History table.

About this task

This task is performed on the Predictive Failure page.

Procedure

Click **Lenovo XClarity Integrator > Predictive Failure**.

Predictive Failures ?

View Predictive Failure event log and action history.

Event Log

Host	Message ID	Severity	Time Stamp	Description
10.240.197.135	PLAT0038	Warning	10:37:26 03/04/2015	processor 1 is operati
10.240.197.135	PLAT0039	Warning	10:37:37 03/04/2015	The Processor proces
10.240.197.135	PLAT0188	Warning	06:05:25 03/20/2015	The System IBM Flex S
10.240.197.135	PLAT0188	Warning	06:32:46 03/20/2015	The System IBM Flex S
10.240.197.135	PLAT0038	Warning	02:44:24 03/27/2015	processor 1 is operati
10.240.197.135	PLAT0039	Warning	02:44:44 03/27/2015	The Processor proces

Action History

Host	Message ID	Status	Start Time	End Time
10.240.197.135	PLAT0188	Success	17:01:28 03/20/2015	17:02:01 03/20/20
10.240.197.135	PLAT0188	Success	17:30:00 03/20/2015	17:30:36 03/20/20

Lenovo
Version information: 4.0
[View More](#)
©2014, All Rights Reserved

Figure 10. Viewing Predictive Failures

Managing hardware events

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

Before you begin

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

Procedure

1. On the Cluster overview page, find the IMM nodes and request IMM access to ensure that the vCenter server has an out-of-band (OOB) network connection with the IMM managed ESXi servers.
2. Enable TCP on the https port that you selected for Lenovo XClarity Integrator for VMware vCenter. The default is 9500 when you install Lenovo XClarity Integrator for VMware. Lenovo XClarity Integrator for VMware vCenter listens on this port for incoming indications.

What to do next

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

Alarms

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

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

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

Chapter 5. Managing servers

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

Before you begin

Verify that these prerequisites have been completed:

- The vCenter Server server has an out-of-band (OOB) network connection with the IMM of the managed ESXi servers.
- You can locate the IMM and have requested access for the IMM on the Cluster Overview page.

About this task

Complete these steps to view the Lenovo XClarity Integrator server management functions.

Procedure

1. Select a host from the inventory tree.
2. Click the **Manage** tab.
3. Click the **Lenovo XClarity Integrator** tab. The following management functions are available to use for a single Lenovo server:
 - System
 - Alerts and Events
 - Firmware Updates
 - Power and Cooling
 - Configuration

System function

The System function collects and analyzes system inventory information and health status to aid in diagnosing system problems.

Information about the following aspects of a system are collected:

- Basic system information
- System event logs
- Installed applications and hot fixes
- Network interfaces and settings
- Hardware inventory
- Vital product data and firmware information

System provides an organized view that you can use to perform the following functions:

- View the system information
- Launch system diagnostic collection
- View the categorized system inventory results

Chassis Map function

If a server is also managed by Lenovo XClarity Administrator, and you have already registered Lenovo XClarity Administrator to this vCenter, you can use the Chassis Map function.

For information about using the Chassis Map function, refer to the “Working with the Chassis Map function” on page 53 in “Working with the Lenovo Infrastructure view” on page 51.

System Overview

The System Overview page provides a snapshot view of the current system. You can view basic system information such as the machine type, operating system, version, IMM firmware version, and uEFI firmware version. You can also view the System Hardware Event Summary and System Inventory Collection History.

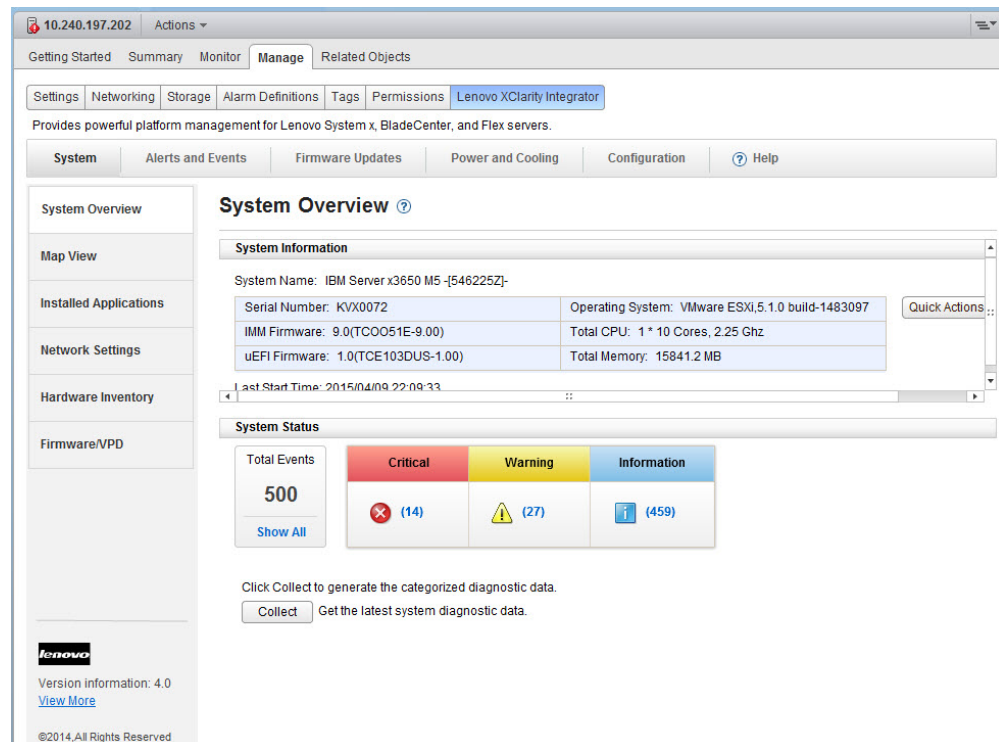


Figure 11. System Overview page

Launching the System Diagnostic Collection function

This topic describes how to launch the System Diagnostic Collection function to get an up-to-date and detailed system analysis.

Procedure

1. Click **Collect** located in the bottom section of the System Overview page. This collect operation can take up to five minutes to complete.

Important: During the collection process, the Installed Applications page, Network Settings page, Hardware Inventory page, and Firmware/VPD page are blocked. To avoid possibly disrupting the process, do not navigate to any other host.

When the collection process finishes, the last collection time is displayed on the System Overview page. The hyperlink **Download log** is displayed after the collection time.

2. Click **Download log** to download the latest system diagnostic data. The latest system diagnostic data can be viewed from each of the categorized pages. See “Viewing the categorized analysis results for vSphere Web Client.”

Viewing the categorized analysis results for vSphere Web Client

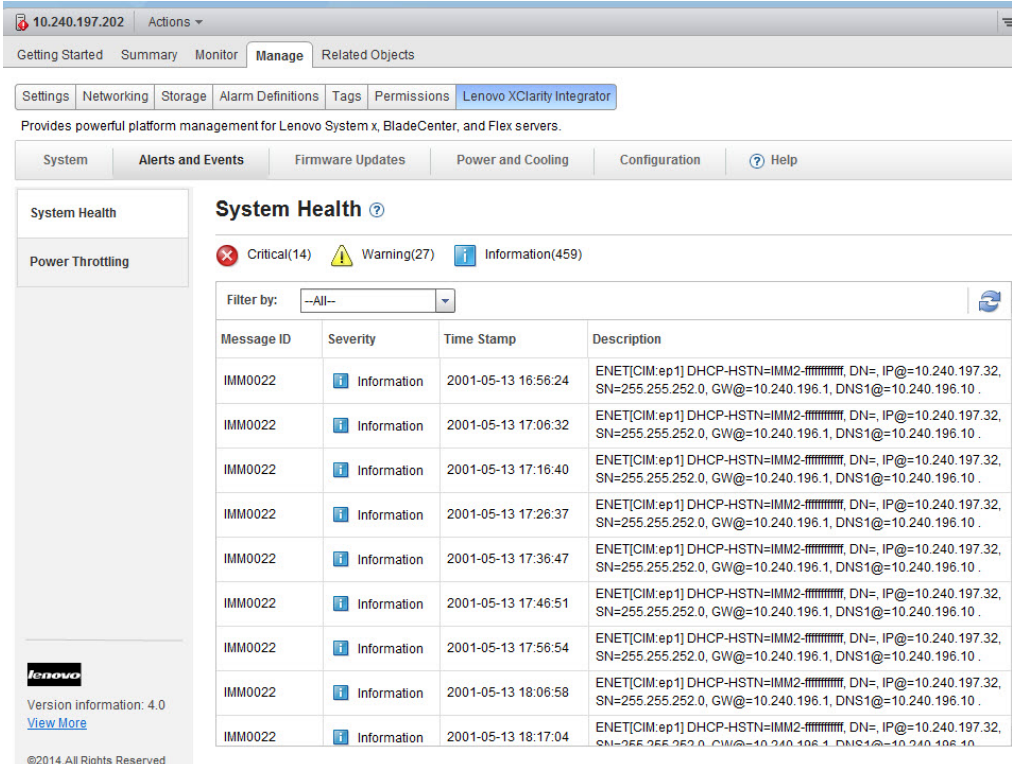
After you launch a full system diagnostic collection, you can view the latest categorized analysis results.

The categorized analysis results are contained in tables located on the pages listed below. On the System Overview page, select a page to view the results:

- Installed Applications
- Network Settings
- Hardware Inventory
- Firmware/VPD

Working with Alerts and Events

The Alerts and Events function collects system health information and displays hardware events and Power Throttling alerts.



The screenshot shows the vSphere Web Client interface for a system with IP 10.240.197.202. The 'Alerts and Events' tab is selected, showing a summary of 14 Critical, 27 Warning, and 459 Information events. A table of recent events is displayed, all with an 'Information' severity.

Message ID	Severity	Time Stamp	Description
IMM0022	Information	2001-05-13 16:56:24	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.
IMM0022	Information	2001-05-13 17:06:32	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.
IMM0022	Information	2001-05-13 17:16:40	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.
IMM0022	Information	2001-05-13 17:26:37	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.
IMM0022	Information	2001-05-13 17:36:47	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.
IMM0022	Information	2001-05-13 17:46:51	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.
IMM0022	Information	2001-05-13 17:56:54	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.
IMM0022	Information	2001-05-13 18:06:58	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.
IMM0022	Information	2001-05-13 18:17:04	ENET[CIM.ep1] DHCP-HSTN=IMM2-ffffffffff, DN=, IP@=10.240.197.32, SN=255.255.252.0, GW@=10.240.196.1, DNS1@=10.240.196.10.

Figure 12. Viewing Alerts and Events

The System Health table contains alerts and events that can be sorted by clicking the table columns. The table can also be filtered by choosing a severity level from the **Filter by** menu. To collect the latest alerts and events from the host, click **Refresh**.

Working with Firmware Updates

The Firmware Updates function applies recommended updates UpdateXpress System Pack (UXSP) and individual updates to your ESXi system. You can use this function to obtain and deploy UXSP firmware updates and individual firmware updates.

The main functions of the Firmware Updates function include:

Acquire Updates:

The Acquire Updates function downloads the UpdateXpress System Pack and individual updates for supported server types from a remote location, such as the Lenovo website.

Compare and Update:

- Inventories the system on which the update is being performed.
- Queries the update directory for a list of applicable update packages.
- Compares the inventory to the applicable update list.
- Recommends a set of updates to apply.
- Deploys the updates to the system

Prerequisites for updating firmware

This topic describes the necessary prerequisites for updating firmware.

Before you begin

Complete the following prerequisite steps before updating the firmware.

1. Enable **Commands** on the USB interface in uEFI by changing the uEFI settings.
2. Reboot the host.

Selecting an update preference

The Firmware Updates function can update a remote ESXi host by using either recommended (UXSP) or individual updates acquired from the Lenovo website or from a specific location. On the Updates Preferences page, you can select the method for acquiring the updates package.

Procedure

1. Select **Firmware Updates** on the Manage Lenovo XClarity Integrator page. The Updates Preferences page is displayed.

Figure 13. Update Preferences page

2. On the Update Preferences page, click to select one of the following update options.

Check the Lenovo website:

Downloads the appropriate updates automatically from the Lenovo site.

Notes:

- If the vCenter Server cannot access the website directly, you can enter the proxy server and port.
- When you select this option to update firmware, the updates package is saved in the Installation folder\IVP\bin\data\uxspi\repository\ directory on the vCenter Server after download.
- Select the location method to update the other host servers that have the same machine type.
- Before updating the host firmware, you must input the root account of the host for updates.

Look in a directory on vCenter Server

Locates the appropriate updates from a local repository.

Note: When you select the **Look in a directory on vCenter server** option, the Firmware Updates function acquires updates from a specified directory on vCenter Server: Installation folder\webroot\bin\data\uxspi\repository\. However, you are not allowed to change the directory, but you can put updates under this directory.

Firmware Updates scenarios

The topics in this section describe two scenarios for Firmware Updates: Recommended Updates (UXSP) and Individual Updates.

An UpdateXpress System Pack (UXSP) is an integration-tested bundle of online firmware and driver updates for Lenovo System x and BladeCenter servers. UpdateXpress System Packs simplify the downloading and installation of all online driver and firmware updates for a given system, ensuring that you are always working with a complete, current set of updates that have been tested together and bundled by UpdateXpress System Pack.

Recommended Updates (UXSP)

If you select **Check the Lenovo website** on the Update Preferences page, the Recommended Updates option downloads and installs firmware and driver updates from the latest UXSP for Lenovo System x and BladeCenter servers. If you select **Look in a directory on vCenter server**, Recommended Updates will install firmware and driver updates from a local vCenter directory.

Procedure

1. To use Recommended Updates, select one of the following methods:
 - **Check the Lenovo website:** Verify that the vCenter Server has Internet access to connect to the Lenovo website.
 - **Look in a directory on vCenter server:** Verify that the UXSP in the specified vCenter Server directory is applicable for the target machine type.
2. Click **Start Update Wizard** on the Recommended Updates page. The Recommended Updates wizard starts and the Check Compliance dialog box is displayed.



Figure 14. Recommended Updates wizard - Check Compliance dialog box

3. Click **Check Compliance**. If you do not have this type of account for the target host or if the account is wrong, a dialog box opens and prompts you for the host account information.
4. When the Check Compliance action has completed, make any necessary changes, and click **Next**.

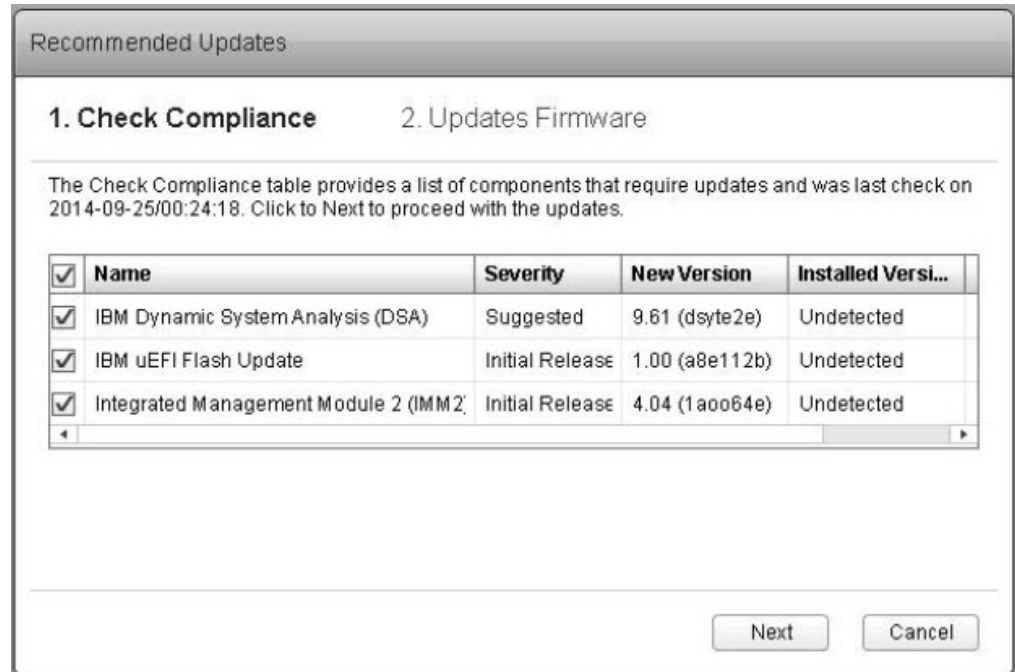


Figure 15. Check Compliance complete

After all of the selected downloads are complete, the selected updates are installed on the target host.

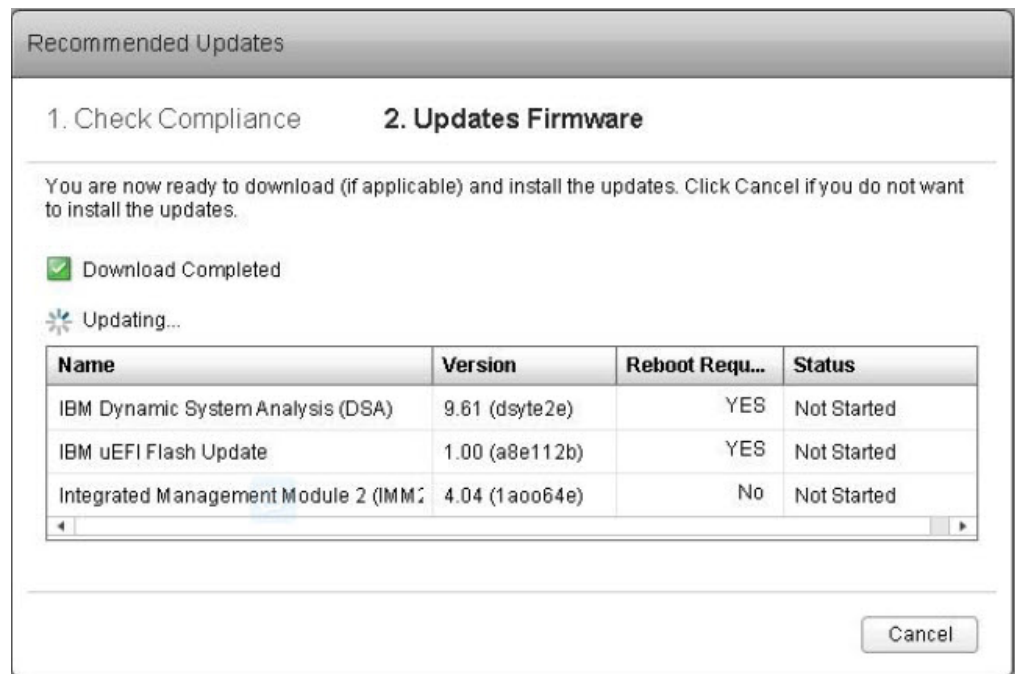


Figure 16. Recommended Updates wizard - updating firmware

5. After all of the updates have been installed, click **Close** to exit the wizard.

Individual Updates

This topic provides information about updating a remote server using the Individual Updates option.

Before you begin

Verify one of the following methods for using the Individual Updates option:

- The vCenter Server has Internet access to connect with the Lenovo website.
- The directory of vCenter Server has a UXSP that can apply to the target machine type when you selected location mode in Update Preferences.

About this task

To update a remote server using the Individual Updates option, perform these steps.

Procedure

1. Click **Start Update Wizard** on the Individual Updates page. The Individual Updates wizard opens.
2. Click **Check Firmware Compliance**. If you do not have this type of account for the target host or if the account is wrong, a dialog box opens and prompts you for the host account information.
3. When the Check Compliance action has completed, make any necessary changes, and click **Next**. After all the selected downloads are complete, the selected updates are applied to the target host.
4. After all of the updates have been applied, click **Close** to exit the wizard.

Working with Power and Cooling

The topics in this section describe Power Metric options that provide you with the ability to manage power usage with the Power Capping and Power Throttling features.

Power Metric page

The Power Metric page has options for viewing the power usage history, thermal history, and fan summary. If a host is being monitored, the current power usage, thermal history, fan history, and the time of the monitor reading is displayed. This information is automatically refreshed every five minutes. This information is helpful for determining whether to reassign the workload.

System	Alerts and Events	Firmware Updates	Power and Cooling	Configuration	Help
--------	-------------------	------------------	--------------------------	---------------	------

General
Power History
Thermal History
Fan History

General

After enabling power metric, you can set the value for each power metric function.

Attribute	Value	Actions
Host Monitoring	Enabled	
Poll Time	2014-09-25 01:56:33	
Power Input	154 watts	
Thermal Input	26 °C	
Fan Input		
Power Capping	Enabled	Disable
	440 watts Edit	
Power Throttling	Enabled	Disable
Warning Throttling	480 watts Edit	
Critical Throttling	516 watts Edit	

Figure 17. Power Metric page

Set Power Capping on vSphere Web Client

You can use the Power Capping feature to allocate less power and cooling to a system if the firmware supports Power Capping and it is enabled. This feature can help lower datacenter infrastructure costs and potentially allow more servers to be put into an existing infrastructure. By setting a Power Capping value, you can ensure that system power consumption stays at or below the value defined by the setting. The Power Capping value is the value you set for a rack or Blade server that will be capped by the firmware. The Power Capping value is persistent across power cycles for both rack and blade servers.

If the server supports Power Capping, XClarity Integrator retrieves the minimum and maximum Power Capping values from the server and displays it as a range. In the following figure, 473 is the minimum value, and 567 is the maximum value.

System	Alerts and Events	Firmware Updates	Power and Cooling	Configuration	Help
--------	-------------------	------------------	--------------------------	---------------	------

General
Power History
Thermal History
Fan History

General

After enabling power metric, you can set the value for each power metric function.

Attribute	Value	Actions
Host Monitoring	Enabled	
Poll Time	2014-09-25 01:56:33	
Power Input	154 watts	
Thermal Input	26 °C	
Fan Input		
Power Capping	Enabled	Disable
	440 <input type="text"/> (437 - 516) <input type="button" value="Save"/> <input type="button" value="Cancel"/>	
Power Throttling	Enabled	Disable
Warning Throttling	480 watts Edit	
Critical Throttling	516 watts Edit	

Figure 18. Setting Power Capping on vSphere Web Client

Set Power Throttling on vSphere Web Client

You can use the Power Throttling feature on vSphere Web Client to receive alerts when power consumption exceeds a set value. You can set two different Power Throttling values, one for a warning and one for a critical alert. When the power

consumption exceeds a defined Power Throttling value, LXCI receives a throttling event, which is then displayed in the Power Throttling Indications table.

Click **Enable** to enable the Power Throttling feature before setting a value for Watts.

System

Alerts and Events

Firmware Updates

Power and Cooling

Configuration

Help

General

Power History

Thermal History

Fan History

General

After enabling power metric, you can set the value for each power metric function.

Attribute	Value	Actions
Host Monitoring	Enabled	
Poll Time	2014-09-25 01:56:33	
Power Input	154 watts	
Thermal Input	26 °C	
Fan Input		
Power Capping	Enabled	Disable
	440 watts Edit	
Power Throttling	Enabled	Disable
Warning Throttling	480 (437 - 516) Save Cancel	
Critical Throttling	516 (437 - 516) Save Cancel	

Figure 19. Setting Power Throttling on vSphere Web Client

Viewing the Power Usage History, Thermal Usage History, and Fan Usage History for vSphere Web Client

You can customize the duration and interval for the Power Usage History, Thermal History, and Fan History charts. These charts are displayed in the right pane.

Procedure

- Click the **Power and Cooling** tab. For each of the history charts, you can:
 - Use the mouse wheel to zoom in and out of the charts, and use the drag and drop feature to move charts.
 - Click **Set Duration** to change the collection of history data to a different time interval.
- Select one of the following options from the left pane.

General

On this page, you can set the value of each power metric attribute after enabling power monitoring on a host.

Power History

The Power Usage History chart provides power consumption readings for a 24-hour period.

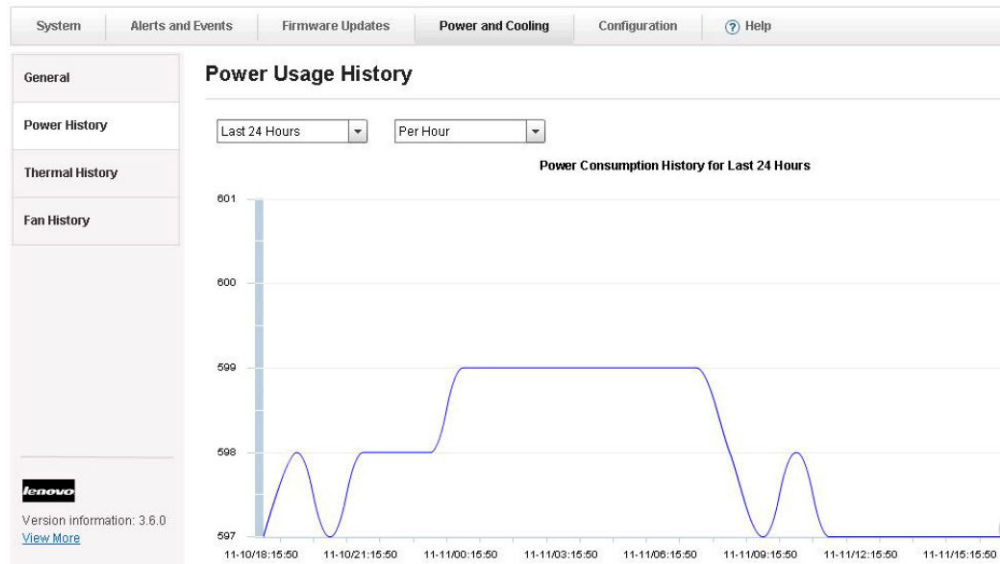


Figure 20. Power Usage History for vSphere Web Client

Thermal History

The Thermal Usage History chart provides temperature readings for a 24-hour period.

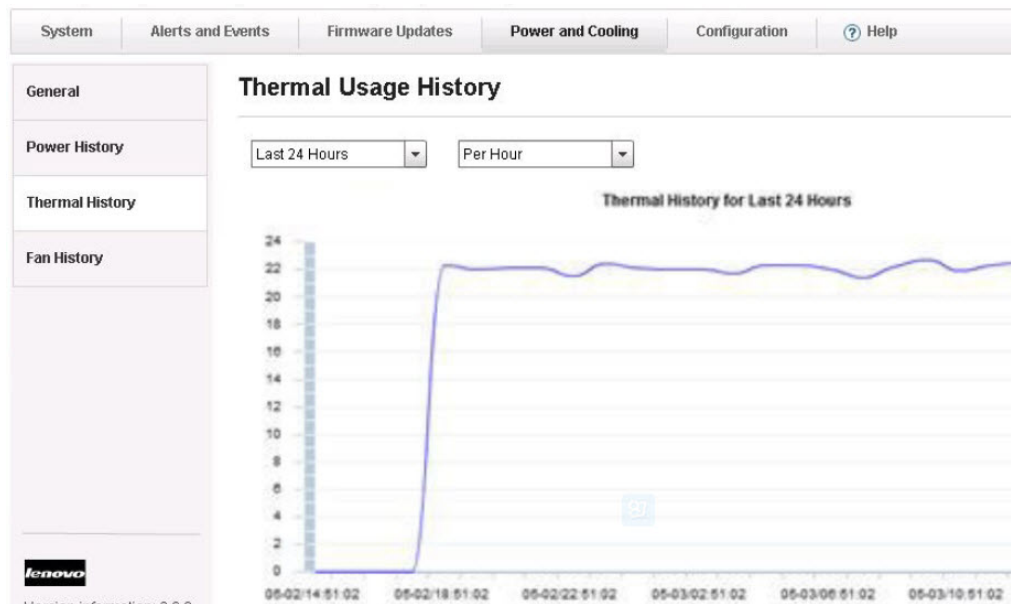


Figure 21. Thermal Usage History for vSphere Web Client

Fan History

The Fan Usage History chart provides fan usage readings for a 24-hour period.

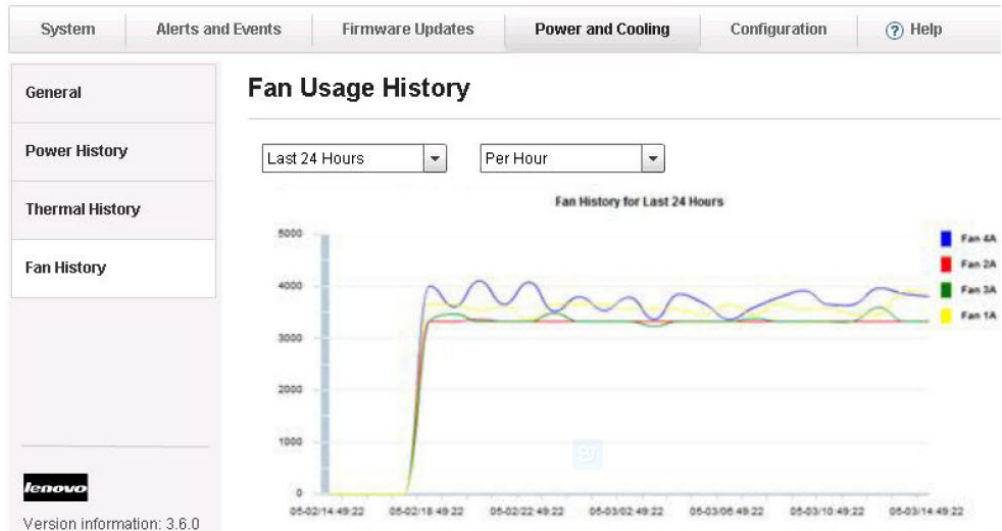


Figure 22. Fan Usage History for vSphere Web Client

Working with configuration

The Configuration page manages the system settings for a host. This includes deploying a configuration pattern or settings for IMM and uEFI, and changing the boot order of the host.

Deploying a configuration pattern on a server

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

About this task

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

Procedure

1. Click **Lenovo XClarity Integrator > Configuration > Configuration Pattern**.
The Configuration Pattern page is displayed.

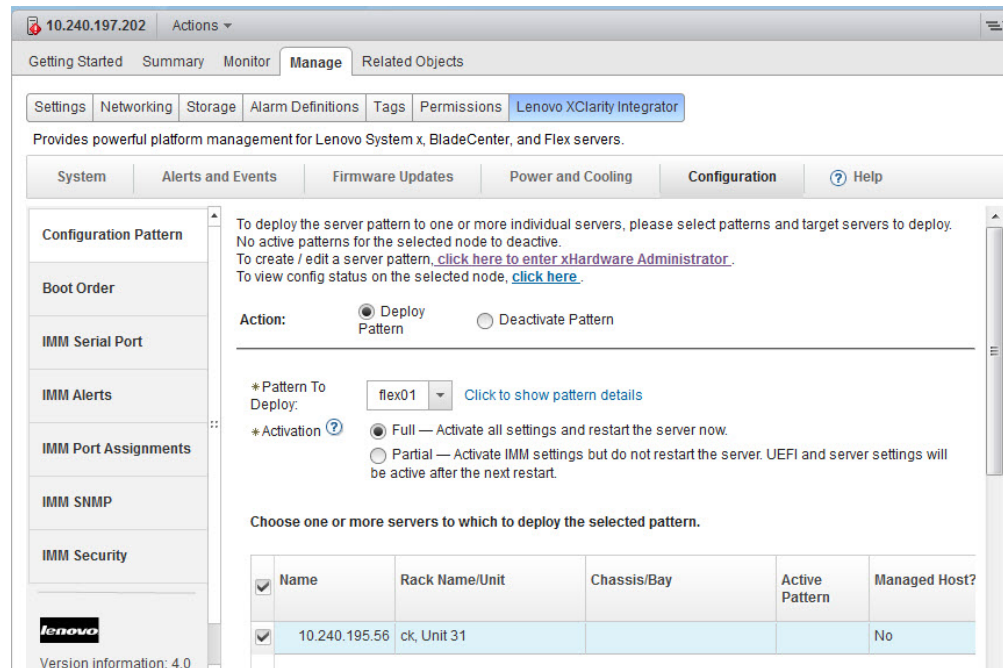


Figure 23. Deploy Pattern

2. Select one of the following actions:

Option	Description
Deploy pattern	Deploys the selected pattern to your servers.
Deactivate pattern	Deactivates the pattern from your servers.

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

Notes:

- The Configuration Pattern page is not visible if your server is not managed by LXCA, or if LCXA is not registered to this Lenovo XClarity Integrator.
- You can select to configure your server from the Configuration Pattern page. However, if your sever does not have any deployment patterns, you can use other setting pages, such as Boot Order or IMM Serial Port.
- If your server has deployed a pattern, other setting pages are not available. It is recommended that you use a pattern to configure your server by deactivating a pattern on your server, then other setting pages will be available.

Viewing advanced system settings

You can view the advanced system settings of your Lenovo System x, BladeCenter, or Flex server using the following procedure. Some configuration settings, such as uEFI settings, are only supported on a certain machine type or firmware version. If a host does not support a setting, it is disabled to indicate that it is not supported.

About this task

The following steps illustrate how to view two different advanced system settings: IMM Port Assignments and Boot Order.

Configuration settings are listed in the left pane. A date stamp with the last update date and time is displayed to the right of **Refresh** button. Click **Refresh** to get the latest setting values.

Procedure

- Click **IMM Port Assignments** to view the current IMM port assignments.

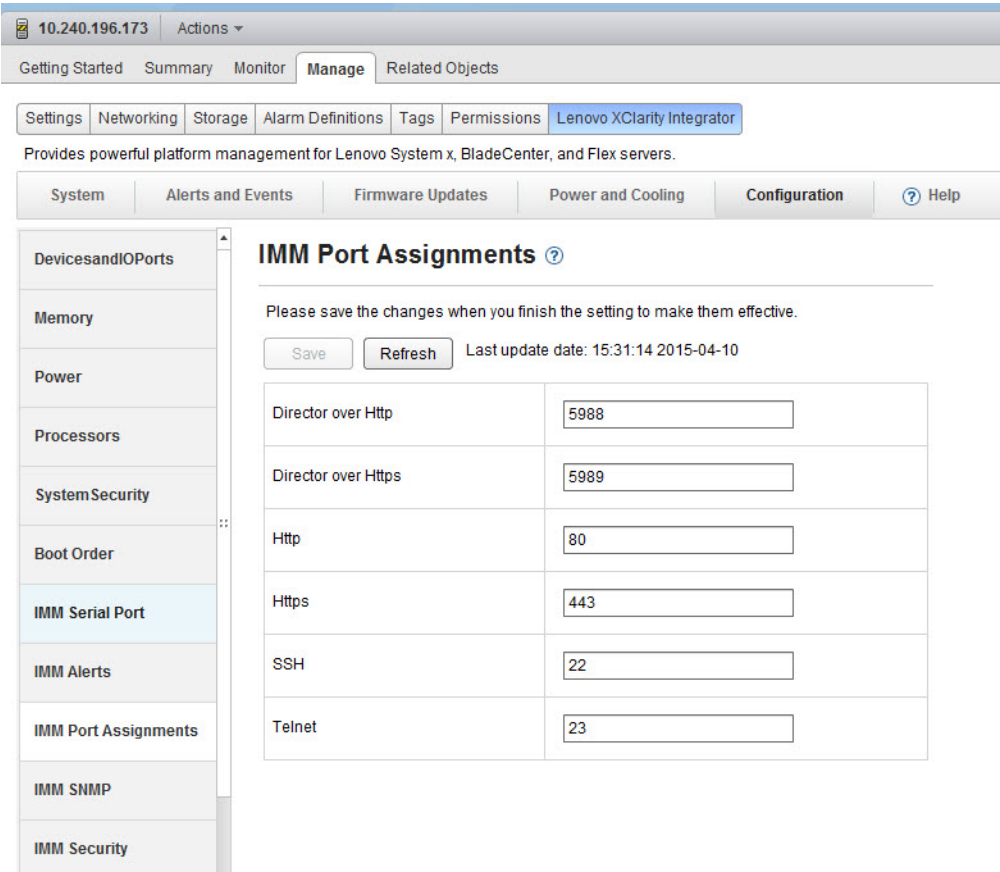


Figure 24. Viewing IMM Port Assignments

- Click **Boot Order** to view the current Boot Order, Wake-on-LAN boot order, or uEFI ROM order.

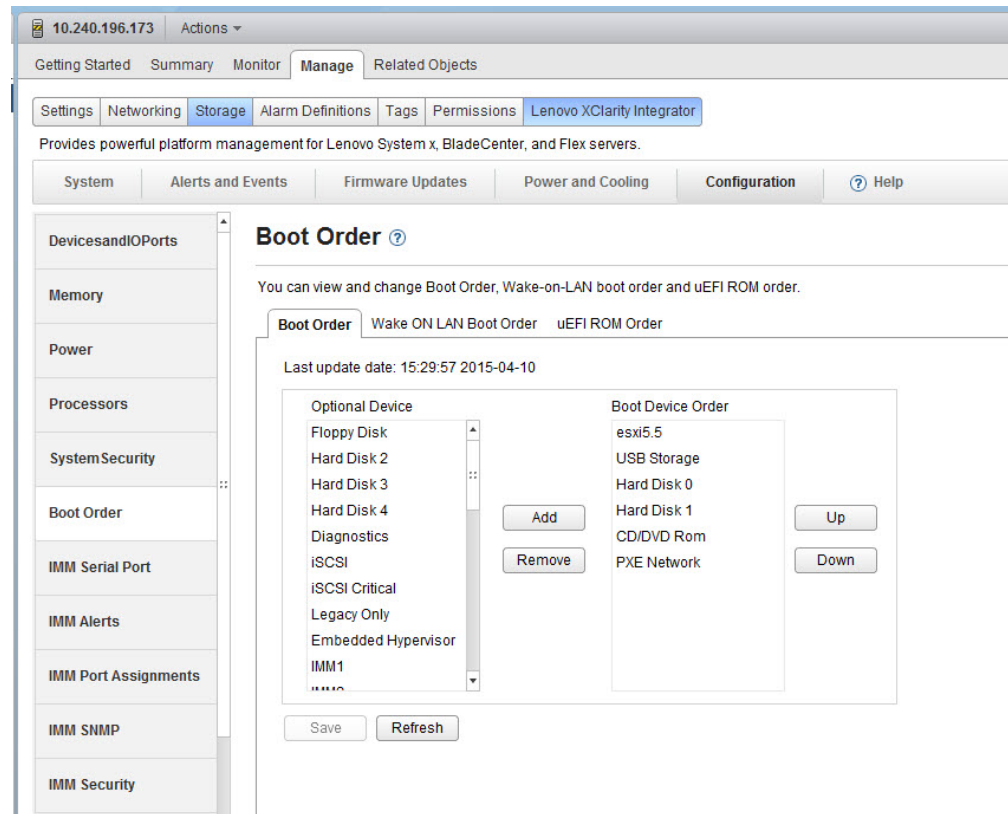


Figure 25. Viewing Boot Order

Changing advanced system settings

This topic describes how to change advanced system settings on the host.

About this task

The following procedure provides an example of changing the IMM Alerts settings.

Procedure

1. Click **IMM Alerts** the left pane to view the Alerts section of IMM settings.

10.240.196.173 Actions ▾

Getting Started Summary Monitor **Manage** Related Objects

Settings Networking Storage Alarm Definitions Tags Permissions **Lenovo XClarity Integrator**

Provides powerful platform management for Lenovo System x, BladeCenter, and Flex servers.

System Alerts and Events Firmware Updates Power and Cooling **Configuration** ? Help

Devices and I/O Ports

Memory

Power

Processors

System Security

Boot Order

IMM Serial Port

IMM Alerts

IMM Port Assignments

IMM SNMP

IMM Security

IMM Alerts ?

Please save the changes when you finish the setting to make them effective.

Last update date: 15:33:22 2015-04-10

Alert Recipient Email	<input type="text"/>
Alert Recipient Name	<input type="text"/>
Delay between entries	0.5 minutes ▾
Delay between retries	0.5 minutes ▾
Recipient Include EventLog	Disabled ▾
Remote Alert Recipient Status	Disabled ▾
Remote alert retry limit	5 times ▾

Figure 26. Viewing IMM Alerts

- Enter the new value, and click **Save**. The change is executed on the endpoint.
 - If the change is successfully executed, the following symbol is displayed.



Figure 27. Setting change success symbol

- If the change is not successfully executed, the following symbol is displayed.



Figure 28. Setting change not success symbol

To view detailed information about why the setting change failed, place the cursor over the symbol.

Example

The following list provides an example for some of the different types of settings and how to change these settings. The manner in which each setting is changed varies.

text string

Before you enter any information, a prompt showing the requirements is

displayed. If the information you entered does not match the requirements, place the cursor over the text string to view the description.

selection type

Select a value from the list.

boot order

The left column displays the current boot order, and the right column displays the optional device. To change the order, you can move a boot order option up or down and between the two columns, by clicking the corresponding button.

Chapter 6. Managing Lenovo infrastructure

Lenovo XClarity Administrator (LXCA) can assist you in managing your Lenovo infrastructure. The topics in this section describe how to use Lenovo XClarity Administrator to manage Lenovo infrastructure.

Before you begin

Refer to “Configuring Lenovo XClarity Administrator” on page 9 for information about the how to complete the LXCA prerequisites and registration.

Working with the Lenovo Infrastructure view

The Lenovo Infrastructure view shows the managed Lenovo XClarity Administrator (LXCA) domains, chassis, rack, and node in vSphere Web Client. This function allows you to use the features of Lenovo XClarity Administrator, such configuration pattern deployment and chassis map.

Before you begin

Before you can work with Lenovo XClarity Administrator, ensure the following:

1. Lenovo XClarity Administrator is registered in vSphere Web Client. For more information, see Chapter 6, “Managing Lenovo infrastructure.”
2. You have *LenovoXClarityIntegrator.AccessLenovoInfrastructure* privileges.

About this task

This procedure describes how to view and manage an LXCA domain using the Lenovo Infrastructure view.

Procedure

1. Click **Home > Center > Lenovo Infrastructure**. The managed Lenovo XClarity Administrator list is displayed.

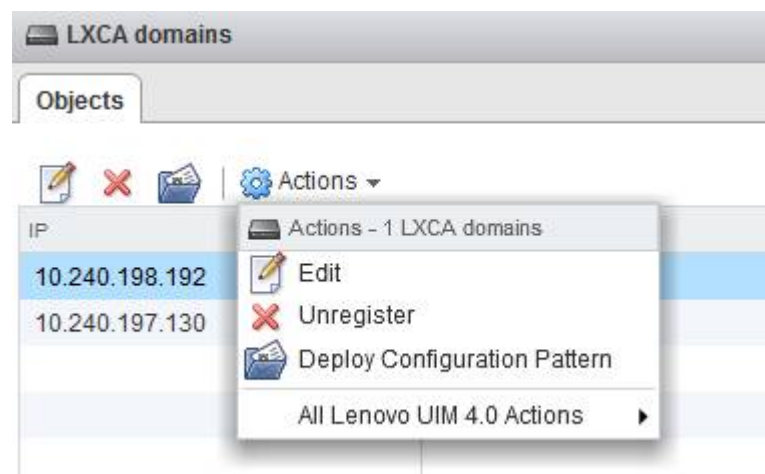


Figure 29. LXCA domains Actions list

2. Select one of the following options:

Option	Description
Edit	Allows you to edit your Lenovo XClarity Administrator registered information.
Unregister	Allows you to unregister your Lenovo XClarity Administrator.
Deploy Configuration Pattern	Allows you to deploy a pattern for all the nodes managed by this Lenovo XClarity Administrator.

3. Select a domain managed by Lenovo XClarity Administrator. The managed Chassis and Racks table is displayed, where you can run the Deploy Configuration Pattern action to deploy a pattern for all the nodes managed by this Chassis.

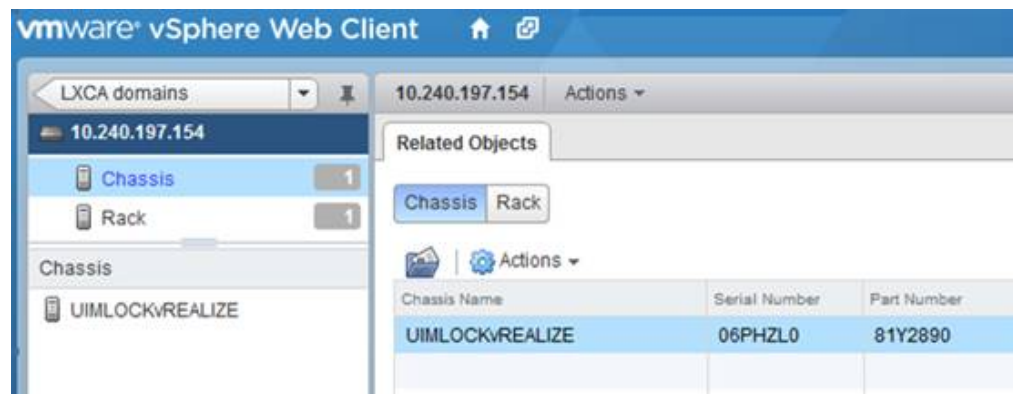


Figure 30. Managed Chassis and Racks table

4. Click either **Chassis** or **Rack** to view details for a chassis or a rack in the LXCA domain.

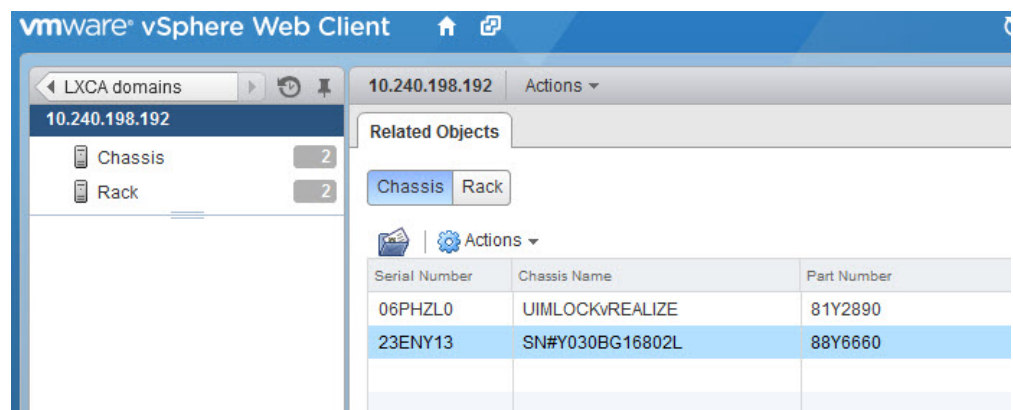


Figure 31. Chassis view

5. After selecting a Chassis or Rack view, you can:
 - a. Select **Deploy Configuration Pattern** to deploy a pattern for all the servers managed by this chassis or rack.
 - b. Click the **Monitor** tab to view the Chassis Map.

- c. Click the **Related Objects** tab to view the nodes list managed by this chassis or rack.

Working with the Chassis Map function

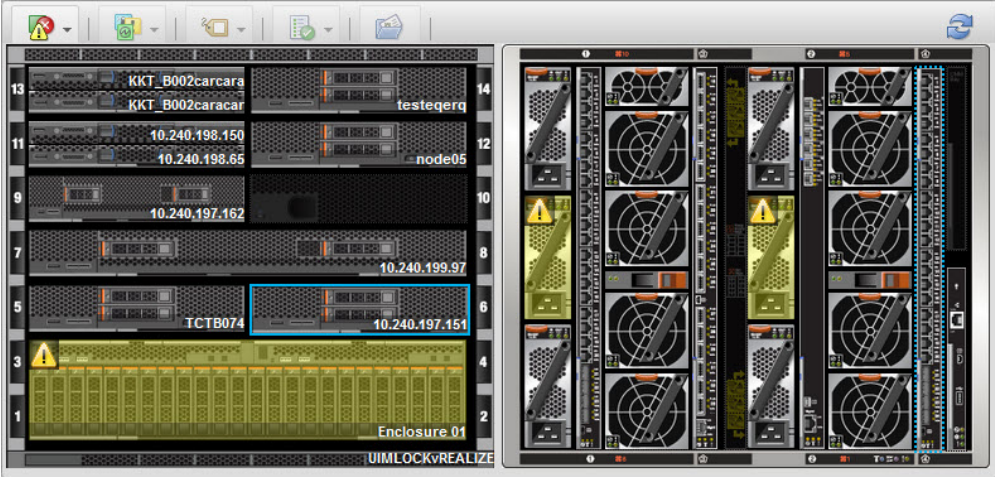
The Chassis Map provides a graphical view of a chassis. From this interface, you can also display the component status in a tabular list.

About this task

This task is performed on the Chassis page.

Procedure

1. In the **Chassis** column, click the link for a chassis. The Chassis view page for that chassis is displayed.



The screenshot shows the Chassis Map interface. On the left, a graphical view of a chassis is displayed with components like compute nodes, fans, power supplies, and Flex switches. A summary table is displayed below the graphical view. The table contains the following information:

Summary		Open xHMC for Details	All Actions
Name:	10.240.197.151		
Status:	Offline		
Chassis/Bay:	UIMLOCKvREALIZE / 6		
Host names (IMM):	IMM2-40f2e990dcd1		
Architecture:	x86_64		
Type-Model:	9532-AC1		
System FRU:			
System Board UUID:	DUMMY-73CBE41AFA1D4FEF-010103060000		

Figure 32. Chassis view

The graphical view shows components in the front of the chassis, such as compute nodes and components in the rear of the chassis such as fans, power supplies, and Flex switches.

2. Click **Table view** to display the component status in a tabular list.
You can choose among several overlays to help you quickly determine the status for all of the components in the chassis.

Table 11. Hardware map overlays


Overlay	Icon	Description
Hardware status		<p>Use this overlay to display the status for each of the components. You can choose one or more of the following status criteria:</p> <p>Critical Components have one or more critical alerts. Immediate user action is required.</p> <p>Warning Components have one or more warning alerts. User investigation is needed to determine the cause of the warnings, but there is no immediate risk of an outage.</p> <p>Synchronizing LXCA is waiting for the components to provide an updated status.</p> <p>Offline Components are not online.</p> <p>Unknown LXCA is not able to retrieve the status from one or more of the components in a chassis. User investigation might be needed.</p> <p>Normal Components are operating normally. Hover over a specific component to view information about the current status.</p>

Table 11. Hardware map overlays (continued)





Overlay	Icon	Description
Highlight front panel LEDs		<p>Use this overlay to view the LEDs that are available for each of the components. You can choose one or more of the following LEDs to view:</p> <p>Power LED Displays the current power LED for each component.</p> <p>Event Log LED Displays the event log LED, which is lit when there are events specific to a component in the LXCA event log.</p> <p>Location LED Displays the location LED, which can be turned on from the CMM to help you identify where a component is physically located.</p> <p>Fault LED Displays the status of the Fault LED for each component.</p> <p>Other LED Displays all of the other LEDs that are available for each component.</p> <p>Only Active LEDs Displays only the LEDs that are currently lit.</p> <p>Hover over a specific component to view more information about all of the LEDs for a component. For detailed information about each of the LEDs that can be displayed for a component, refer to the product documentation that is available for that component.</p>

Table 11. Hardware map overlays (continued)

Overlay	Icon	Description
Component names and properties		Use this overlay to display the name for each component in the chassis. When you hover over a component, additional properties about that component, such as the IP address and UUID, are displayed.
Compliance		Use this overlay to determine whether the firmware that is currently installed on a component complies with the compliance policy that has been defined for that component.
Configuration patterns		Use this overlay to determine which server patterns are assigned to each compute node.

Viewing the details of a managed chassis

You can view detailed information about a managed chassis.

About this task

To view the information about a managed chassis, complete these steps.

Procedure

1. Open Lenovo XClarity Administrator.
2. Select the **Open Lenovo XClarity Administrator for Details** link.

Launching an Integrated Management Module Interface

This topic explains how to launch management web console for a selected chassis or server on the Chassis Map.

About this task

This task is performed on the Chassis Map page.

Procedure

1. Click **vCenter > Lenovo Infrastructure > LXCA Domains**.
2. In the Lenovo XClarity Administrator domains section, select the Lenovo XClarity Administrator IP node and double click the chassis node in the right pane.
3. On the Chassis Map page, select a chassis or host and click **All Actions**.
4. Click **Launch Management Module Interface**. The web console is launched within Explorer.

Launching Remote Control

You can launch the Remote Control of a selected server on the Chassis Map.

About this task

This task is performed on the Chassis Map page.

Procedure

1. Click **vCenter > Lenovo Infrastructure > LXCA Domains**.
2. In the Lenovo XClarity Administrator domains section, select the Lenovo XClarity Administrator IP node and double click the chassis node in the right pane.
3. Select a chassis or a host on the Chassis Map page, and click **All Actions**.
4. Click **Launch Remote Control**. The remote console opens.

Working with configuration patterns

You can easily deploy or deactivate a server pattern to one or more individual servers or groups of servers using the Lenovo XClarity Administrator **Deploy Configuration Pattern** option from either the domains list view or Chassis list view. For example, you can deploy a server pattern to a chassis and have all of the servers in that chassis configured the same.

About this task

This task is performed from the LXCA domains page.

Procedure

1. Click **vCenter > Lenovo Infrastructure > LXCA Domains**. The LXCA domains page is displayed.
2. Select a Lenovo XClarity Administrator domain or Chassis, then click **Action > Deploy Configuration Pattern**. The Lenovo LXCA Configuration Pattern dialog box is displayed.

Lenovo LXCA Configuration Pattern

Please choose **Deploy Pattern** to deploy the server pattern to one or more individual servers, or **Deactivate Pattern** to deactivate a active pattern.
To create / edit a server pattern, [click here to enter LXCA](#).
To view config status on the selected node, [click here](#).

Action: ☒ Deploy Pattern ☐ Deactivate Pattern

+ Pattern To Deploy: flex01 [Click to show pattern details](#)

+ Activation [?](#) ☒ Full — Activate all settings and restart the server now.
☐ Partial — Activate IMM settings but do not restart the server. UEFI and server settings will be active after the next restart.

Choose one or more server to deploy the selected pattern.

☐ Show Empty Bays ☐ Show vSphere Managed Hosts By Deploy Status: All Systems Filter

Name	Rack Name/Unit	Chassis/Bay	Active Pattern	Managed Host?	Deploy Readiness
10.240.195.56	ck, Unit 31			No	⚠ Not Supported

Deploy

Figure 33. LXCA Configuration Pattern dialog box

3. Select one of the following actions:

Option	Description
Deploy pattern	Deploys the selected pattern to your servers.
Deactivate pattern	Deactivates the pattern from your servers.

4. Select a pattern from the **Pattern to Deploy** list.
5. Select one or more servers and click **Deploy**. The deployment progress is displayed.

Working with firmware compliance

Firmware management is simplified by assigning compliance policies to managed endpoints to ensure that firmware on those endpoints remains compliant. You can update and apply firmware compliance policies for all LXCA-supported System x and Flex System servers.

The following figure illustrates the workflow for updating firmware on managed endpoints.



Figure 34. Workflow for updating firmware on managed endpoints

Note: In LXCI you can only assign an existing compliance policy and activate updates. See the *Lenovo XClarity Administrator User's Guide* for information about managing the repository and creating compliance policies in LXCA.

To access this function, click **LXCA domains** under Lenovo Infrastructure. Then select a registered LXCA and click the **Firmware Updates: Apply / Activate** button.

Assigning compliance policies

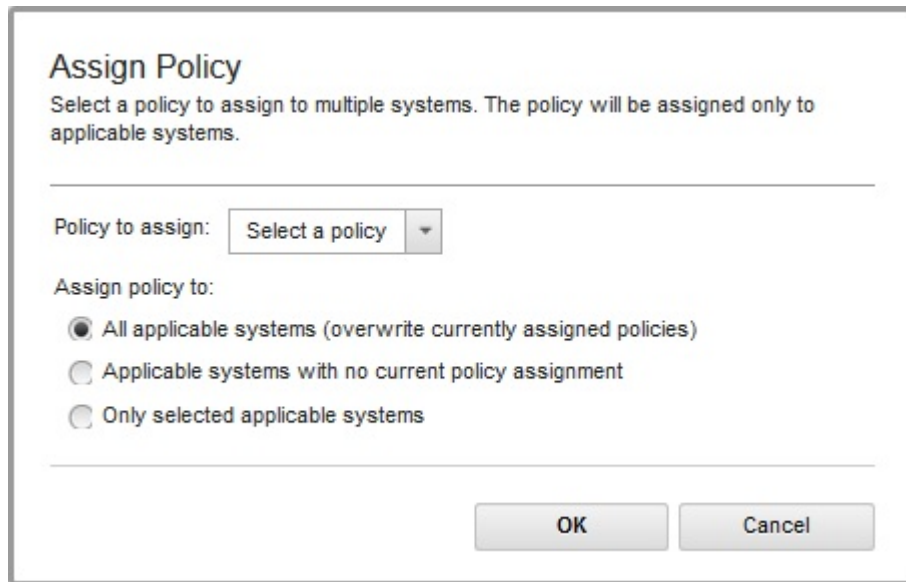
You must assign a compliance policy to an endpoint before you can apply and activate firmware updates on the endpoint.

About this task

Complete the following steps to assign a compliance policy to an endpoint.

Procedure

1. Select one or more systems to which you want to assign a compliance policy.
2. Click the Assign policy icon (📄). The Assign Policy dialog is displayed.



Assign Policy
Select a policy to assign to multiple systems. The policy will be assigned only to applicable systems.

Policy to assign: Select a policy ▼

Assign policy to:

- ☒ All applicable systems (overwrite currently assigned policies)
- ☐ Applicable systems with no current policy assignment
- ☐ Only selected applicable systems

OK Cancel

3. Select a compliance policy from the **Policy to assign** drop-down menu.
4. Select the scope for the policy assignment:
 - All applicable systems (this option overwrites currently assigned policies)
 - Applicable systems with no current policy assignment
 - Only selected applicable systems
5. Click **OK**. The Assigned Policy column in the Firmware Updates page changes to the name of the selected compliance policy.

Applying and activating firmware updates

The Firmware Updates feature does not automatically apply firmware updates to managed endpoints. After an endpoint is identified as not being compliant, you can manually apply and activate the firmware updates on managed endpoints using the Firmware Updates interface.

Before you begin

Firmware updates on compute nodes and rack servers are performed out-of-band. This means that the servers are shut down when firmware updates are being applied. Ensure that any running workloads either have been stopped or, if you are working in a virtualized environment, have been moved to a different server.

About this task

Complete the following steps to apply updates and activate managed endpoints.

Procedure

1. Click **Firmware Updates > Apply / Activate** in the menu bar. The Firmware Updates: Apply/Activate dialog is displayed.

Firmware Updates: Apply / Activate

To update firmware for a device, assign a compliance policy and select Perform Updates.

All Actions ▾ | Critical Release Information | Show: All Systems ▾ | Filter

System	Rack Name / Unit	Chassis / Bay	Power	Installed Version	Assigned Compliance Policy
4p3cmm 10.240.61.45	Unit 0	4p3cmm, Bay 1	On	2.50.0 / 2PET062	DEFAULT-2015-04-04 ▾
IO Module 01 192.168.70.120	Unit 0	4p3cmm, Bay 1	On	Compliant	DEFAULT-2015-04-04 ▾
Boot ROM		4p3cmm, Bay 1		7.8.7.0	
Main Application 1 (Active)		4p3cmm, Bay 1		7.8.7.0	
Main Application 2 (Not Act)		4p3cmm, Bay 1		7.7.7.15	
DC - lower node 10.240.61.47	Unit 0	4p3cmm, Bay 2	Off	No Compliance Pi	No applicable policies ▾
CC x222 Upper 10.240.61.48	Unit 0	4p3cmm, Bay 2	On	No Compliance Pi	No applicable policies ▾

- Select one or more endpoints and components to which firmware updates are to be applied.
- Click the Perform updates icon () to display the Assign Policy dialog. The Update Summary dialog is displayed.

Update Summary

Select your Update Rule and review your updates. Then click Perform Update.

* Update Rule: Stop all updates on error ▾

* Activation Rule: Immediate activation ▾

☒ Attempt to update components already in compliance

| All Actions ▾ | Filter

System	Chassis / Bay	Installed Version	Compliance Target
IO Module 03 10.240.63.245	4p3cmm, Bay 3		ibm_fw_scs_w_en2092-7.8.7... 7.8.7.0 / BRFP (2014-09-25)
Boot ROM	4p3cmm, Bay 3	WMP00019	
Main Application 1	4p3cmm, Bay 3	WMP00019	
Main Application 2	4p3cmm, Bay 3	WMP00019	

Simulate Update Perform Update Close

- Select a rule that specifies what to do when an error occurs during this firmware-update operation:

Stop all updates on error

Stop making updates for all selected endpoints.

Continue on error

Continue making updates for the other devices in the endpoint where the error occurs, and continue making updates for all other endpoints.

Continue to next system on error

Stop making updates to all firmware in the endpoint where the error occurs, but continue making updates for all other endpoints.

5. Select an activation rule:

Immediate activation


During the update operation, the endpoint might be restarted automatically a number of times until the entire update operation is complete. Be sure to quiesce all applications on the endpoint before proceeding.

Delayed activation

Some update operations are performed, but not all. Endpoints must be restarted manually to continue the update process. Additional restarts are then performed until the update operation completes.

6. Optionally, select **Attempt to update components already in compliance** to update firmware on the selected components even if the firmware level is up to date.
7. Click **Perform Update**.

What to do next

You can cancel an update that is being applied to an endpoint by selecting the endpoint and clicking the Cancel Update icon ().

You can monitor the status of the update process from the Jobs log in the Lenovo XClarity Administrator. For more information about the job, see the Lenovo XClarity Administrator help page.

Identifying endpoints that are not compliant

If a compliance policy has been assigned to a managed endpoint, you can determine whether the firmware on that endpoint is compliant with the policy.


About this task

To determine whether the firmware on an endpoint is compliant with its assigned compliance policy, follow these steps.

Procedure

1. Click **Firmware Updates > Apply / Activate** in the menu bar. The Firmware Updates: Apply/Activate dialog is displayed.

Firmware Updates: Apply / Activate

 To update firmware for a device, assign a compliance policy and select Perform Updates.



All Actions

Critical Release Information

Show: All Systems

Filter

System	Rack Name / Unit	Chassis / Bay	Power	Installed Version	Assigned Compliance Policy
<div>4p3cmm</div> <div>10.240.61.45</div>	Unit 0	4p3cmm, Bay 1	<div>On</div>	<div>2.50.0 / 2PET062</div>	<div>DEFAULT-2015-04-04</div>
<div>IO Module 01</div> <div>192.168.70.120</div>	Unit 0	4p3cmm, Bay 1	<div>On</div>	<div>Compliant</div>	<div>DEFAULT-2015-04-04</div>
<div>Boot ROM</div>		4p3cmm, Bay 1		<div>7.8.7.0</div>	
<div>Main Application 1 (Active)</div>		4p3cmm, Bay 1		<div>7.8.7.0</div>	
<div>Main Application 2 (Not Act</div>		4p3cmm, Bay 1		<div>7.7.7.15</div>	
<div>DC - lower node</div> <div>10.240.61.47</div>	Unit 0	4p3cmm, Bay 2	<div>Off</div>	<div>No Compliance Pi</div>	<div>No applicable policies</div>
<div>CC x222 Upper</div> <div>10.240.61.48</div>	Unit 0	4p3cmm, Bay 2	<div>On</div>	<div>No Compliance Pi</div>	<div>No applicable policies</div>

- Check the Installed Version column for the endpoint you are interested in. The Installed Version column contains one of the following values:

Firmware version

The firmware version installed on the endpoint is compliant with the assigned policy.

Not Compliant

The firmware installed on the endpoint is not compliant with the assigned policy.

No Compliance Policy Set

No compliance policy is assigned for the endpoint.

You can click the Refresh icon () to refresh the content in the Installed Version column.

Chapter 7. Using Lenovo XClarity Integrator for VMware vCenter with vSphere Client

The topics in this section describe how to use Lenovo XClarity Integrator for VMware vCenter with vSphere Client.

Lenovo XClarity Integrator for VMware vCenter with vSphere Client provides the following functions:

- Dashboard
- Dynamic System Analysis
- Firmware Updates
- Power Metric
- Advanced System Settings

You can navigate to each of these functions from the navigation pane.

The Dashboard

The Dashboard provides an overview of the host status.

The Dashboard displays summaries of:

- System Information
- System Health
- Power Throttling
- Predictive Failure Alerts

System Information Summary

The System Information Summary contains information about a managed host.

The System Information Summary provides the following information:

- Manufacturer
- Model
- Serial number
- Operating system
- Operating system version
- Last boot

System Health, Power Throttling, and Predictive Failure Alert summaries

These summaries provide an overview of the system running status (health messages from the host), the Power Throttling status, and the PFA status.

All of the messages are grouped into three categories by severity.

Critical events:

Events that can or have already caused a host failure that requires your immediate attention.

Attention events:

Events that indicate that there is something abnormal on the host but the abnormality will not cause immediate failure of the host.

Information Events:

Events that indicate something happened on the host that will not prevent the host running.

Each of the summary categories is grouped in an accordion box. The title indicates how many events are in the category. Because the events are effective for a limited period, a maximum of 20 events are shown in each category; however, you can check all power throttling events on the Power Metric page and all of the PFA indication events on the Predictive Failure Management page.

If you click on the title, the box extends and contains the following information:

- Message
- Event time
- MessageID

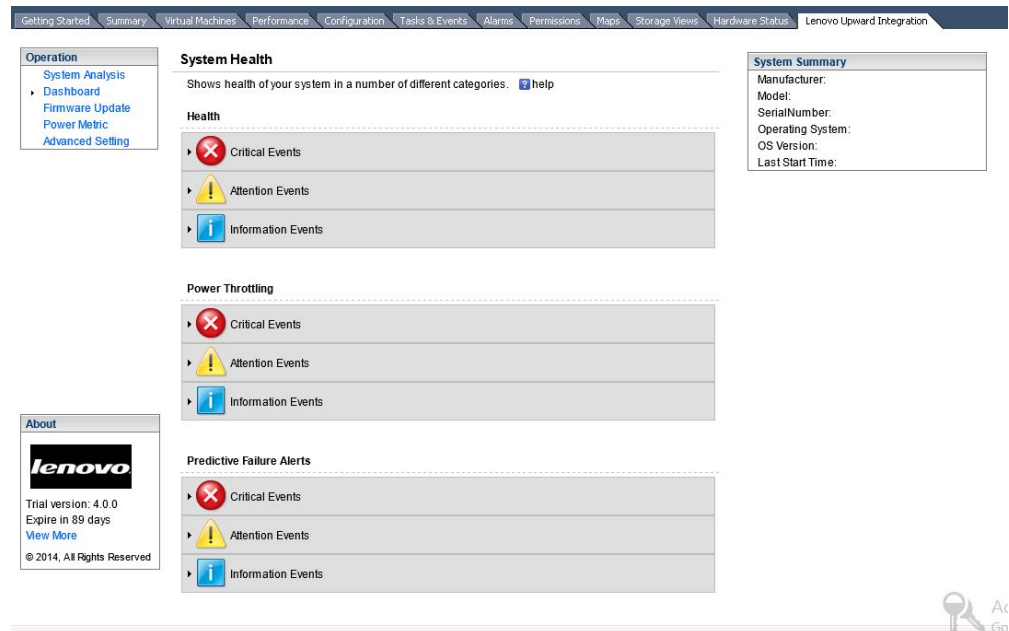


Figure 35. System Health Summary Dashboard view

Working with Dynamic System Analysis

The Dynamic System Analysis function collects and analyzes system information to aid in diagnosing system problems.

Dynamic System Analysis collects information about the following aspects of a system:

- System configuration
- Installed applications and hot fixes
- Device drivers and system services
- Network interfaces and settings

- Performance data and running process details
- Hardware inventory, including PCI information
- Vital product data and firmware information
- SCSI device sense data
- ServeRAID configuration
- Application, system, security, ServeRAID, and service processor system event logs

The DSA plug-in provides functions inherited from the standalone version of Dynamic System Analysis and provides an organized view of the following DSA functions:

- Launch system inventory collection
- View and manage system inventory history
- View the categorized system inventory results

Firmware updates

The Firmware Updates function applies the latest UpdateXpress System Packs (UXSPs) and individual updates to your ESXi system. UpdateXpress System Packs contain updates for Windows and Linux firmware.

You can use Firmware Updates to obtain and deploy UpdateXpress System Packs firmware updates and individual firmware updates with these functions:

Acquire Updates:

Downloads the UpdateXpress System Pack and individual updates for supported server types from a remote location such as Lenovo support

Compare and Update:

Performs the following actions:

- Inventories the system on which the update is being performed
- Queries the update directory for a list of applicable update packages
- Compares the inventory to the applicable update list
- Recommends a set of updates to apply
- Deploys the updates to the system

Prerequisites

This procedure describes how to complete the necessary prerequisites for updating firmware.

Before you begin

Complete these steps before updating the firmware.

Procedure

1. Enable **Commands** on the USB interface in uEFI by changing the uEFI settings.
2. Reboot the host.

Firmware update scenarios

The topics in this section describe two scenarios for firmware updates:

- Updating a remote server from the Lenovo website
- Updating a remote server from a local directory

Updating a remote server from the Lenovo website

The firmware update function can update a remote ESXi host with either (UXSPs) or individual updates that are acquired from the Lenovo website.

About this task

Perform the following steps to update a remote server from the Lenovo website.

Procedure

1. Click **Firm Update** in the navigation pane on the left.
2. On the Updates page, select **Check the Lenovo web site**.

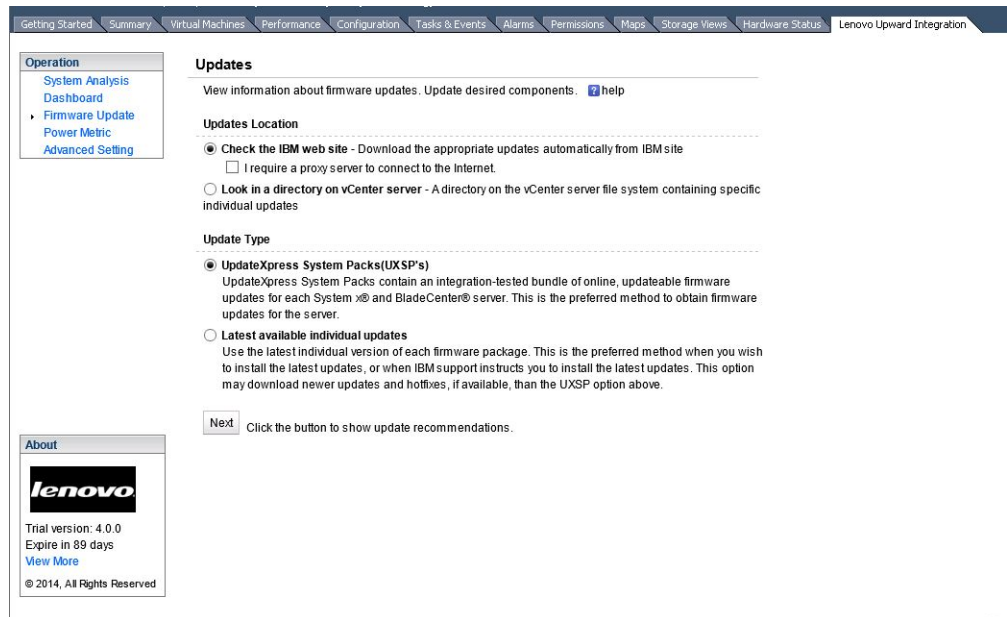


Figure 36. Updates page

3. On the HTTP Proxy Setting page, specify the proxy information if required.
4. On the Update Type page, select an update type:
 - **UpdateXpress System Packs (UXSPs)** contain an integration-tested bundle of online, updatable firmware and device driver updates for each system. This is the preferred method for obtaining firmware updates for the server.
 - **Individual updates** use the latest individual version of each firmware and device driver package. This is the preferred method when you want to install the latest updates, or when Lenovo support instructs you to install the latest updates. This option can download newer updates and hotfixes, if available, than the UXSP option.
5. Click **Next**. The Update Recommendation page is displayed.

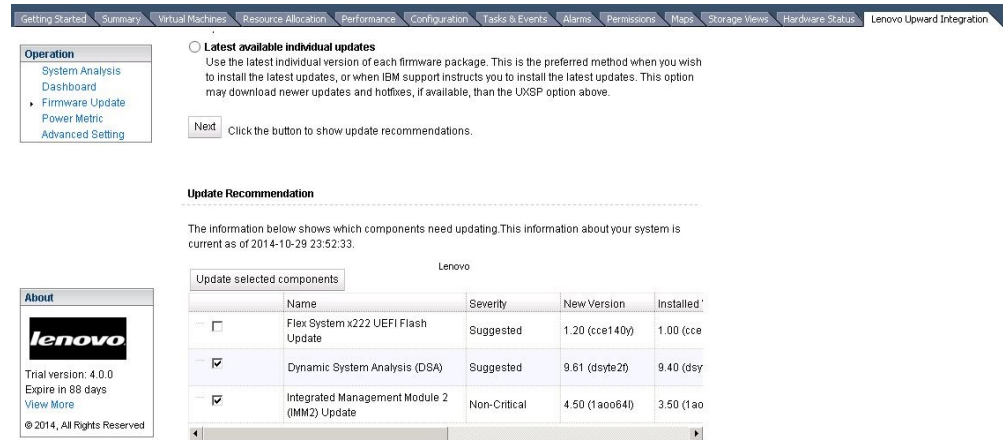


Figure 37. Update Recommendation example

- On the Update Recommendation page, make the required changes and then click **Update**.

The plug-in acquires the updates from the Lenovo website. The progress bar indicates that the installer is processing, and shows the percentage of progress completed. If necessary, click **Cancel** to stop the download. Once you click **Cancel**, the **Cancel** button is replaced with the **Begin** button. Use the **Begin** button to resume the download.

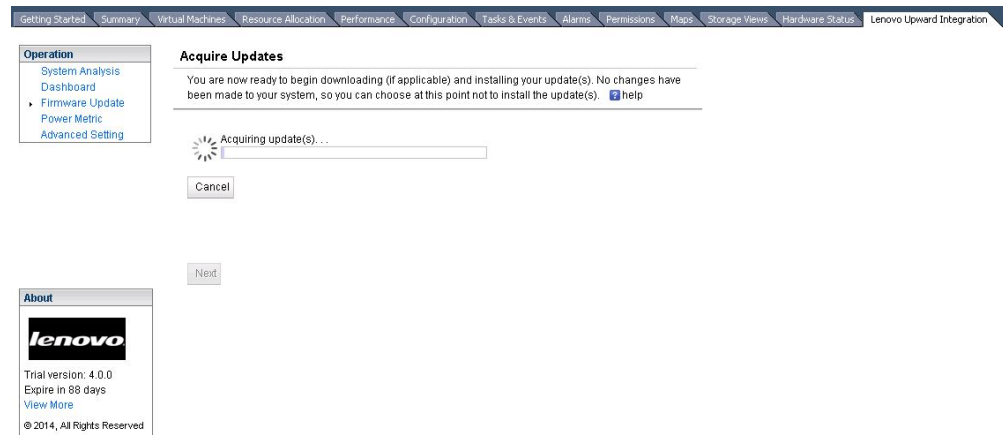


Figure 38. Acquire Updates

- After all the selected downloads are complete, click **Next**.

On the ESXi credentials page, enter the administrative account information of the target ESXi, and click **Next**.

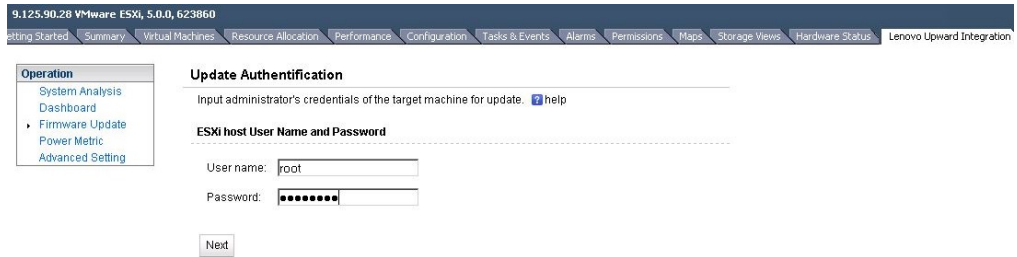


Figure 39. Update Authentication page

The Update Execution page is displayed while the updates are installing to the target host. The progress bar indicates that the installer is processing the updates and also shows the percentage of progress completed.

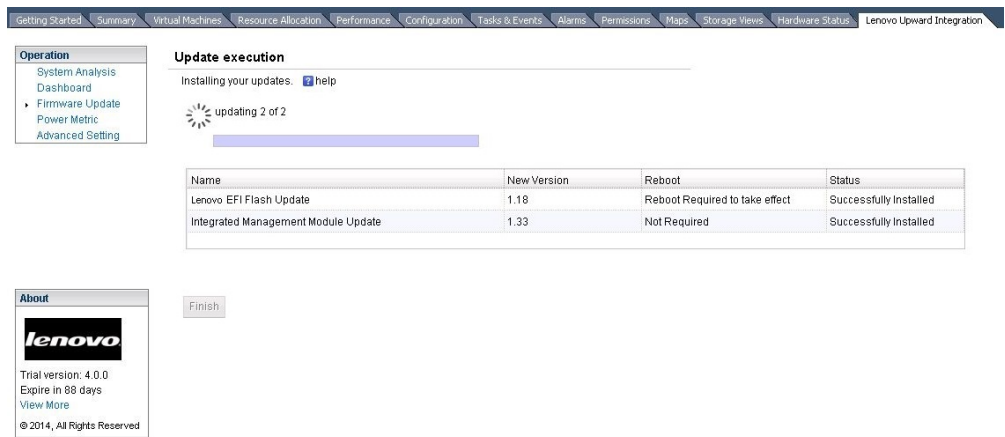


Figure 40. Update execution page

8. After the updates are applied, click **Finish** to complete the update.

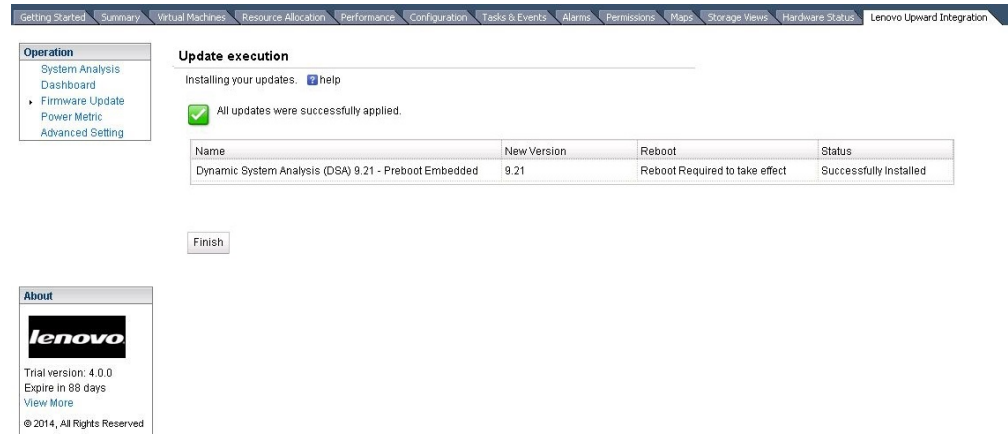


Figure 41. All updates successfully applied

Updating a remote server from a local directory

The firmware update function can update a remote ESXi host with either UpdateXpress System Packs (UXSPs) or individual updates that are stored in a directory (repository) on the vCenter Server.

Procedure

1. Click **Update** in the navigation pane on the left.
2. On the Updates page, select **Look in a directory on vCenter server**. A gray text box displays the absolute path of the directory. Once the plug-in is installed, it is a fixed directory. You must save all updates there manually, before the update.
3. On the Update Type page, select the type of updates you want to acquire.
4. Click **Next**. The Update Recommendation page is displayed.
5. On the Update Recommendation page, make the required changes, and then click **Update**.
6. On the ESXi credential page, enter the administrative account information of the target ESXi host, and then click **Next**.

The Update Execution page is displayed while updates are installed on the target host. The progress bar indicates the installer is processing, and shows the percentage of progress completed.

7. After the updates are applied, click **Finish** to complete the updates.

Working with Power Metric

Power Metric provides information about power usage, thermal and fan speed values, and the trend for a managed host. This information is helpful in determining whether a workload should be reassigned. The Power Capping feature sets the upper limit value of power management. The Power Throttling feature allows you to receive warning or critical alerts when power consumption exceeds the values you set.

About this task

This procedure describes how to enable and disable Power Metric on a host. The **Enable** button is visible when Power Metric is not enabled on a host.

Procedure

- To enable Power Metric, complete these steps:
 - Click **Enable**. The Input credentials dialog box is displayed.

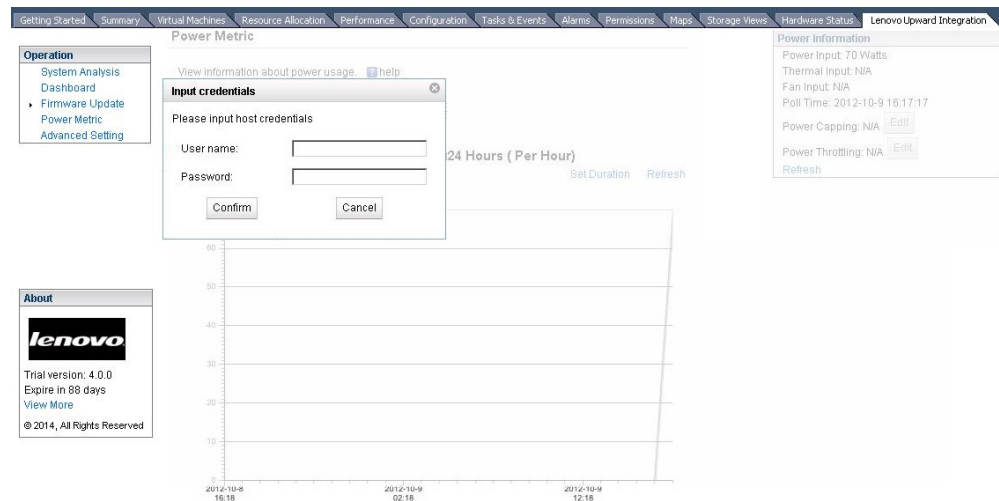


Figure 42. Enabling Power Metric

- Enter the host credentials and click **Confirm**.
 - Enable **Commands** on the USB Interface in uEFI by changing the uEFI settings before booting the OS.
- To disable Power Metric, complete these steps:
 - Click **Disable**.
 - Click **OK** to confirm disabling Power Metric.

Viewing power usage, thermal history, and fan summary information

If a host is being monitored, you can view the current power usage, thermal history, and fan summary information as a summary or as a detailed chart.

About this task

This task is performed on the Power Metric page. These steps describe how to view and use the latest poll reading summary and detailed charts.

Procedure

- In the Information window on the right, click **Refresh** to see the latest poll reading summary for the power usage, thermal history, and fan summary.
 - To add or change the Power Capping value, click **Edit**. For more information about Power Capping, see “Power Capping” on page 72.
 - To add or change the Power Throttling value, click **Edit**. For more information about Power Throttling, see “Power Throttling” on page 72.

- Select a chart to view. The default duration for each of the charts is 1-hour intervals during the last 24-hour period.

The Power Usage chart provides an example of power usage for the last 24 hours on an hourly basis.

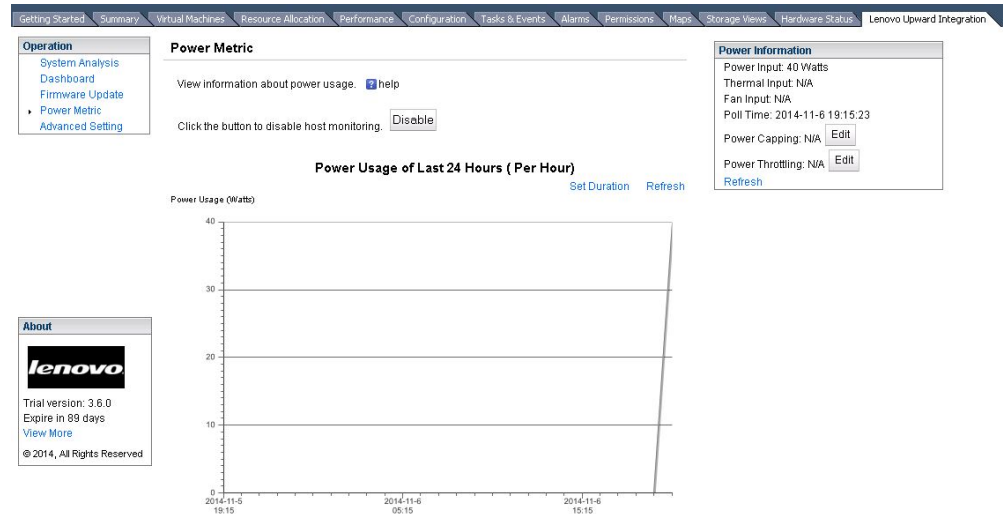


Figure 43. Power Usage Chart

1. To view the power usage history data for a different time period, click **Set Duration**. Select the required duration and interval.
2. Click **Refresh** to see the latest information or for the defined duration interval.

The Thermal History chart provides an example of information for the last four hours in 5-minute intervals.

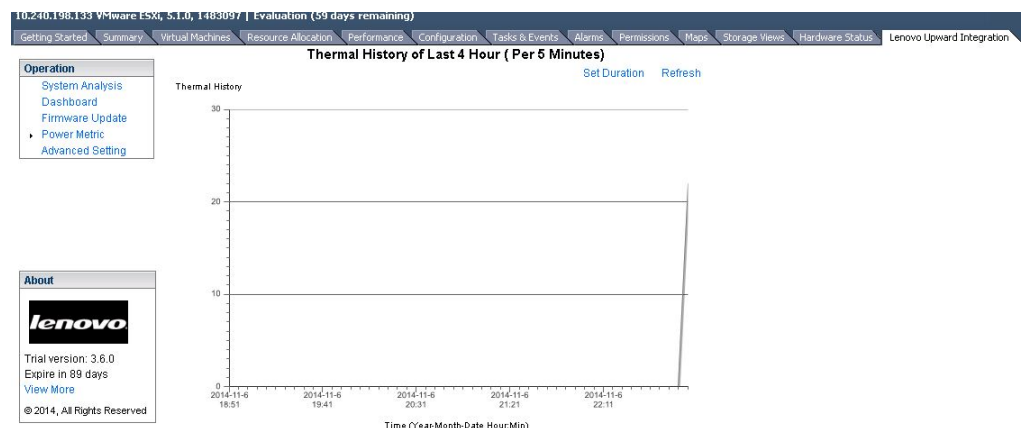


Figure 44. Thermal History chart

The Fan History chart provides an example of fan history for the last 24 hours on an hourly basis.

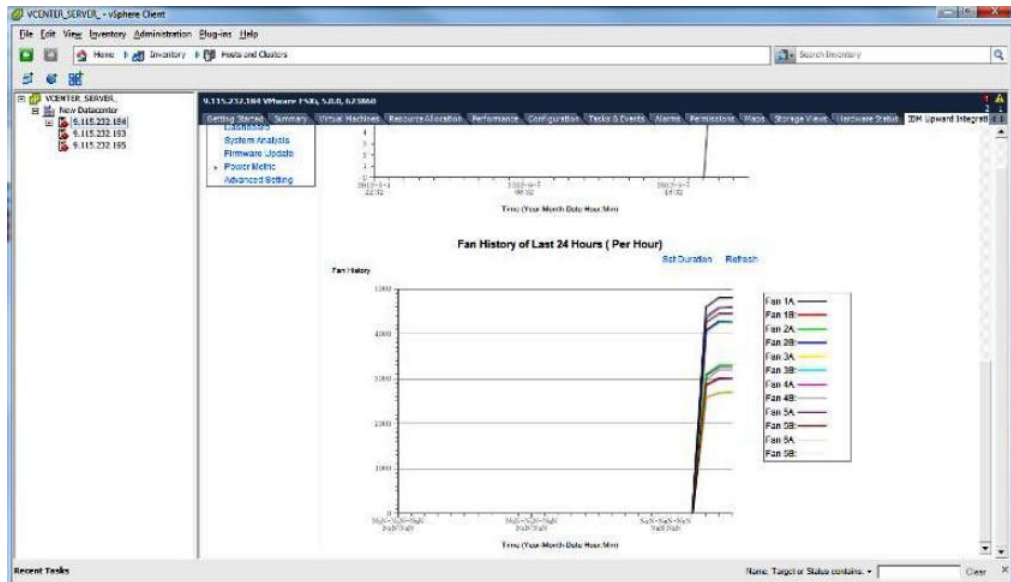


Figure 45. Fan History chart

Power Capping

The Power Capping feature allows you to allocate less power and cooling to a system. This feature can help lower datacenter infrastructure costs and potentially allow more servers to be put into an existing infrastructure. By setting a Power Capping value, you can ensure that system power consumption stays at or below the value defined by the setting.

The Power Capping value is the value you set for a rack or blade server that will be capped by the firmware, if the firmware supports capping. The Power Capping value is persistent across power cycles for both rack and blade servers.

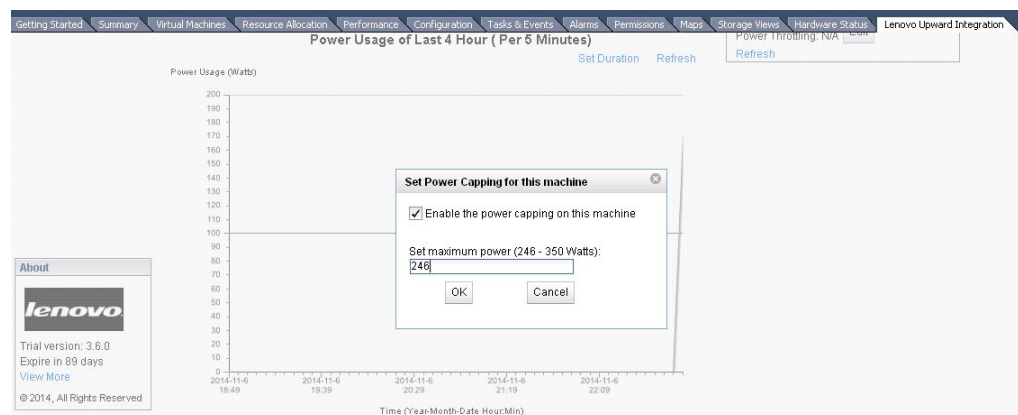


Figure 46. Set Power Capping

Power Throttling

The Power Throttling feature provides alerts when power consumption exceeds the value you set. You can set two different Power Throttling values, one for a warning and one for a critical alert.

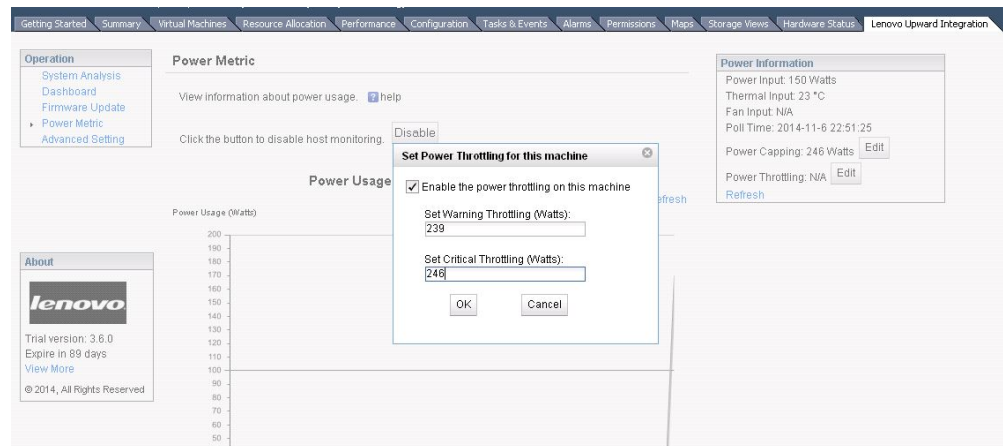


Figure 47. Set Power Throttling

When power consumption exceeds a defined Power Throttling value, Lenovo XClarity Integrator for VMware vCenter with vSphere Client receives a throttling event, which is then displayed in the Power Throttling Indications table.

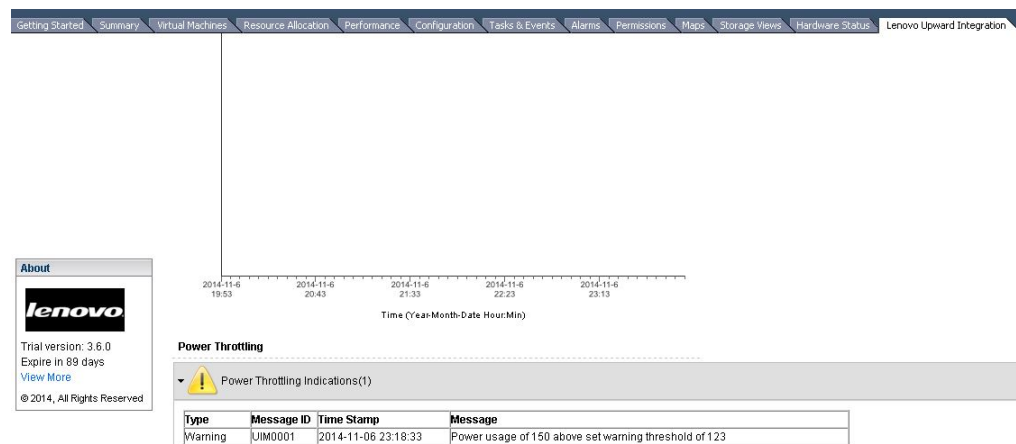


Figure 48. Power Throttling Indications

Working with Advanced System Settings

The Advanced System Settings page shows the current system settings on the host. This includes settings for IMM, uEFI, and the boot order of a host.

Viewing Advanced System Settings

This topic describes how to view Advanced System Settings on the host.

Settings are grouped into three categories represented by the following three tabs:

- IMM Settings
- uEFI Settings
- Boot Order Settings

Settings in each tab are further categorized into expandable subsections. You can easily find a setting by expanding the subsection. On the initial view, each subsection provides a description of the field functions. Scroll down to view all of the fields.

To view a setting, click to expand and display all of the settings with a subsection.

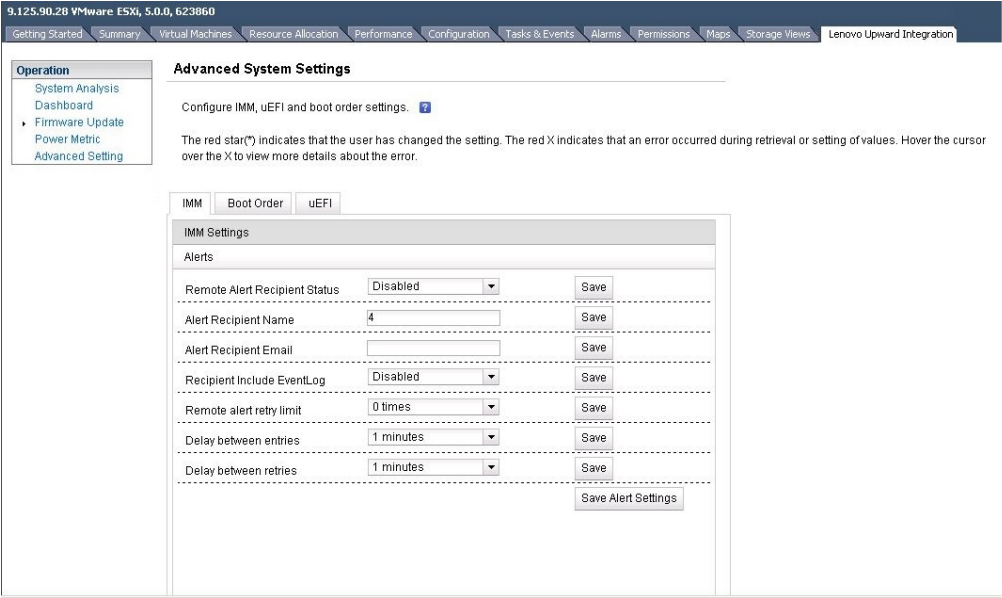


Figure 49. Viewing Advanced System Settings

Some settings, such as uEFI settings, are only supported on a certain machine type or firmware version. If your host does not support a setting, the following symbol is displayed to indicate this setting is currently not supported on your host:



Figure 50. Setting not supported symbol

Changing Advanced System Settings

This procedure describes how to change Advanced System Settings on the host.

About this task

The following list provides an example of the different types of settings and how to change these settings. The manner in which each setting is changed varies.

- *text string*: Place the cursor on the text string to view the type of required input.
- *selection type*: Select the value from the list.
- *password*: Enter the password and then re-enter the password to confirm the new password. Click **Clear the password** to clear the password field.

Note: **Save** and **Clear the password** are executed immediately on the managed endpoint.

- *boot order*: The left column shows the current boot order, and the right column shows the optional device. To change the order, you can move a boot order option up or down and between the two columns, by clicking the corresponding button.

Procedure

- To change an Advanced System Setting, enter the new value and click **Save**. The change is executed on the endpoint, and the following symbol is displayed when the action is complete.



Figure 51. Setting change is successful symbol

If there is a problem with changing the setting, the following symbol is displayed:



Figure 52. Setting change is not successful symbol

To view detailed information about why the setting change failed, place the cursor over the symbol.

- You can also click **Save xxx Settings** in each section, to save all the settings contained within that section. This will not impact settings in other sections. The setting result for each setting will show up as a single setting result.
- To save all of the settings in the IMM section, click **Save Alert Settings**. The following image provides an example of the Alert section for IMM Settings.

9.125.90.28 VMware ESXi, 5.0.0, 623860

Getting Started | Summary | Virtual Machines | Resource Allocation | Performance | Configuration | Tasks & Events | Alarms | Permissions | Maps | Storage Views | Lenovo Upward Integration

Operation

- System Analysis
- Dashboard
- Firmware Update
- Power Metric
- Advanced Setting

Advanced System Settings

Configure IMM, uEFI and boot order settings. ⓘ

The red star(*) indicates that the user has changed the setting. The red X indicates that an error occurred during retrieval or setting of values. Hover the cursor over the X to view more details about the error.

IMM | Boot Order | uEFI

IMM Settings

Alerts

Remote Alert Recipient Status	Disabled	Save
Alert Recipient Name	4	Save
Alert Recipient Email		Save
Recipient Include EventLog	Enabled	Save
Remote alert retry limit	0 times	Save
Delay between entries	1 minutes	Save
Delay between retries	1 minutes	Save

Save Alert Settings

Figure 53. Changing Advanced System Settings

Appendix A. Troubleshooting

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

Help information

When you click on a question mark icon, an Online help page is displayed for that item.

The first time you access online help, you are asked to trust the certification of the site. Click **Yes** to trust the certification.

Finding the vCenter plug-in version

This procedure describes how to find the vCenter plug-in version.

Procedure

1. In the vCenter interface, click **Plug-in > Manage Plug-in**.
2. Locate **Lenovo XClarity Integrator for VMware vCenter**. The version column displays the version of the installed plug-in.

Installed version field shows Undetected in firmware updates

The **Installed version** field in the Firmware Update Recommendation table indicates Undetected.

About this task

If the **Installed version** field displays Undetected, try restarting the IMM and the ESXi host.

IMM Discovery failure

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

About this task

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

Procedure

1. Verify that the network connection between vCenter and the host is working.
2. Try the discovery process again by clicking **Discovery**.

Cannot display a chassis map or a configuration pattern page because of a certificate issue

This topic will help you fix certification errors when launching a chassis map or a configuration pattern page.

About this task

If the page is blocked by the browser with a certificate is not trusted message, complete the steps for your browser.

Procedure

- For Internet Explorer:
 1. Navigate to the **Lenovo XClarity Integrator** tab located below the **Host Manage** tab, and click the **Help** tab.
 2. Click the **Download Certification** link to download the certificate.
 3. Double-click the ca.cer file in **General** tab and click **Install Certificate..**
 4. Click **Next**.
 5. From the **Certificate Store** page, select **Place all certificates in the following store**, and click **Browse...**
 6. Select **Trusted Root Certificate Authorities**, and click **OK**.
 7. Click **Finish**.
- For Firefox:
 1. In an open browser, click **Firefox > Options > Advanced > Certificates > View Certificates > Servers > Add Exception...**
 2. In the **Location** field, enter the fully-qualified domain name or the IP address of the host where you installed Lenovo XClarity Integrator..
 3. Click **Get Certificate**.
 4. Click **Confirm Security Exception** and then refresh your browser.

Appendix B. Accessibility features

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

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

The *Lenovo XClarity Integrator for VMware vCenter, Version 4.1 Installation and User's Guide* supports the accessibility features of the system-management software in which they are integrated. Refer to your system management software documentation for specific information about accessibility features and keyboard navigation.

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

You can view the publications for Lenovo XClarity Integrator for VMware vCenter, Version 4.1 in Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader. Publications are available for download from the product website: [Lenovo XClarity Integrator for VMware vCenter, v4.1 - Lenovo x86 servers](#) :

Lenovo and accessibility

See the [Lenovo Accessibility website](#) for more information about the commitment that Lenovo has to accessibility.

Notices

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

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

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

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

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

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

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

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

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

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

Trademarks

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

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

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

Linux is a registered trademark of Linus Torvalds.

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

Important notes

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

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Index

A

about this publication ix
accessibility features 79
activating the premium features 9
Adobe Acrobat Reader xi
Advanced Settings Utility 2
Advanced System Settings 73
applying firmware updates 65

B

Blade System 4
boot order 73
Boot Order Settings 73

C

changing advanced system settings 74
changing advanced system settings on
the vSphere Web Client 47
compliance policies 58
compliance, firmware
 See firmware compliance
configure Lenovo XClarity Integrator 9
conventions and terminology ix

D

Dashboard 63
deploying configuration patterns 44
disabling Power Metric 70
disk space requirements 6
Dynamic System Analysis 1, 64

E

enabling Power Metric 70
endpoints 61
ESXi 3
ESXi CIMOM port 6

F

Fan Summary 70
fan usage history 42
finding the vCenter plug-in version 77
firmware compliance
 activating updates 59
 applying updates 59
 assigning policies 58
 description 58
 identifying noncompliant
 endpoints 61
firmware update scenarios for the
vSphere Web Client 38
firmware updates 1, 59, 65
 Installed version field 77

H

hardware requirements 6
Help Information 77

I

IMM 73
IMM Discovery failure 77, 78
IMM discovery process 77, 78
IMM port 6
IMM Settings 73
important notices 82
Individual Updates (UXSP) for the
vSphere Web Client 40
information resources xi
Installed version field 77
installing Lenovo XClarity Integrator for
VMware vCenter 3, 7
installing the Lenovo License Tool 9

L

launching system inventory for the
vSphere Web Client 34
Lenovo UpdateXpress System Packs 1
Lenovo XClarity Integrator for VMware
vCenter 1
Lenovo XClarity Integrator for VMware
vCenter site xi
LXCI database port 6
LXCI Unified Service port 6

M

managed host 63
managing hardware events 31
memory requirements 6

N

notes, important 82
notices 81

O

Online help 77

P

pdf files xi
policies 58
port requirements 6
Power Capping 72
Power Metric 1, 70
Power Throttling 73
Power Usage 70
power usage history 42
predictive failure management 2

Prerequisites 31, 65
prerequisites for updating firmware on
vSphere Web Client 36
processor requirements 6

R

Recommended Updates (UXSP) for the
vSphere Web Client 38
required hardware 6

S

saving pdf files xi
selecting update preferences on the
vSphere Web Client 36
ServerProven websites xii
set Power Throttling on vSphere Web
Client 42
setting Power Capping on vSphere Web
Client 41
supported hardware 4
supported operating systems 3
System Health Summary 63
System Information Summary 63
System Management with Lenovo
XClarity Solution xii
System Overview on vSphere Web
Client 34
system requirements for Lenovo XClarity
Integrator for VMware vCenter 3
System settings 44
System x 4

T

technical support portal xi
Thermal History 70
thermal usage history 42
trademarks 82
Troubleshooting 77

U

uEFI 73
uEFI Settings 73
updating a remote server from a local
directory 69
updating a remote server from the
Lenovo website 66
USB interface 65
using Lenovo XClarity Integrator for
VMware vCenter with vSphere Web
Client 11
Using Lenovo XClarity Integrator with
VMware vCenter 63
UXSP 1

V

- vCenter xii
- viewing Action History table 30
- viewing advanced system settings 73
- viewing advanced system settings on the vSphere Web Client 45
- viewing Predictive Failure Events on the vSphere Web Client 30
- viewing the categorized analysis results for vSphere Web Client 35
- viewing the Fan Summary chart 70
- viewing the Power Usage chart 70
- viewing the Thermal History chart 70
- VMware xii, 11, 63
- VMware vCenter 4.1 3
- VMware vCenter 5.0 (U1) 3
- VMware vCenter Server 3
- vSphere Web Client 11, 42

W

- Web resources xi
- working with Alerts and Events on vSphere Web Client 35
- working with Chassis Map 34
- working with Configuration 44
- working with Dynamic System Analysis 64
- working with Firmware Updates on vSphere Web Client 36
- working with Power Metric 70
- working with System Analysis on vSphere Web Client 33
- working with the Dashboard 63
- working with the Power Metric on the vSphere Web Client 40



Printed in USA