Lenovo XClarity Administrator User's Guide

Version 3.6.0

Eighth Edition (June 2022)

© Copyright Lenovo 2015, 2022.
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.

Contents

Tables v

Summary of changes vii

Chapter 1. Lenovo XClarity Administrator Overview 1

Logging in to XClarity Administrator 5
User interface tips and techniques 9
Using the Lenovo XClarity Mobile app 10

Chapter 2. Administering Lenovo XClarity Administrator 17

Managing authentication and authorization 17
- Managing the authentication server 17
- Managing user accounts 32
- Managing stored credentials 38
- Managing roles and role groups. 39
- Managing access to devices 56

Implementing a secure environment 59
- Changing the user-account security settings 60
- Configuring cryptography settings. 63
- Working with security certificates 65
- Enabling encapsulation 75
- Implementing NIST SP 800-131A compliance. 76

Using VMware Tools 78
Configuring network access 78
Setting the date and time 84
Setting inventory preferences 86
Setting threshold preferences for generating alerts and events. 87
Setting up automatic problem notification to Lenovo Support (Call Home) 87
Setting up automatic problem notification to a preferred service provider 92
Connecting XClarity Administrator as a hub to the TruScale portal 94
Backing up, restoring, and migrating system data and settings 95
- Backing up Lenovo XClarity Administrator. . . 95
- Restoring Lenovo XClarity Administrator . . . 96
- Migrating system data and settings to another XClarity Administrator instance 98

Managing disk space 100
Managing remote shares 102
Changing the language of the user interface . . . 103
Shutting down XClarity Administrator 104
Restarting XClarity Administrator 104

Chapter 3. Monitoring devices and activities 109

Viewing a summary of your environment 109
- Viewing a summary of your hardware status 110
- Viewing a summary of your provisioning status 111
- Viewing a summary of Lenovo XClarity Administrator activity 113

Monitoring system resources 113
Monitoring trends in provisioning status 115
Monitoring historical metrics 116
Placing devices in maintenance mode 117
Working with alerts 118
- Viewing active alerts 118
- Excluding alerts 122
- Resolving an alert 123
- Acknowledging alerts. 124

Working with events 124
- Monitoring events in the event log 124
- Monitoring events in the audit log 126
- Resolving an event. 128
- Excluding events 128
- Forwarding events 129

Working with jobs 161
- Monitoring jobs 161
- Scheduling jobs 164
- Adding a resolution and comments to a job 167

Viewing relationships between jobs and events . . 167

Chapter 4. Management considerations 171

Chapter 5. Managing resource groups 173

Viewing the status of devices in a resource group. 173
Viewing the members of a resource group 175
Creating a dynamic resource group 178
Creating a static resource group 180
Removing a resource group 181
Modifying resource-group properties 182

Chapter 6. Managing racks 183

Viewing the status of devices in a rack 187
Removing a rack 189

© Copyright Lenovo 2015, 2022

Chapter 7. Managing chassis 191
Viewing the status of a managed chassis 200
Viewing the details of a managed chassis. 201
Backing up and restoring CMM-configuration data 204
Launching the CMM web interface for a chassis 204
Modifying the system properties for a chassis . . . 205
Modifying the management-IP settings for a chassis 205
Configuring CMM failover 206
Restarting a CMM 207
Virtually reseating a CMM 208
Resolving expired or invalid stored credentials for a chassis 209
Recovering management with a CMM after a management server failure 210
Unmanaging a chassis 211
Recovering a chassis that was not unmanaged correctly 212

Chapter 8. Managing servers 215
Viewing the status of a managed server 225
Viewing the details of a managed server 228
Backing up and restoring server-configuration data 233
Securely erasing drive data 233
Using remote control. 235
Using remote control to manage ThinkSystem or ThinkAgile servers 235
Using remote control to manage ThinkServer and NeXtScale sd350 M5 servers 236
Using remote control to manage Converged, Flex System, NeXtScale, and System x servers 237
Managing access to operating-systems on managed servers 247
Viewing Features on Demand keys 249
Managing energy and temperature 250
Powering on and off a server. 251
Virtually reseating a server in a Flex System chassis 252
Launching the management controller interface for a server 252
Modifying the system properties for a server . . . 254
Resolving expired or invalid stored credentials for a server 254
Recovering a failed server after deploying a server pattern 255
Recovering boot settings after server pattern deployment 256
Recovering rack or tower server management after a management server failure 257
Recovering rack or tower server management after a management server failure by force management 257
Recovering a System x or NeXtScale M4 server that was not unmanaged correctly by using the management controller 257
Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by resetting the management controller 258
Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by using cimcli. 259
Recovering ThinkServer server management after a management server failure by using the management controller interface 261
Unmanaging a rack or tower server 261
Recovering a rack or tower server that was not unmanaged correctly 262

Chapter 9. Managing storage devices 269
Storage management considerations 272
Viewing the status of storage devices 273
Viewing the details of a storage device 275
Backing up and restoring storage-configuration data 278
Powering on and off a storage device 278
Virtually reseating storage controllers in a Flex System storage device 279
Launching the management controller interface for a storage device 279
Modifying the system properties for a storage device 280
Recovering management of a rack storage device after a management server failure. 281
Recovering management of a Lenovo ThinkSystem DE Series storage device after a management server failure 281
Unmanaging a storage device 282
Recovering a rack storage device that was not unmanaged correctly 282

Chapter 10. Managing switches . . .283
Switch management considerations. 289
Viewing the status of switches 290
Viewing the details of a switch 293
Powering on and off a switch 296
Enabling and disabling switch ports 296
Backing up and restoring switch-configuration data 297
Backing up switch-configuration data 298
Restoring switch-configuration data 299

Exporting and importing switch-configuration files . . . 301
Launching the management controller interface for a switch . . . 302
Launching a remote SSH session for a switch . . . 303
Modifying the system properties for a switch . . . 304
Resolving expired or invalid stored credentials for a switch . . . 305
Recovering management with a switch after a management server failure . . . 305
Unmanaging a switch . . . 306
Recovering a switch that was not unmanaged correctly . . . 307

Chapter 11. Configuring servers using configuration patterns . . . 309
Configuration considerations . . . 311
Defining address pools . . . 312
Creating an IP address pool . . . 314
Creating an Ethernet address pool . . . 315
Creating a Fibre Channel address pool . . . 317
Working with server patterns . . . 322
Creating a server pattern . . . 324
Deploying a server pattern to a server . . . 348
Modifying a server pattern . . . 349
Exporting and importing server and category patterns . . . 350
Working with server profiles . . . 351
Activating a server profile . . . 352
Deactivating a server profile . . . 353
Deleting a server profile . . . 355
Working with placeholder chassis . . . 355
Creating a placeholder chassis . . . 355
Deploying a server pattern to a placeholder chassis . . . 356
Deploying a placeholder chassis . . . 357
Resetting storage adapters to default values . . . 358
Configuring memory . . . 360

Chapter 12. Configuring switches using configuration templates . . . 361
Setting default server-configuration preferences . . . 362
Creating a switch-configuration template . . . 363
Defining VLAN port-membership settings . . . 365
Defining VLAN properties . . . 366
Removing VLAN settings . . . 367
Deleting VLANs . . . 367
Defining port-channel basic settings . . . 368
Defining port-channel advanced settings . . . 369
Deleting port channels . . . 369
Defining general switch settings . . . 370
Defining global L2 interface settings . . . 370
Defining peer VLAG settings . . . 371
Defining VLAG instance settings . . . 372
Defining VLAG advanced settings . . . 372
Deleting a VLAG instance . . . 373
Defining a spine-leaf topology . . . 373
Deploying switch-configuration templates to a target switch . . . 374
Viewing switch-configuration deployment history . . . 375

Chapter 13. Updating firmware on managed devices . . . 377
Firmware-update considerations . . . 384
Managing the firmware-updates repository . . . 390
Using a remote repository for firmware updates . . . 394
Refreshing the product catalog . . . 395
Downloading firmware updates . . . 396
Exporting and importing firmware updates . . . 403
Deleting firmware updates . . . 404
Creating and assigning firmware-compliance policies . . . 405
Identifying devices that are not compliant . . . 410
Configuring global firmware-update settings . . . 410
Applying and activating firmware updates . . . 412
Applying bundled firmware updates using compliance policies . . . 413
Applying selected firmware updates using compliance policies . . . 417
Applying selected firmware updates without using compliance policies . . . 423

Chapter 14. Updating Windows device drivers on managed servers . . . 431
OS device-driver update considerations . . . 433
Managing the OS device-drivers repository . . . 435
Refreshing the OS device-driver catalog . . . 436
Downloading Windows device drivers . . . 437
Configuring Windows Server for OS device-driver updates . . . 440
Configuring a domain account for OS device-drivers updates . . . 441
Configuring global Windows device-driver update settings . . . 442
Applying Windows device drivers . . . 443

Chapter 15. Installing operating systems on bare-metal servers . . . 447
Operating-system deployment considerations . . . 450
Supported operating systems . . . 454
Operating-system image profiles . . . 458

© Copyright Lenovo 2015, 2022

Port availability for deployed operating systems 462
Configuring a remote file server 464
Importing operating-system images 466
Customizing OS-image profiles. 468
Importing a customized OS image profile . . . 475
Importing boot files 477
Importing device drivers. 482
Importing custom configuration settings . . . 485
Importing custom unattend files. 502
Associating an unattend file with a configuration settings file 507
Importing custom installation scripts 508
Importing custom software 513
Creating a custom OS-image profile 515
Configuring global OS-deployment settings 517
Configuring network settings for managed servers 519
Choosing the storage location for managed servers 521
Deploying an operating-system image 524
Integrating with Windows Active Directory 527
OS-deployment scenarios. 531
Deploying RHEL with custom device drivers 531
Deploying RHEL and a Hello World PHP application using a custom unattend file . . . 533
Deploying RHEL and a Hello World PHP application using custom software and a post-installation script 537
Deploying SLES 12 SP3 with custom packages and time zone 540
Deploying SLES 12 SP3 with custom software 546
Deploying SLES 12 SP3 with a configurable locale and NTP servers 548
Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address 553
Deploying VMware ESXi v6.7 with Lenovo Customization with a configurable locale and second-user credentials. 556
Deploying Windows 2016 with custom features 560
Deploying Windows 2016 with custom software 563
Deploying Windows 2016 for Japanese. . . . 567

Chapter 16. End-to-end scenarios for setting up new devices. 575

Deploying ESXi to a local hard drive 575
Deploying a predefined virtualization pattern 575
Deploying VMware ESXi to a Flex System x240 Compute Node 577
Deploying ESXi to SAN storage. 582
Deploying a server pattern to support SAN boot 582
Deploying VMware ESXi to SAN storage . . . 585
Notices . . . . . .dxci
Trademarks . . . . . .dxcii

Tables

1. Account Security settings. 61
2. Role of each network interface based on network topology 80
3. Lenovo MAC address pool 316
4. Brocade WWN address pool 318
5. Emulex WWN address pool 319
6. Lenovo WWN address pool 320
7. QLogic WWN address pool 321
8. Port availability for RHEL Virtualization profiles 463
9. Port availability for RHEL Basic and Minimal profiles 463
10. Port availability for Windows profiles 464

© Copyright Lenovo 2015, 2022

Summary of changes

Follow-on releases of Lenovo XClarity Administrator management software support new hardware, software enhancements, and fixes.

Refer to the change history file (*.chg) that is provided in the update package for information about fixes.

This version supports the following enhancements to the management software.

For information about changes in earlier releases, See What's new in the XClarity Administrator online documentation.

Function	Description
Device management	You can manage NVIDIA Mellanox switches (see Managing switches).. You can securely erase data on all disk drives in specific managed servers (see Securely erasing drive data). You can view the capacity of drives in ThinkSystem DM storage devices (see Viewing the details of a storage device). You can view the firmware levels for IBM Tape Drives (see Viewing the details of a storage device). You can view the size of each drive in a specific storage device (see Viewing the details of a storage device). You can view the available capacity of each storage device from the Storage page (see Viewing the status of storage devices). You can view capacity information about a specific storage device from the storage summary page (see Viewing the status of storage devices).
Server configuration	You can manually change the status of "Not Compliant" devices to "Compliant" without redeploying the profile (see Configuration considerations).
Firmware updates	You can apply firmware updates to IBM TS4300 Tape Library devices (see Updating firmware on managed devices). You can assign firmware-compliance policies to all or only selected devices that are non-compliant in addition to devices with no policy assignment (see Creating and assigning firmware-compliance policies).
Operating system deployment	VLAN tagging is not supported for Linux operating-system deployments; however, you can force deploying under VLAN mode by setting the VLAN ID to 1 for all Linux deployments (see Configuring network settings for managed servers). You can import multiple customized ESXi images with the same major/minor version and build number (see Importing operating-system images).

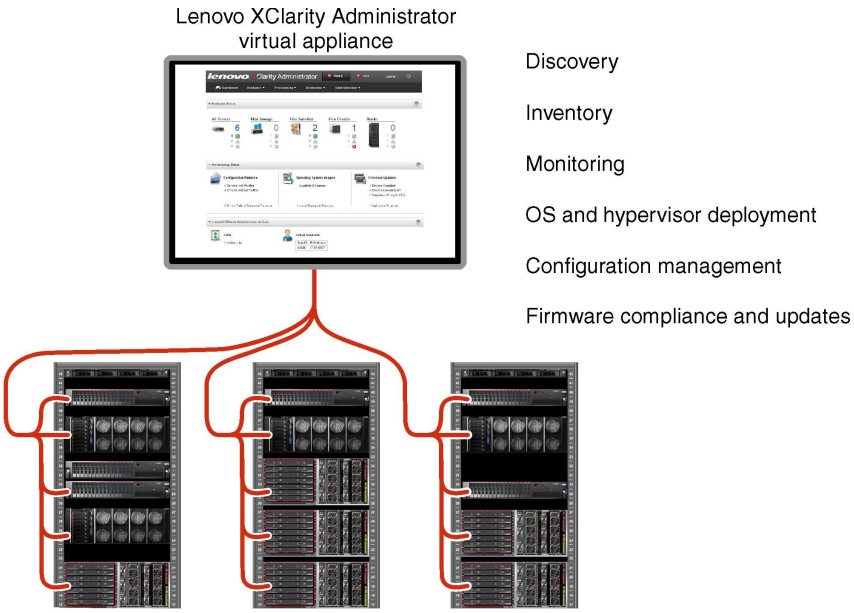
© Copyright Lenovo 2015, 2022

Chapter 1. Lenovo XClarity Administrator Overview

Lenovo XClarity Administrator is a centralized, resource-management solution that simplifies infrastructure management, speeds responses, and enhances the availability of Lenovo® server systems and solutions. It runs as a virtual appliance that automates discovery, inventory, tracking, monitoring, and provisioning for server, network, and storage hardware in a secure environment.

Learn more:

- XClarity Administrator: Managing hardware like software
- XClarity Administrator: Overview



XClarity Administrator provides a central interface to perform the following functions for all managed devices.

Hardware management

XClarity Administrator provides agent-free hardware management. It can automatically discover manageable devices, including server, network, and storage hardware. Inventory data is collected for managed devices for an at-a-glance view of the managed hardware inventory and status.

There are various management tasks for each supported device, including viewing status and properties, and configuring system and network settings, launching the management interfaces, powering on and off, and remote control. For more information about managing devices, see Managing chassis, Managing servers, and Managing switches.

Tip: Server, network, and storage hardware that can be managed by XClarity Administrator is referred to as *devices*. Hardware that is under XClarity Administrator management is referred to as *managed devices*.

You can use the rack view in XClarity Administrator to group your managed devices to reflect the physical rack setup in your datacenter. For more information about racks, see Managing racks.

Learn more:

- XClarity Administrator: Discovery

© Copyright Lenovo 2015, 2022

- XClarity Administrator: Inventory
- XClarity Administrator: Remote control

Hardware monitoring

XClarity Administrator provides a centralized view of all events and alerts that are generated from the managed devices. An event or alert is passed to the XClarity Administrator and is displayed in the events or alerts log. A summary of all events and alerts is visible from the Dashboard and the Status bar. Events and alerts for a specific device are available from the Alerts and Events detail page for that device.

For more information about monitoring hardware, see Working with events and Working with alerts.

Learn more: XClarity Administrator: Monitoring

Configuration management

You can quickly provision and pre-provision all of your servers using a consistent configuration. Configuration settings (such as local storage, I/O adapters, boot settings, firmware, ports, and management controller and UEFI settings) are saved as a server pattern that can be applied to one or more managed servers. When the server patterns are updated, the changes are automatically deployed to the applied servers.

Server patterns also integrate support for virtualizing I/O addresses, so you can virtualize Flex System fabric connections or repurpose servers without disruption to the fabric.

For more information about configuring servers, see Configuring servers using configuration patterns.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Configuration patterns

Firmware compliance and updates

Firmware management is simplified by assigning firmware-compliance policies to managed devices. When you create and assign a compliance policy to managed devices, XClarity Administrator monitors changes to the inventory for those devices and flags any devices that are out of compliance.

When a device is out of compliance, you can use XClarity Administrator to apply and activate firmware updates for all devices in that device from a repository of firmware updates that you manage.

Note: Refreshing the repository and downloading firmware updates requires an Internet connection. If XClarity Administrator has no Internet connection, you can manually import firmware updates to the repository.

For more information about updating firmware, see Updating firmware on managed devices.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Firmware updates
- XClarity Administrator: Provisioning firmware security updates

Operating-system deployment

You can use XClarity Administrator to manage a repository of operating-system images and to deploy operating-system images to up to 28 servers managed servers concurrently.

For more information about deploying operating systems, see Installing operating systems on bare-metal servers.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Operating-system deployment

User management

XClarity Administrator provides a centralized authentication server to create and manage user accounts and to manage and authenticate user credentials. The authentication server is created automatically when you start the management server for the first time. The user accounts that you create for XClarity Administrator can also be used to log in to managed chassis and servers in managed-authentication mode. For more information about users, see Managing user accounts.

XClarity Administrator supports three types of authentication servers:

- **Local authentication server**. By default, XClarity Administrator is configured to use the local authentication server that resides on the management node.
- **External LDAP server**. Currently, only Microsoft Active Directory is supported. This server must reside on an outboard Microsoft Windows server that is connected to the management network. When an external LDAP server is used, the local authentication server is disabled.
- **External SAML 2.0 identity provider**. Currently, only Microsoft Active Directory Federation Services (AD FS) is supported. In addition to entering a user name and password, multi-factor authentication can be set up to enable additional security by requiring a PIN code, reading smart card, and client certificate.

For more information about authentication types, see Managing the authentication server.

When you create a user account, you assign a predefined or customized role group to the user account to control the level of access for that user. For more information about role groups, see Creating a custom role group.

XClarity Administrator includes an audit log that provides a historical record of user actions, such as logging on, creating new users, or changing user passwords. For more information about the audit log, see Working with events.

Device authentication

XClarity Administrator uses the following methods for authenticating with managed chassis and servers.

- **Managed authentication**. When managed authentication is enabled, the user accounts that you create in XClarity Administrator are used to authenticate managed chassis and servers.

  For more information about users, see Managing user accounts .
- **Local authentication**. When managed authentication is disabled, the stored credentials that are defined in XClarity Administrator are used to authenticate managed servers. The stored credentials must correspond to an active user account on the device or in Active Directory.

  For more information about stored credentials, see Managing stored credentials.

Security

If your environment must comply with NIST SP 800-131A standards, XClarity Administrator can help you achieve a fully compliant environment.

XClarity Administrator supports self-signed SSL certificates (which are issued by an internal certificate authority) and external SSL certificates (which are issued by a private or commercial CA).

Firewalls on chassis and servers can be configured to accept incoming requests from only XClarity Administrator.

For more information about security, see Implementing a secure environment.

Service and support

XClarity Administrator can be set up to collect and send diagnostic files automatically to your preferred service provider when certain serviceable events occur in XClarity Administrator and the managed devices. You can choose to send diagnostic files to Lenovo Support using Call Home or to another service provider using SFTP. You can also manually collect diagnostic files, open a problem record, and send diagnostic files to the Lenovo Support Center.

Learn more: XClarity Administrator: Service and support

Task automation using scripts

XClarity Administrator can be integrated into external, higher-level management and automation platforms through open REST application programming interfaces (APIs). Using the REST APIs, XClarity Administrator can easily integrate with your existing management infrastructure.

The PowerShell toolkit provides a library of cmdlets to automate provisioning and resource management from a Microsoft PowerShell session. The Python toolkit provides a Python-based library of commands and APIs to automate provisioning and resource management from an OpenStack environment, such as Ansible or Puppet. Both of these toolkits provide an interface to XClarity Administrator REST APIs to automate functions such as:

- Logging in to XClarity Administrator
- Managing and unmanaging chassis, servers, storage devices, and top-of-rack switches (devices)
- Collecting and viewing inventory data for devices and components
- Deploying an operating-system image to one or more servers
- Configuring servers through the use of Configuration Patterns
- Applying firmware updates to devices

Integration with other managed software

XClarity Administrator modules integrate XClarity Administrator with third-party management software to provide discovery, monitoring, configuration, and management functions to reduce the cost and complexity of routine system administration for supported devices.

For more information about XClarity Administrator, see the following documents:

- Lenovo XClarity Integrator for Microsoft System Center
- Lenovo XClarity Integrator for VMware vCenter
- Lenovo XClarity Integrator for Nutanix Prism

For additional considerations, see Management considerations in the XClarity Administrator online documentation.

Learn more:

- Lenovo XClarity Integrator for Microsoft System Center overview
- Lenovo XClarity Integrator for Nutanix
- Lenovo XClarity Integrator for VMware vCenter

Documentation

The XClarity Administrator documentation is updated regularly online in English See the XClarity Administrator online documentation for the most current information and procedures.

The online documentation is available in the following languages:

- German (de)
- English (en)
- Spanish (es)
- French (fr)

- Italian (it)
- Japanese (ja)
- Korean (ko)
- Brazilian Portuguese (pt_BR)
- Russian (ru)
- Thai (th)
- Simplified Chinese (zh_CN)
- Traditional Chinese (zh_TW)

You can change the language of the online documentation in the following ways:

- Change the language setting in your web browser
- Append `?lang=<language_code>` to the end of URL, for example, to display the online documentation in Simplified Chinese:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**?lang=zh_CN**

Logging in to XClarity Administrator

Log in to the Lenovo XClarity Administrator web interface using a supported web browser.

Before you begin

Ensure that you are using one of the following supported web browsers:
- Chrome™ 48.0 or later (55.0 or above for Remote Console)
- Firefox® ESR 38.6.0 or later
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 or later (IOS7 or later and OS X)

Note: Launching the management-controller interfaces from XClarity Administrator using the Safari web browser is not supported.

Ensure that you log in to the XClarity Administrator web interface from a system that has network connectivity to XClarity Administrator management node.

Procedure

Complete the following steps to log in to the XClarity Administrator web interface.

Step 1. Point your browser to the IP address of XClarity Administrator.

Tip: Access to the web interface is through a secure connection. Ensure that you use **https**.

- **For containers** Use the IPv4 address that is specified for the ${ADDRESS} variable to access XClarity Administrator using the following URL:
  `https://<IPv4_address>/ui/login.html`

  For example:
  `https://192.0.2.10/ui/login.html`
- **For virtual appliances**. The IP address that you use depends on how your environment is set up.

  If you have Eth0 and Eth1 networks on separate subnets, and if DHCP is used on both subnets, use the *Eth1* IP address when accessing the web interface for initial setup. When XClarity Administrator starts for the first time, both Eth0 and Eth1 get a DHCP-assigned IP address, and the XClarity Administrator default gateway is set to the DHCP-assigned gateway for *Eth1*.

Using static a IPv4 address

If you specified an IPv4 address in eth0_config, use that IPv4 address to access XClarity Administrator using the following URL:

`https://<IPv4_address>/ui/login.html`

For example:

`https://192.0.2.10/ui/login.html`

Using a DHCP server in the same broadcast domain as XClarity Administrator

If a DHCP server is set up in the same broadcast domain as XClarity Administrator, use the IPv4 address that is displayed in the XClarity Administrator virtual-machine console to access XClarity Administrator using the following URL:

`https://<IPv4_address>/ui/login.html`

For example:

`https://192.0.2.10/ui/login.html`

Using a DHCP server in a different broadcast domain as XClarity Administrator

If a DHCP server *is not* set up in the same broadcast domain, use the IPv6 Link-Local Address (LLA) that is displayed for eEth0 (the management network) in the XClarity Administrator virtual-machine console to access XClarity Administrator, for example:

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

Tip: The IPv6 link local address (LLA) is derived from the MAC address of the interface.

Attention: If you are configuring XClarity Administrator remotely, you must have connectivity to the same layer 2 network. It must be accessed from a non-routed address until the initial setup is complete. Therefore, consider accessing XClarity Administrator from another VM that has connectivity to XClarity Administrator. For example, you can access XClarity Administrator from another VM on the host where XClarity Administrator is installed.

– **Firefox:**

  To access the XClarity Administrator web interface from a Firefox browser, log in using the following URL. Note that brackets are required when entering IPv6 addresses.

  `https://[<IPv6_LLA>/ui/login.html]`

  For example, based on the previous example shown for Eth0, enter the following URL in your web browser:

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

– **Internet Explorer:**

  To access the XClarity Administrator web interface from an Internet Explorer browser, log in using the following URL. Note that brackets are required when entering IPv6 addresses.

  `https://[<IPv6_LLA>%25<zone_index>]/ui/login.html`

  where *<zone_index>* is the identifier for the Ethernet adapter that is connected to the management network from the computer on which you launched the web browser. If you are using a browser on Windows, use the **ipconfig** command to find the zone index, which is displayed after the percent sign (%) in the **Link-Local IPv6 Address** field for the adapter. In the following example, the zone index is "30."

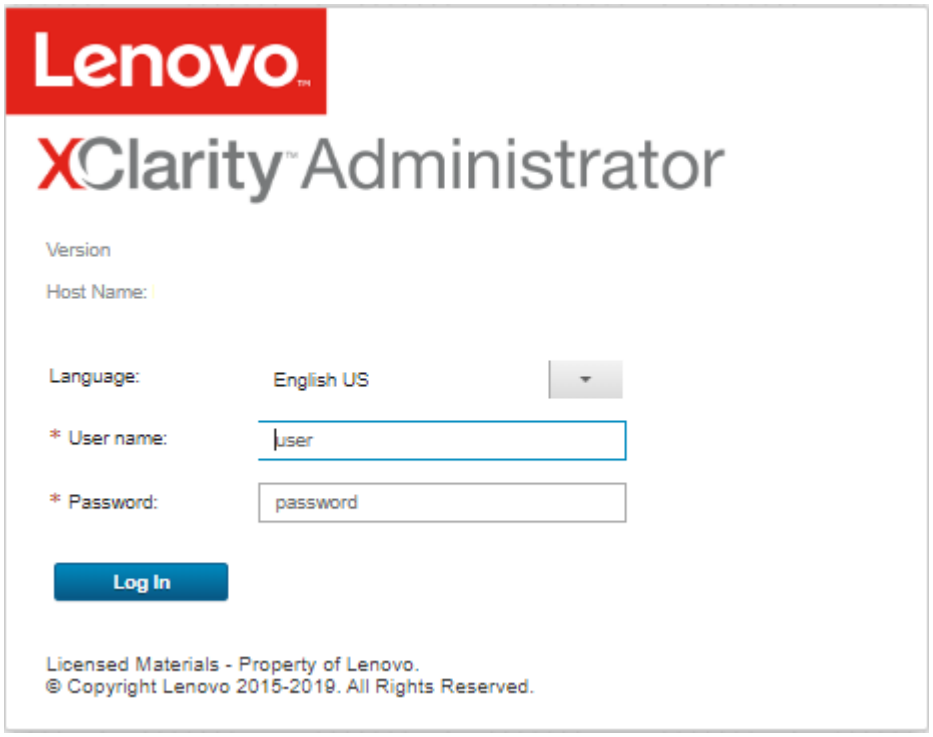
```
PS C:> ipconfig
Windows IP Configuration

Ethernet adapter vEthernet (teamVirtualSwitch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : 2001:db8:56ff:fe80:bea3%30
   Autoconfiguration IPv4 Address. . : 192.0.2.30
   Default Gateway . . . . . :
```

  If you are using a browser on Linux, use the **ifconfig** command to find the zone index. You can also use the name of the adapter (typically Eth0) as the zone index.

  For example, based on the examples shown for Eth0 and the zone index, enter the following URL in your web browser:

  `https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html`

The XClarity Administrator initial login page is displayed:



Step 2. Select the desired language from the **Language** drop-down list.

Note: The configuration settings and values that are provided by the managed devices might be available only in English.

Step 3. Enter a valid user ID and password, and click **Log In**.

The first time you log in with a user account, you are required to change the password. Passwords must meet the following criteria:

- (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed).
- (2) Must contain at least one number (0 - 9).
- (3) Must contain at least *two* of the following characters.
  - Uppercase alphabetic characters (A – Z)
  - Lowercase alphabetic characters (a – z)
  - Special characters ; @ _ ! ' $ & +
- (4) Must not repeat or reverse the user name.
- (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed).

After you finish

The XClarity Administrator dashboard page is displayed:

Note: If the host operating system is shut down unexpectedly, you might receive an authentication error when you attempt to log in to XClarity Administrator. To resolve this problem, restore XClarity Administrator from the last backup to access the management server (see Backing up Lenovo XClarity Administrator).

You can perform the following actions from the user-actions menu (

) on the XClarity Administrator title bar.

- Find information about how to use XClarity Administrator in the embedded help system by clicking **Help**.

  The XClarity Administrator documentation is updated regularly online in English See the XClarity Administrator online documentation for the most current information and procedures.
- View the XClarity Administrator license by clicking **License**.
- View information about the XClarity Administrator release by clicking **About**.
- Change the language of the user interface by clicking **Change language**.
- Log out of the current session by clicking **Log out**.
- Submit ideas or provide feedback about XClarity Administrator by clicking **Submit ideas** or **Submit feedback**.
- Ask questions and find answers on the Lenovo XClarity Community forum website by clicking **Visit forum**.

User interface tips and techniques

Consider these tips and techniques when using the Lenovo XClarity Administrator user interface

Viewing more or less data per page

You can change the number of rows that are displayed per page using the links on the bottom right of the table. You can display **10**, **25**, **50**, or **All** rows

Finding data in large lists

Most fields can accept up to 128 characters.

There are several ways to display a subset of a large list based on specific criteria.

- You can sort the table rows by clicking the column header.

  Changing the sort order of a table column is persistent across the user sessions.
- You can use the **Filter By** icons and **Show** drop-down list that is available on some pages to display a subset of data based on the selected criteria.
- You can further refine the subset by entering text (such as a name or IP address) in the **Filters** field to find data that is found in any available column.

  You can choose from the past 10 searches by selecting the searches from the drop-down menu on the **Filters** field. The last active search on a page is persistent across user sessions.

Viewing column data

If the column size prevents all information from displaying in the table cell (indicated by an ellipsis), you can view the complete information in a popup by hovering over text in the cell.

Configure table columns

You can configure tables to show information that is important to you.

- You can choose which columns to show or hide by clicking **All Actions → Toggle Columns**.
- You can reorder columns by dragging the column headers to the preferred location.

Changing the language of the user interface

You have an option to set the language of the user interface when you first log in.

After you are logged in, you can change the language of the user interface by clicking the user-actions menu(

), and then clicking **Change language**. Select the language that you want to display.

Note: The help system displays in the same language that is set for the user interface

Getting help

XClarity Orchestrator offers several ways to get help with the user interface.

- Some pages provide additional details about a specific field or status using **Help** icons ( ). Hover the cursor over the icon to display a pop-up with helpful information.
- To get help about how to perform specific actions from the user interface, click the user-actions menu (

) and then click **Help**.

Using the Lenovo XClarity Mobile app

Lenovo XClarity Administrator offers a mobile app for Android and iOS devices. You can use the Lenovo XClarity Mobile app to securely monitor physical systems, get real-time status alerts and notifications, and take action on common system level tasks. The app can also connect directly via an enabled USB port to a ThinkSystem server and provide virtual LCD capability.

Learn more: Lenovo XClarity Mobile app overview

Using the XClarity Mobile app, you can perform the following activities:

- Configure network settings and properties
- View the status summary of each connected XClarity Administrator.
- View the status summary of all managed devices.
- Display graphical views (maps) for chassis, rack servers, and storage devices.
- View resource groups that are defined on the XClarity Administrator.
- View rack-switch port information and change configured port status.
- Monitor the inventory and detailed status of each managed device.
- Monitor audit events, hardware and management events, alerts, and jobs.
- Turn on or off the location LED on a managed device.
- Power on, power off, restart, or reseat a managed device.
- Trigger the collection of diagnostic data.
- View device warranty information and status
- Set up automatic problem notification through Call Home.
- View the summary of open service tickets and delete service tickets
- Push event notifications to your mobile device (see Forwarding events to mobile devices).
- View the summary of active users and system resource usage
- Send feedback about this mobile app to Lenovo Support.
- Connect your mobile device directly to a ThinkSystem server to manage the server using the XClarity Mobile app (for devices that support USB tethering).
- Download Lenovo XClarity Controller service data when the mobile device is connected to a ThinkSystem server.

You can also connect your mobile device directly to ThinkSystem servers and then launch the XClarity Mobile app and log in to the server's baseboard management controller using the same web and CLI credentials. A menu of additional information and actions is available, including:

- Service
  - Share summary information using email or other means that is provided by the mobile device
  - Clear the event and audit log
  - Download the event and audit log to the mobile-device local storage or transmitting the log by any means that is provided by the mobile device

  - Download the BMC FFDC service file to the mobile-device local storage or transmitting the file by any means that is provided by the mobile device
  - View historical graph data for power, thermal and system usage
  - Enable "One-Touch" service mode, which provides an immediate summary of active alerts and critical device information
- Configuration and Initial Setup
  - Manage a new device using the selected XClarity Administrator
  - Configure server properties, such as location and contact information for initial setup
  - View and changing the IPv4 and IPv6 BMC network interface settings
  - Specify boot order and one-time boot settings
  - Change the front panel USB port assignment
  - View the number of server reboots and total power on hours
- Power Actions
  - Power the server on or off, restarting the server, or triggering NMI
  - Reset the BMC

Tip: After the app is open, you must refresh the app to see the updated status, inventory, events, and jobs.

Prerequisites

- iOS tablets are supported at iPhone screen-resolution only. Android tablets are not currently supported.
- The following mobile operating systems are supported:
  - Android 7 – 11
  - iOS 10 and later

    Notes:

    - Android 5 is supported only for XClarity Mobile 2.3.0 and earlier.
    - Facial recognition that is used on iPhone X/XR/XS devices is not supported.
- Ensure that a network connection is available from your mobile device to the XClarity Administrator instances. This might require the use of a VPN solution. See your network administrator for assistance.
- Import the CA certificate for each XClarity Administrator instance.

  Important: All connections to XClarity Administrator use HTTPS. However, there must be a valid certificate chain before the connection is considered trusted and data can be passed to the mobile device. To create a trusted certificate chain, you must import the XClarity Administrator self-signed certificate authority (CA) into the mobile device.

  To import the self-signed CA certificate for *each XClarity Administrator instance* into the mobile device, complete the following steps.

  1. Download the CA certificate to a local system:
     a. Connect to the XClarity Administrator instance using a web browser on your local system.
     b. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.
     c. Click **Certificate Authority** under the Certificate Management section. The Certificate Authority page is displayed.
     d. Click **Download Certificate Authority Root Certificate**.

        Attention: Normally, it is not necessary to click **Regenerate Certificate Authority Root Certificate** to complete this process. Doing so might disrupt communication with managed devices unless the correct procedure is followed. For more information, see Working with security certificates.

e. Click **Save as der** or **Save as pem** to save the CA certificate as a DER or PEM file on your local system. PEM format works in most cases.

2. Transfer the CA certificate file to your mobile device, for example, by using an accessible storage repository (such as Dropbox™), email, or file transfer through a connected cable.
3. Import the trusted CA certificate:
   - (Android) Typically this is done by selecting **Settings → Security → Install** from phone storage, and then selecting the certificate file that you downloaded.

     Important: If your successfully installed CA certificate is not signed by a third party, the `Network may be monitored by an unknown third-party` message is displayed on Android devices. Because the CA certificate is generated in your trusted environment, this message can be safely ignored. Ensure that the message is for the XClarity Administrator CA certificate before ignoring the message.
   - (iOS) Open the email on your mobile device, and click the document link in the email to import the trusted CA certificate.

   Attention: For iOS 10.3 and later, imported certificates are not trusted by default. To trust the certificates, select **Settings → General → About → Certificate Trust Settings**, and then enable the certificate trust.

Installing and setting up

1. Download the XClarity Mobile app from iTunes App Store (iOS) or Google Play Store (Android).

   Note: Users in China can also download the Android version from Lenovo app store (乐商城), Baidu app store website (百度手机助手) or Tencent app store website (应用宝). After logging in to the website, search for "XClarity."
2. To install the app, follow instructions on the mobile device.

   Important: A mobile OS-level security code to unlock screen access is required to use the XClarity Mobile app. If one is not already set up, you are instructed to set one up during installation.
3. Click **Settings** to add or edit connections to multiple XClarity Administrator instances using the automatic discovery or by providing an IP address and user credentials, set a PIN code for the app, change the event and audit log settings, and select your preferred language.

Important: For Android devices, XClarity Mobile app v2.1.0 and earlier is not automatically updated to v2.2.0. You must manually uninstall the current XClarity Mobile app before installing v2.2.0 (see "Resolving issues" for more information).

Updating to XClarity Mobile app v3.0

XClarity Mobile app v3.0 has upgrades to the most modern technologies with emphasis on performance and security. This includes changes to the local storage model, which requires you to reconfigure some settings when updating to the latest app:

- Connections to XClarity Administrator instances (IP addresses or hostnames, user name, and password)
- Security settings, including your four-digit passcode and fingerprint authentication, . if applicable
- Language setting (English is the default)

Connecting directly to ThinkSystem servers

Lenovo Think System servers include a front panel USB port that you can use to connect to your mobile device to provide similar capabilities that were available on the LCD system-information display panel on other Lenovo servers.

To manage a ThinkSystem server by directly connecting to server, complete these steps.

1. Switch the server front panel USB from host to BMC by performing one of the following steps.
   a. From the management controller CLI, run the **usbfp** command
   b. From the management controller web interface, click **BMC Configuration → Network → Front Panel USB Port Management**.
   c. Hold the blue ID location LED on the front panel for at least 3 seconds until the light blinks every couple of seconds.
2. Connect your phone USB cable to the front panel USB port on the ThinkSystem server.
3. On your mobile device, enable USB tethering.
   a. For iOS, click **Settings → Cellular → Personal Hotspot**.
   b. For Android, click **Settings → Mobile hotspot and tethering → USB tethering**.
4. On your mobile device, launch the XClarity Mobile app.
5. If automatic discovery is disabled, click **Discovery** on the USB Discovery page to connect to the server's management controller and collect information, including inventory, health, firmware, network configuration, and a list of the latest active events.

Tip:

- Ensure that you use a high-quality USB cable that supports data and power. Be aware that some cables that are supplied with mobile devices are only for charging purposes.

  Note: To connect to ThinkSystem SD530, you must also use a high-quality micro USB to USB cable or adapter.
- The USB-attached server must be powered on to report the full set of voltage, temperature, and usage statistics in the summary status cards.
- If the USB-attached server does not have an external "blue identification" LED/button on the front panel, you must use the management controller web interface or CLI to change the front panel USB port management selection, if needed.
- Changes made to the management-controller network interface from the XClarity Mobile app take effect immediately without requiring management controller to be restarted. For example, if the IPv4 interface is changed from a static address to DHCP, the interface immediately obtains a DHCP assigned address.
- On the Newsfeed tab, the "Latest active events" card initially displays up to three active events that are listed on the management controller's Active Events tab. On the mobile app, if you tap that card, all of the active events are displayed. Note that this is a list of active and resolved events, not a full list of all events.

Using demonstration mode

You can enable **Demonstration Mode** on the Settings page to populate the XClarity Mobile app with demo data for two XClarity Administrator instances, including racks and chassis. In this mode, you can view the status summary of the XClarity Administrator instances, view detailed status and inventory of devices, and monitor events and alerts. However, management actions, such as powering on and off, are not supported.

Notes:

- You can enable demonstration mode only when there are no connections to actual XClarity Administrator instances.
- You cannot add connections to actual XClarity Administrator instances while demonstration mode is enabled.

Searching

You can use the **Search** field to display managed devices with a specific name or status (Critical, Warning, or Normal). For example, if you search for “crit,” only managed devices in the Critical status and with names that include “crit” are displayed.

Resolving issues

Installation issues:

- Typically, when a new version of the Android mobile app is posted to the app store, the app automatically updated on your mobile device. However, due to enhanced security measures, the newly released mobile app v2.2.0 is no longer updated automatically. This is a one-time "transition" issue and only affects the upgrade to v2.2.0. Subsequent updates will operate as expected.

  The Android mobile app is "signed" with a secure key to enhance security. The secure key size was increased in the new release. Because the signed app does not match the earlier apps signature, the Android installation security process prevents the automatic update.

  To update the mobile app, uninstall the current version of the mobile app, download the latest version of the Android app from the app store, and reinstall the app. On most Android devices, the app can be uninstalled using the **Settings → Applications → Application Manager** menu item.

Connectivity issues:

- The USB tethering function in iOS 14, 14.0.1, and 14.0.2 is not working correctly, and therefore, the Lenovo XClarity Mobile app tethering function is not available for these iOS versions. This affects only the USB-attached handheld management in the datacenter. Remote management using mobile devices that support cellular and Wi-Fi communications are not affected and can be used to connect and collect data from XClarity Administrator and to perform management actions on managed devices.

  If the USB-attached handheld management function is needed, do not upgrade to iOS 14.

  This notification will be updated when Apple resolves the issue with iOS 14.
- XClarity Mobile requires an available network connection from your mobile device to the XClarity Administrator instances. This might require the use of a VPN solution. See your network administrator for assistance.
- Connections from your mobile device to each XClarity Administrator instance require a trusted certificate chain. See the online documentation for instructions to download and install the trusted CA certificates on your mobile device.

  If your successfully installed CA certificate is not signed by a third party, the `Network may be monitored by an unknown third-party` message is displayed. Because the CA certificate is generated in your trusted environment, this message can be safely ignored. Ensure that the message is for the XClarity Administrator CA certificate before ignoring the message.
- When switching your mobile device from a virtual private network (VPN) to a local network or vice versa, you might see the message `The secure gateway has rejected the connection attempt. A new connection attempt to the same or other secure gateway is needed, which requires reauthentication.` Log on to Lenovo XClarity Mobile to continue using the app.

Security issues:

- If you forget your PIN code, uninstall and reinstall the XClarity Mobile app. Then, re-establish all connections.
- If you clear credentials on an Android device, the encryption key is erased. You must re-establish all connections.

Event issues:

- By default, the event log shows hardware and management events that were received in the last 24 hours, and the audit log shows audit events that were received in the last 2 hours. If no events were received during the selected time periods, then the event log and audit log are not shown on the Monitoring page in XClarity Mobile.
- If you set up event forwarding in XClarity Administrator to send events to an email account, links in the email might not work on Android devices. Ensure that your version of Android and your email app support hyperlinks. If hyperlinks are unsupported, use another email app.

Help system issues:

- On some devices, the help system does not scale correctly to the size of the screen. Use the help-system controls to maximize and then minimize the page.

Chapter 2. Administering Lenovo XClarity Administrator

Several administration tasks, such as adding users or viewing jobs, are available from Lenovo XClarity Administrator.

Managing authentication and authorization

Lenovo XClarity Administrator provides security mechanisms to verify a user's credentials and control access to resources and tasks.

Managing the authentication server

By default, Lenovo XClarity Administrator uses a local Lightweight Directory Access Protocol (LDAP) server to authenticate user credentials.

About this task

Supported authentication servers

The *authentication server* is a user registry that is used to authenticate user credentials. Lenovo XClarity Administrator supports the following types of authentication servers.

- **Local authentication server**. By default, XClarity Administrator is configured to use the embedded Lightweight Directory Access Protocol (LDAP) server that resides in the management server.
- **External LDAP server**. Currently, only Microsoft Active Directory and OpenLDAP are supported. This server must reside on an outboard Microsoft Windows server that is connected to the management network. When an external LDAP server is used, the local authentication server is disabled.

  Attention: To configure the Active Directory binding method to use login credentials, the baseboard management controller for each managed server must be running firmware from September 2016 or later.
- **External identity-management system**. Currently only CyberArk is supported.

  If user accounts for a ThinkSystem or ThinkAgile server are onboarded onto CyberArk, you can choose to have XClarity Administrator retrieve credentials from CyberArk to log in to the server when initially setting up the servers for management (with managed or local authentication). Before credentials can be retrieved from CyberArk, the CyberArk paths must be defined in XClarity Administrator and mutual trust must be established between CyberArk and XClarity Administrator using TLS mutual authentication through client certificates.
- **External SAML identity provider**. Currently, only Microsoft Active Directory Federation Services (AD FS) is supported. In addition to entering a user name and password, multi-factor authentication can be set up to enable additional security by requiring a PIN code, reading smart card, and client certificate. When an SAML identity provider is used, the local authentication server is not disabled. Local user accounts are required to log in directly to a managed chassis or server (unless Encapsulation is enabled on that device), for PowerShell and REST API authentication, and for recovery if external authentication is not available.

  You can choose to use both an external LDAP server and an external identity provider. If both are enabled, the external LDAP server is used to log in directly to the manage devices, and the identity provider is used to log in to the management server.

Device authentication

© Copyright Lenovo 2015, 2022

By default, devices are managed using XClarity Administrator managed authentication to log in to the devices. When managing rack servers and Lenovo chassis, you can choose to use local authentication or managed authentication to log in to the devices.

- When *local authentication* is used for rack servers, Lenovo chassis, and Lenovo rack switches, XClarity Administrator uses a stored credential to authenticate to the device. The *stored credential* can be an active user account on the device or a user account in an Active Directory server.

  You must create a stored credential in XClarity Administrator that matches an active user account on the device or a user account in an Active Directory server before managing the device using local authentication (see Managing stored credentials in the XClarity Administrator online documentation).

  Notes:

  – RackSwitch devices support only stored credentials for authentication. XClarity Administrator user credentials are not supported.

- Using *managed authentication* allows you to manage and monitor multiple devices using credentials in the XClarity Administrator authentication server instead of local credentials. When managed authentication is used for a device (other than ThinkServer servers, System x M4 servers, and switches), XClarity Administrator configures the device and its installed components to use the XClarity Administrator authentication server for centralized management.

  – When managed authentication is enabled, you can manage devices using either manually-entered or stored credentials (see Managing user accounts and in the XClarity Administrator online documentation).

    The stored credential is used only until XClarity Administrator configures the LDAP settings on the device. After that, any change to the stored credential has no impact the management or monitoring of that device.

    Note: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.

  – If a local or external LDAP server is used as the XClarity Administrator authentication server, user accounts that are defined in the authentication server are used to log in to XClarity Administrator, CMMs and baseboard management controllers in the XClarity Administrator domain. Local CMM and management controller user accounts are disabled.

  – If an SAML 2.0 identity provider is used as the XClarity Administrator authentication server, SAML accounts are not accessible to managed devices. However, when using an SAML identity provider and an LDAP server together, if the identity provider uses accounts that exist in the LDAP server, LDAP user accounts can be used to log into the managed devices while the more advanced authentication methods that are provided by SAML 2.0 (such as multifactor authentication and single sign-on) can be used to log into XClarity Administrator.

  – Single sign-on allows a user that is already logged in to XClarity Administrator to automatically log in to the baseboard management control (XCC). Single sign-on is enabled by default when a ThinkSystem or ThinkAgile server is brought into management by XClarity Administrator (unless the server is managed with CyberArk passwords). You can configure the global setting to enable or disable single sign-on for all managed ThinkSystem and ThinkAgile servers. Enabling single sign-on for a specific ThinkSystem and ThinkAgile server overrides the global setting for all ThinkSystem and ThinkAgile servers (see Managing servers).

    Note: Single sign-on is disabled automatically when using the CyberArk identity-management system for authentication.

  – When managed authentication is enabled for ThinkSystem SR635 and SR655 servers:

    – Baseboard management-controller firmware supports up to five LDAP user roles. XClarity Administrator adds these LDAP user roles to the servers during management: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin**, and **lxc-os-admin**.

Users must be assigned to at least one of the specified LDAP user roles to communicate with ThinkSystem SR635 and SR655 servers.

  - Management-controller firmware does not support LDAP users with the same username as local user of the sever.

- For ThinkServer and System x M4 servers, the XClarity Administrator authentication server is not used. Instead, an IPMI account is created on the device with the prefix “LXCA_” followed by a random string. (The existing local IPMI user accounts are not disabled.) When you unmanage a ThinkServer server, the “LXCA_” user account is disabled, and the prefix “LXCA_” is replaced with the prefix “DISABLED_”. To determine whether a ThinkServer server is managed by another instance, XClarity Administrator checks for IPMI accounts with the prefix “LXCA_”. If you choose to force management of a managed ThinkServer server, all the IPMI accounts on the device with the “LXCA_” prefix are disabled and renamed. Consider manually clearing IPMI accounts that are no longer used.

  In XClarity Administrator v2.4 and later, if you use manually-entered credentials, XClarity Administrator automatically creates a stored credential and uses that stored credential to manage the device.

  Notes: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.

  - Each time you manage a device using manually-entered credentials, a new stored credential is created for that device, even if another stored credential was created for that device during a previous management process.
  - When you unmanage a device, XClarity Administrator does not delete stored credentials there were automatically created for that device during the management process.

Recovery account

If you specify a recovery password, XClarity Administrator disables the local CMM or management-controller user account and creates a new recovery user account (`RECOVERY_ID`) on the device for future authentication. If the management server fails, you can use the `RECOVERY_ID` account to log in to the device to take recovery actions to restore account-management functions on the device until the management node is restored or replaced.

If you unmanage a device that has a `RECOVERY_ID` user account, all local user accounts are enabled, and the `RECOVERY_ID` account is deleted.

- If you change the disabled local user accounts (for example, if you change a password), the changes have no effect on the `RECOVERY_ID` account. In managed-authentication mode, the `RECOVERY_ID` account is the only user account that is activated and operational.
- Use the `RECOVERY_ID` account only in an emergency, for example, if the management server fails or if a network problem prevents the device from communicating with XClarity Administrator to authenticate users.
- The `RECOVERY_ID` password is specified when you discover the device. Ensure that you record the password for later use.

For information about recovering a device management, see “Recovering management with a CMM after a management server failure” on page 210 and “Recovering rack or tower server management after a management server failure” on page 257.

Setting up an external LDAP authentication server

You can choose to use an external LDAP authentication server instead of the local Lenovo XClarity Administrator authentication server on the management node.

Before you begin

The initial setup of XClarity Administrator must be completed before setting up the external authentication server.

The following external authentication servers are supported:

- OpenLDAP
- Microsoft Active Directory. It must reside on an outboard Microsoft Windows server that is connected to the management network, data network, or both

Ensure that all ports that are required for the external authentication server are open on the network and firewalls. For information about port requirements, see Port availability in the XClarity Administrator online documentation.

You must create or rename role groups in the local authentication server to match the groups that are defined in the external authentication server.

Ensure that there are one or more users with **lxc-recovery** authority in the local authentication server. You can use this local user account to authenticate directly to XClarity Administrator when a communication error occurs with the external LDAP server.

Note: When XClarity Administrator is configured to use an external authentication server, the Users Management page in the XClarity Administrator web interface is disabled.

Attention: For Active Directory, to configure the binding method to use login credentials, the baseboard management controller for each managed server must be running firmware from September 2016 or later.

XClarity Administrator performs a connectivity check every 5 minutes to maintain connectivity to configured external LDAP servers. Environments with many LDAP servers might experience high CPU usage during this connectivity check. To achieve the best performance, ensure that most or all of the LDAP servers in the domain are reachable, or set the authentication-server selection method to **Use Pre-Configured Servers** and specify only known, reachable LDAP servers.

Procedure

To configure XClarity Administrator to use an external authentication server, complete the following steps.

Step 1. Set up the user-authentication method for Microsoft Active Directory or OpenLDAP.

If you choose to use non-secure authentication, no additional configuration is required. The Windows Active Directory or OpenLDAP domain controllers use non-secure LDAP authentication by default.

If you choose to use secure LDAP authentication, you must set up the domain controllers to allow secure LDAP authentication. For more information about setting configuring secure LDAP authentication in Active Directory, see the LDAP over SSL (LDAPS) Certificate article on the Microsoft TechNet website.

To verify that the Active Directory domain controllers are configured to use secure LDAP authentication:

- Look for the `LDAP over Secure Sockets layer (SSL) is now available` event in the domain controllers Event Viewer window.
- Use the **ldp.exe** Windows tool to test secure LDAP connectivity with the domain controllers.

Step 2. Import the Active Directory or OpenLDAP server certificate or the root certificate of the certificate authority that signed the server certificate.

a. From the XClarity Administrator menu bar, click **Administration → Security**.

b. Click **Trusted Certificates** in the Certificate Management section.

c. Click the **Create** icon ( ) to add a certificate.

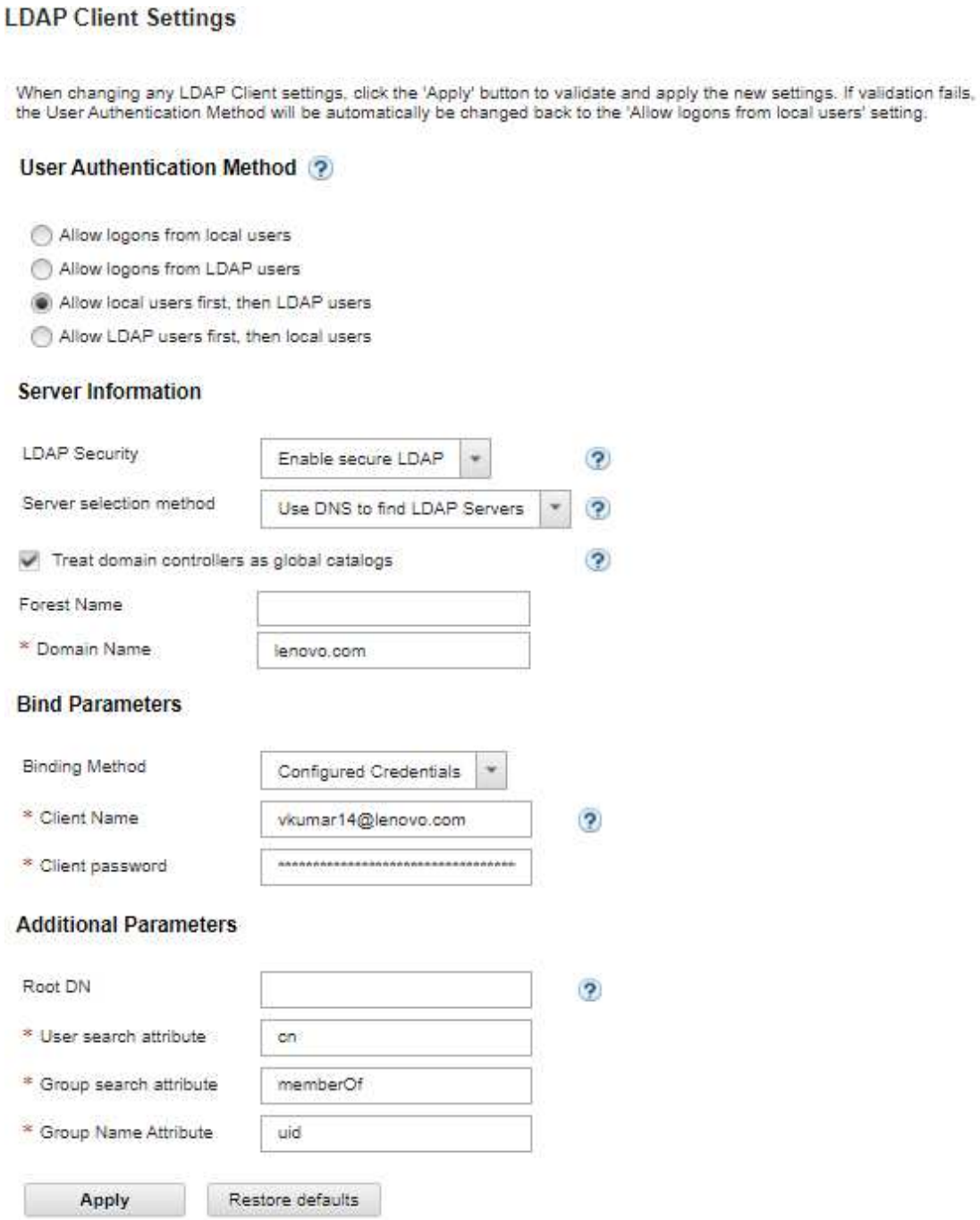
d. Browse for the file or paste the PEM-formatted certificate text.

e. Click **Create**.

Step 3. Configure the XClarity Administrator LDAP client:

a. From the XClarity Administrator menu bar, click **Administration → Security**.

b. Click **LDAP Client** under the Users and Groups section to display the LDAP Client Settings dialog.



c. Fill in the dialog based on the following criteria.

1. Select one of these user-authentication methods:

   - **Allow logons from local users**. Authentication is performed using the local authentication. When this option is selected, all user accounts exist in the local authentication server on the management node.
   - **Allow logons from LDAP users**. Authentication is performed by an external LDAP server. This method enables remote management of user accounts. When this option is selected, all user accounts exist remotely in an external LDAP server.
   - **Allow local users first, then LDAP users**. The local authentication server performs the authentication first. If that fails, an external LDAP server performs the authentication.
   - **Allow LDAP users first, then local users**. An external LDAP server performs the authentication first. If that fails, the local authentication server performs the authentication.

2. Choose whether to enable or disable secure LDAP:

   - **Enable secure LDAP**. XClarity Administrator uses the LDAPS protocol to connect securely to the external authentication server. When this option is selected, you must also configure trusted certificates for the purpose of enabling secure LDAP support.
   - **Disable secure LDAP**. XClarity Administrator uses an unsecure protocol to connect to the external authentication server. If you choose this setting, your hardware might be more vulnerable to security attacks.

3. Select one of these server-selection methods:

   - **Use Pre-Configured Servers**. XClarity Administrator uses the specified IP addresses and ports to discover the external authentication server.

     If you select this option, specify up to four pre-configured server IP addresses and ports. The LDAP client attempts to authenticate using the first server address. If authentication fails, the LDAP client attempts to authenticate using the next server IP address.

     If the port number for an entry *is not* explicitly set to `3268` or `3269`, the entry is assumed to identify a domain controller.

     When the port number is set to `3268` or `3269`, the entry is assumed to identify a global catalog. The LDAP client attempts to authenticate using the domain controller for the first configured server IP address. If this fails, the LDAP client attempts to authenticate using the domain controller for the next server IP address.

     Important: At least one domain controller must be specified, even if the global catalog is specified. Specifying only the global catalog seems to be successful but is not a valid configuration.

     When the cryptography mode is set to NIST-800-131A, XClarity Administrator might not be able to connect to an external LDAP server using a secure port (for example, using LDAPS over default port 636) if the LDAP server is not capable of establishing a Transport Layer Security (TLS) version 1.2 connection with the LDAP client in XClarity Administrator.
   - **Use DNS to find LDAP Servers**. XClarity Administrator uses the specified domain name or forest name to discover the external authentication server dynamically. The domain name and forest name are used to obtain a list of domain controllers, and the forest name is used to obtain a list of global catalog servers.

Attention: When using DNS to find LDAP servers, ensure that the user account to be used to authenticate to the external authentication server is hosted on specified domain controllers. If the user account is hosted on a child domain controller, include the child domain controller in the service request list.

4. Select one of these binding methods:

   - **Configured Credentials**. Use this binding method to use the client name and password to bind XClarity Administrator to the external authentication server. If the bind fails, the authentication process also fails

     The client name can be any name that the LDAP server supports, including a distinguished name, AMAccountName, NetBIOS name, or UserPrincipalName. The client name must be a user account within the domain that has at least read-only privileges. For example:
     ```
     cn=administrator,cn=users,dc=example,dc=com
     example\administrator
     administrator@example.com
     ```

     Attention: If you change the client password in the external authentication server, ensure that you also updated the new password in XClarity Administrator. For more information, see Cannot log in to XClarity Administrator in the XClarity Administrator online documentation.

   - **Login Credentials**. Use this binding method to use an Active Directory or OpenLDAP user name and password to bind XClarity Administrator to the external authentication server.

     The user ID and password that you specify are used only to test the connection to the authentication server. If successful, the LDAP client settings are saved, but the test login credential that you specified are not saved. All future binds use the user name and password that you used to log in to XClarity Administrator.

     Notes:

     – You must be logged in to XClarity Administrator using a fully-qualified user ID (for example, `administrator@domain.com` or `DOMAIN\admin`).

     – You must use a fully qualified test client name for the binding method.

     Attention: To configure the binding method to use login credentials, the management controller for each managed server must be running firmware from September 2016 or later.

5. In the **Root DN** field, it is recommended that you do not specify a root distinguished name, especially for environments with multiple domains. When this field is blank, XClarity Administrator queries the external authentication server for the naming contexts. If you use DNS to discover the external authentication server or if you specify multiple servers (for example, `dc=example,dc=com`), You can optionally specify the top-most entry in your LDAP directory tree. In this case, searches are started using the specified root distinguished name as the search base.

6. Specify the attribute to use to search for the user name.

   When the binding method is set to **Configured Credentials**, the initial bind to the LDAP server is followed by a search request that retrieves specific information about the user, including the user's DN, login permissions, and group membership. This search request must specify the attribute name that represents the user IDs on that server. This attribute name is configured in this field. If this field is left blank, the default is **cn**.

7. Specify the attribute name that is used to identify the groups to which a user belongs. If this field is left blank, the attribute name in the filter defaults to **memberOf**.

8. Specify the attribute name that is used to identify the group name that is configured by the LDAP server. If this field is left blank, the default is **uid**.

d. Click **Apply**.

The XClarity Administrator attempts to test the configuration to detect common errors. If the test fails, error messages are displayed that indicate the source of the errors. If the test succeeds and connections to the specified servers complete successfully, user authentication might still fail if:

- A local user with **lxc-recovery** authority does not exist.
- The root distinguished name is incorrect.
- The user is not a member of at least one group in the external authentication server that matches the name of a role group on the XClarity Administrator authentication server. XClarity Administrator cannot detect whether the root DN is correct; however, it can detect whether a user is a member of at least one group. If a user is not a member of at least one group, an error message is displayed when the user attempts to log in to XClarity Administrator. For more information about troubleshooting issues with the external authentication servers, see Connectivity Issues in the XClarity Administrator online documentation.

Step 4. Create an external user account that can access XClarity Administrator:

a. From the external authentication server, create a user account. For instructions , see the Active Directory or OpenLDAP documentation.

b. Create an Active Directory or OpenLDAP global group with the name of a predefined and authorized group. The group must exist within the context of the root distinguished name that is defined in the LDAP client.

c. Add the Active Directory or OpenLDAP user as a member of the security group that you created previously.

d. Log on to XClarity Administrator using the Active Directory or OpenLDAP user name.

e. **Optional:** Define and create additional groups. You can authorize these groups and assign roles to them from the Users and Groups page.

f. If secure LDAP is enabled, import trusted certificates to the external LDAP server (see Installing a customized, externally signed server certificate).

Results

XClarity Administrator validates the LDAP server connection. If the validation passes, user authentication occurs on the external authentication server when you log in to XClarity Administrator, CMM, and management controller.

If the validation fails, the authentication mode is automatically changed back to the **Allow logons from local users** setting, and a message that explains the cause of the failure is displayed.

Note: The correct role groups must be configured in XClarity Administrator, and user accounts must be defined as member of one of those role groups on the Active Directory server. Otherwise, user authentication fails.

Setting up an external SAML identity provider

You can choose to use a Security Assertion Markup Language (SAML) 2.0 identity provider to perform authentication and authorization for Lenovo XClarity Administrator.

Before you begin

The initial setup of XClarity Administrator must be completed before setting up the identity provider.

The identity provider must be Microsoft Active Directory Federated Service (AD FS) and can be connected to either the management network, data network, or both. Because authentication is done through your web browser, your web browser must be able to access XClarity Administrator and the SAML server.

You can download IDP metadata using the following URL: `https://<ADFS_IP_Address>/federationmetadata/2007-06/federationmetadata.xml`, where *<ADFS_IP_Address>* is the IP address for AD FS (for example, https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml).

You must create or rename role groups in the location authentication server to match the groups that are defined in the external authentication server.

To set up an SAML identity provider, you must be logged in as a user that is a member of the **lxc_admin** or **lxc_supervisor** group.

About this task

XClarity Administrator supports using a Security Assertion Markup Language 2.0 identity provider to authenticate and authorize users. In addition to entering a user name and password, the identity provider can be set up to require additional criteria to validate a user's identity, such as entering a PIN code, reading a smart card, and authenticating using a client certificate.

When XClarity Administrator is set up to use a identity provider, interactive login requests from the XClarity Administrator web interface are redirected to the identity provider for authentication. After the user is authenticated, the web browser is redirected back to XClarity Administrator.

Note: If the identity provider is enabled, you can bypass the identity provider and log in to XClarity Administrator using the local or external LDAP authentication server by opening your web browser to the XClarity Administrator login page (for example, `https://<ip_address>/ui/login.htm`).

When XClarity Administrator is configured to use an identity provider profile, the Users Management page in the XClarity Administrator web interface is not disabled. Local user accounts are required to directly log in to a managed chassis or server (except when Encapsulation is enabled on that device) and for PowerShell and REST API authentication.

Procedure

Complete the following steps to set up an external SAML identity provider (AD FS).

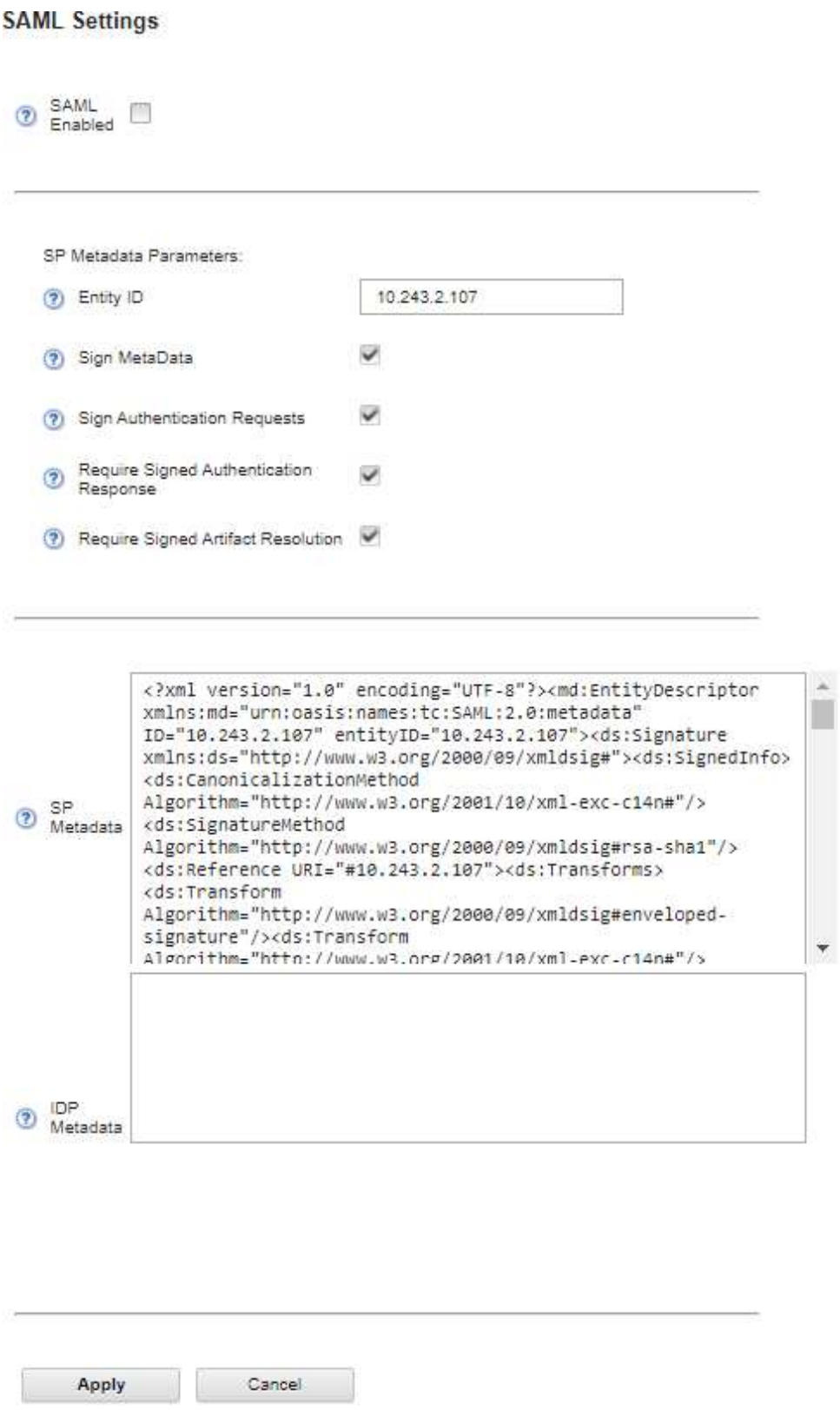
Step 1. Create a recovery user account that can be used to log in to XClarity Administrator if the identity provider becomes unavailable (see Managing user accounts).

Step 2. Retrieve the identity provider (IDP) metadata from the identity provider, and save the file on the XClarity Administrator host.

Step 3. Configure the XClarity Administrator SAML client.

a. From the XClarity Administrator menu bar, click **Administration → Security**.

b. Click **SAML Settings** under the Users and Groups section to display the SAML Settings dialog.



c. Fill in the fields on the SAML Settings page:

   1. Verify that the entity ID matches the IP address of the XClarity Administrator management server.

2. Choose whether the generated metadata is to be digitally signed.
3. Choose whether authentication requests are to be signed.
4. Choose whether authentication responses must be signed.
5. Choose whether the artifact-resolution requests that are sent to the remote identity provider must be signed.
6. Paste the SAML identity provider (IDP) metadata that was generated by the identity provider and retrieved in step Step 2 3 on page 25 into the **IDP Metadata** field.

d. Click **Apply** to apply the changes and update the text in the SP Metadata field.

Attention: *Do not* select **SAML Enabled** at this point. You will enable SAML in a later step to restart XClarity Administrator.

e. Copy and paste the data in the **SP Metadata** field to a file, and save the file with the .XML extension (for example, sp_metadata.xml). Copy this file to the AD FS host.

Step 4. Configure AD FS.

a. Open the AD FS Management tool.
b. Click **ADFS → Relying Party Trusts**.
c. Right click **Relying Party Trusts**, then click **Add Relying Party Trust** to display the wizard
d. Click **Start**
e. On the Select Data Source page, select **Import data about the relying party from a file**, and then select the SP metadata file that you saved in step 3e.
f. Enter a display name.
g. Click **Next** on all pages to choose the default values.
h. Click **Finish** to display the Claim Rules page
i. Leave **Send LDAP Attributes as Claims** as default, and click **Next**.
j. Enter a claim rule name.
k. Select **Active Directory** for the attribute store.
l. Add a mapping. On the left side select **SAM-Account-Name**, and on the right side, select **Name ID** for the outgoing claim type.
m. Add another mapping. On the left side, select **Token-Groups-Unqualified Names**, and on the right side select **Group** for the outgoing claim type
n. Click **OK**.
o. Locate the trust that you just created in the list of **Relying Party Trusts**.
p. Right-click the trust, and click **Select properties**. The trust Properties dialog is displayed.
q. Click the **Advanced** tab, and select `SHA-1` as the secure hash algorithm.

Step 5. Save the server certificate from AD FS.

a. Click **AD FS console → Service → Certificates**.
b. Select the **Certificate** under Token-signing.
c. Right-click the certificate, and click **View Certificate**.
d. Click the **Details** tab.
e. Click **Copy to File**, and save the certificate as a DER encoded binary X.509 (.CER) file.
f. Copy the server certificate .CER file to the XClarity Administrator host.

Step 6. Import the AD FS trusted certificate into XClarity Administrator web interface.

a. From the XClarity Administrator menu bar, click **Administration → Security**.

b. Click **Trusted Certificates** in the Certificate Management section.

c. Click the **Create** icon ( ) to add a certificate.

d. Select the server certificate .CER file that you saved in the previous step.

e. Click **Create**.

Step 7. Click **SAML Settings** under the Users and Groups section to display the SAML Settings dialog.

Step 8. Select **SAML Enabled** to enable management of user accounts using an external identity provider. When this option is selected, all user accounts exist remotely in an identity provider.

Step 9. Click **Apply** to apply the changes and restart the management server.

Step 10. Wait a few minutes for XClarity Administrator to restart.

Attention: Do not restart the virtual appliance manually during this process.

Step 11. Close and reopen the web browser.

Step 12. Log in to the XClarity Administrator web interface from the identity provider.

Results

The XClarity Administrator attempts to test the configuration to detect common errors. If the test fails, error messages are displayed that indicate the source of the errors.

XClarity Administrator validates the identity provider connection. If the validation passes, user authentication occurs on the identity provider when you log in to XClarity Administrator.

Setting up an external identity-management system

An *identity-management system* is an external password vault that can optionally be used with Lenovo XClarity Administrator to store XClarity Administrator and XClarity Controller credentials. When an identity-management system is added to XClarity Administrator, XClarity Administrator retrieves passwords from the identity-management system, instead of the authentication servers.

About this task

XClarity Administrator supports the following identity-management system.

- CyberArk

Setting up a CyberArk identity-management system

CyberArk is an external password vault that optionally can be used with Lenovo XClarity Administrator to store XClarity Administrator and Lenovo XClarity Controller credentials. After an account password is stored in CyberArk, the password is managed by CyberArk

About this task

XClarity Administrator allows you to store your XCC passwords in identity-management systems provided by CyberArk, a third party service. Lenovo is not responsible for the CyberArk service, and you are responsible for your direct relationship with CyberArk.

If user accounts for a ThinkSystem or ThinkAgile server are onboarded onto CyberArk, you can choose to have XClarity Administrator retrieve credentials from CyberArk to log in to the server when initially setting up the servers for management (with managed or local authentication). Before credentials can be retrieved from CyberArk, the CyberArk paths must be defined in XClarity Administrator and mutual trust must be established between CyberArk and XClarity Administrator using TLS mutual authentication through client certificates.

Procedure

To configure XClarity Administrator to use CyberArk, complete the following steps.

Step 1. Configure CyberArk.

1. From the XClarity Administrator menu bar, click **Administration → Security**.
2. Click **CyberArk** under the Identity Management section.
3. Click **Edit CyberArk Server Details** from the toolbar.
4. Specify the CyberArk hostname or IP address, and the port number.
5. Click **Apply**.

Step 2. Import the XClarity Administrator mutual-authentication certificate into CyberArk.

1. From the XClarity Administrator menu bar, click **Administration → Security**.
2. Click **Server Certificate** in the Certificate Management section.
3. Click **Client Certificate** tab.
4. Select **CyberArk** as the server type.
5. Click **Regenerate Certificate** to generate a new TLS mutual-authentication certificate for CyberArk.

   Attention: If you regenerate the TLS mutual-authentication certificate for CyberArk after a connection is established between XClarity Administrator and CyberArk, the connection is lost until you import the new certificate in CyberArk.
6. Click **Download Certificate**, and then click **Save as der** or **Save as pem** to save the certificate as a file to your local system.
7. Import the downloaded certificate into CyberArk.

Step 3. Import the CyberArk root CA certificate in to XClarity Administrator.

1. Download the root CA certificate from CyberArk.
2. From the XClarity Administrator menu bar, click **Administration → Security**.
3. Click **Trusted Certificates** in the Certificate Management section.
4. Click the **Create** icon ( ) to add a certificate.
5. Browse for the file or paste the PEM-formatted certificate text.
6. Click **Create**.

Step 4. Add paths that identify the location of onboarded user accounts in CyberArk.

1. From the XClarity Administrator menu bar, click **Administration → Security**.
2. Click **CyberArk** under the Identity Management section.
3. Click the **Paths** tab.
4. Click the **Create** icon ( ) to display the Create CyberArk Path dialog.

5. Optionally specify the application ID, safe and folder where the user accounts are stored in CyberArk.

   If you specify the application ID and safe and optionally the folder, XClarity Administrator attempt to find the user account in the specified location.

   If you specify a combination of fields other than application ID and safe (for example, if you specify only the application ID, only the safe and folder, or only the application ID and folder), XClarity Administrator filters the path using the specified values.
6. Click **Apply**.

After you finish

- Modify a selected CyberArk path by clicking the **Edit** icon ( ).
- Delete a selected CyberArk path by clicking the **Delete** icon ( ).

Determining the type of authentication method that is used by Lenovo XClarity Administrator

You can determine the type of authentication method that is used currently from the **LDAP Client** and **SAML Settings** tabs on the Security page.

About this task

The *authentication server* is a user registry that is used to authenticate user credentials. Lenovo XClarity Administrator supports the following types of authentication servers.

- **Local authentication server**. By default, XClarity Administrator is configured to use the embedded Lightweight Directory Access Protocol (LDAP) server that resides in the management server.
- **External LDAP server**. Currently, only Microsoft Active Directory and OpenLDAP are supported. This server must reside on an outboard Microsoft Windows server that is connected to the management network. When an external LDAP server is used, the local authentication server is disabled.

  Attention: To configure the Active Directory binding method to use login credentials, the baseboard management controller for each managed server must be running firmware from September 2016 or later.
- **External identity-management system**. Currently only CyberArk is supported.

  If user accounts for a ThinkSystem or ThinkAgile server are onboarded onto CyberArk, you can choose to have XClarity Administrator retrieve credentials from CyberArk to log in to the server when initially setting up the servers for management (with managed or local authentication). Before credentials can be retrieved from CyberArk, the CyberArk paths must be defined in XClarity Administrator and mutual trust must be

established between CyberArk and XClarity Administrator using TLS mutual authentication through client certificates.

- **External SAML identity provider**. Currently, only Microsoft Active Directory Federation Services (AD FS) is supported. In addition to entering a user name and password, multi-factor authentication can be set up to enable additional security by requiring a PIN code, reading smart card, and client certificate. When an SAML identity provider is used, the local authentication server is not disabled. Local user accounts are required to log in directly to a managed chassis or server (unless Encapsulation is enabled on that device), for PowerShell and REST API authentication, and for recovery if external authentication is not available.

  You can choose to use both an external LDAP server and an external identity provider. If both are enabled, the external LDAP server is used to log in directly to the manage devices, and the identity provider is used to log in to the management server.

Procedure

To determine the type of authentication server that is being used by the management software, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **LDAP Client** under the Users and Groups section to display the LDAP Client Settings dialog.

Verify which user-authentication method is selected:

- **Allow logons from local users**. Authentication is performed using the local authentication. When this option is selected, all user accounts exist in the local authentication server on the management node.
- **Allow logons from LDAP users**. Authentication is performed by an external LDAP server. This method enables remote management of user accounts. When this option is selected, all user accounts exist remotely in an external LDAP server.
- **Allow local users first, then LDAP users**. The local authentication server performs the authentication first. If that fails, an external LDAP server performs the authentication.
- **Allow LDAP users first, then local users**. An external LDAP server performs the authentication first. If that fails, the local authentication server performs the authentication.

Step 3. Click **SAML Settings** under the Users and Groups section to display the SAML Settings page.

If **SAML Enabled** is selected, then a identity provider is used.

Accessing Lenovo XClarity Administrator after an external LDAP server failure

If you are using an external LDAP authentication server and that server fails or is not available, use the following procedure to recover access to the Lenovo XClarity Administrator web interface by using the local authentication server on the management node.

Procedure

To change the LDAP client setting, complete the following steps.

Step 1. Log in to the XClarity Administrator web interface using a user account with **lxc-recovery** authority. For more information about the client domain name, see Setting up an external LDAP authentication server.

Step 2. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 3. Click **LDAP Client** under the Users and Groups section to display the LDAP Client dialog.

Step 4. Select **Allow logons from local users** for the user authentication method to enable local management of user accounts. When this option is selected, all user accounts exist locally on the management server.

Step 5. Click **Apply**.

Results

You can now use the user accounts in the local authentication server to access the XClarity Administrator management server. After your external authentication server is restored and available to the management server, you can change the LDAP client setting back to the external authentication server.

Accessing Lenovo XClarity Administrator after an external SAML identity provider failure

If you are using an external SAML identity provider and that server fails or is not available, use the following procedure to recover access to the Lenovo XClarity Administrator web interface by using the XClarity Administrator local authentication server.

Procedure

Complete the following steps to change the SAML client setting.

Step 1. Open your web browser to the XClarity Administrator login page (for example, `https://<ip_address>/ui/login.html`).

Step 2. Log in to the XClarity Administrator web interface using a local recovery user account that you created when you set up the identity provider.

Step 3. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 4. Click **SAML Settings** under the Users and Groups section to display the SAML Settings dialog.

Step 5. Clear **Enable SAML** to disable the SAML identity provider. When this option is cleared, the local authentication server or external LDAP server (if configured) is used for authentication.

Step 6. Click **Apply**.

Results

You can now use the user accounts in the local authentication server to access the XClarity Administrator management server. After your external identity provider is restored and available to the management server, you can change the authentication method to the identity provider.

Managing user accounts

User accounts are used to log in and manage Lenovo XClarity Administrator and all chassis and servers that are managed by XClarity Administrator. XClarity Administrator user accounts are subjected to two interdependent processes: authentication and authorization.

About this task

Authentication is the security mechanism by which a user's credentials are verified. The authentication process uses the user credentials that are stored in the configured authentication server. It also prevents unauthorized management servers or rogue managed-system applications from accessing the resources. After authentication, a user can access XClarity Administrator. However, to access a specific resource or perform a specific task, the user must also have the appropriate authorization.

Authorization checks the permissions of the authenticated user and controls access to resources based on the users membership in a role group. *Role groups* are used to assign specific roles to a set of user accounts that are defined and managed in the authentication server. For example, if a user is a member of a role group that has Supervisor permissions, that user can create, edit, and delete user accounts from XClarity Administrator. If a user has Operator permissions, that user can only view user-account information.

Note: The SYSMGR_* and SYSRDR_* user accounts (where * is a randomly chosen suffix created from characters A – Z and 0 – 9) are generated and used by XClarity Administrator as service user accounts and are used in functions such as managed authentication, OS deployment, and firmware updates. The SYSMGR_* and SYSRDR_* passwords are rotated each time XClarity Administrator is booted and shortly before the password expiration period is due.

Creating a user

User accounts are used to manage authorization and access to resources.

About this task

The first user account that you create must have the role of Supervisor and must be activated (enabled).

As an added measure of security, create at least two user accounts that have the role of **Supervisor**. Ensure that you record the passwords for these user accounts, and store them in a secure location in case you must restore the Lenovo XClarity Administrator.

Procedure

To add a user to XClarity Administrator, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Local Users** under the Users and Groups section to display the Users Management page.

Step 3. Click the **Create** icon ( ) to create a user. The Create New User dialog is displayed.

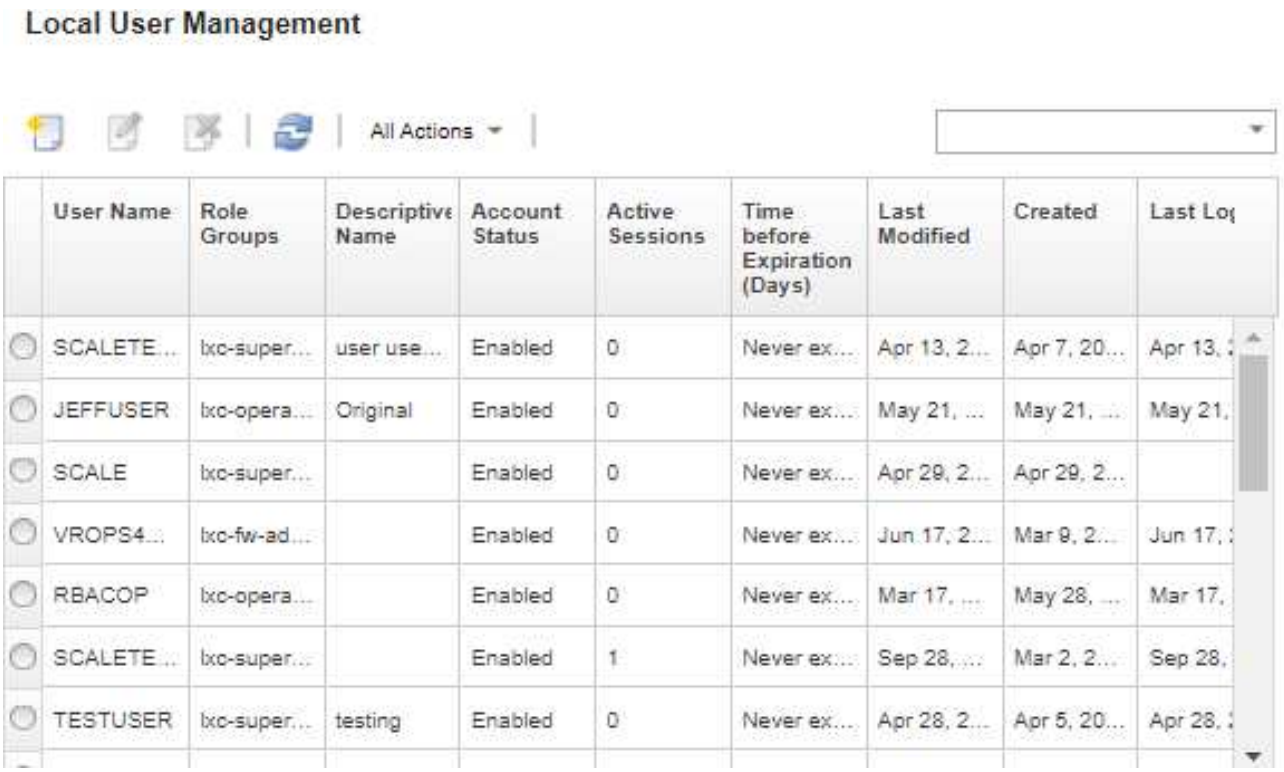
Step 4. Fill in the following information in the dialog.

- Enter a user name and description for the user.
- Enter the new and confirm new passwords. The rules for the passwords are based the current account-security settings.
- Select one or more role groups to authorize the user to perform appropriate tasks.For information about role groups and how to create custom role groups, see Creating a custom role group.
- (Optional) Set **Change password on first access** to `Yes` if you want to force the user to change the password the first time the user logs in to XClarity Administrator.

Step 5. Click **Create**.

After you finish

The user account is displayed in the Users Management table. The table shows the associated role groups and the account status for each user account.



After you create a user account, you can perform the following actions on a selected user account:

- Modify the user name, description, and role for a user account by clicking the **Edit** icon ( ).
- Delete the user account by clicking the **Delete** icon ( ).
- Reset the password for the user account (see Resetting the password for a user).
- Unlock the account (see Unlocking a user).
- Enable or disable a user account (see Enabling or disabling a user).

Enabling or disabling a user

You can change enable or disable a local user account in the authentication server.

Procedure

To enable or disable a user account, complete the following steps.

- If the local authentication server is used:
  1. From the Lenovo XClarity Administrator title bar, click **Administration → Security**.
  2. Click **Local Users** under the Users and Groups section to display the Users Management page.
  3. Select a user account.
  4. If the user account is enabled, click **All Actions → Disable selected account** to disable the user. The account status in the table changes to `Disabled`.
  5. If the user account is disabled, click **All Actions → Enable selected account** to enable the user. The account status in the table changes to `Enabled`.
- If an external LDAP server is used, enable or disable a user account in Microsoft Active Directory.
- If an external SAML identity provider is used, enable or disable a user account in the identity provider.

Logging off an active user

You can log off (terminate) an active user from Lenovo XClarity Administrator.

You must be logged on to XClarity Administrator using a user account with **lxc-supervisor** or **lxc-security-admin** authority.

Procedure

To log off an active user, complete the following steps.

Step 1. From the XClarity Administrator title bar, click **Administration → Security**.

Step 2. Click **Active Sessions** under the Users and Groups section to display the Active Sessions Management page.

Step 3. Select one or more user accounts.

Step 4. Click **Log Off User**.

Changing the password for your user account

You can change the password for your user account.

Procedure

Complete the following steps to change your password.

- If the local authentication server is used:
  1. From the Lenovo XClarity Administrator title bar, click the user-actions menu (

), and then click **Change Password**. The Change Password dialog is displayed.

  2. Enter the current password.
  3. Enter the new and confirm-new passwords. The rules for the passwords are based the current account-security settings.
  4. Click **Change**.

- If an external authentication server is used, change your password in Microsoft Active Directory.

  Attention: If you updated Microsoft Active Directory with a new password for the client account that is used to bind XClarity Administrator to the external authentication server, ensure that you also update the new password in the XClarity Administrator web interface (see Setting up an external LDAP authentication server).
- If an external SAML identity provider is used, change your password in the identity provider.

Resetting the password for a user

You can reset the password for any user account.

Procedure

To reset a password, complete the following steps.

- If the local authentication server is used, rest the password from the Lenovo XClarity Administrator web interface:
  1. From the XClarity Administrator menu bar, click **Administration → Security**.
  2. Click **Local Users** under the Users and Groups section to display the Users Management page.
  3. Select a user account from the table.
  4. If the user account is enabled, click the **All Actions → Reset Password for Selected User**. The Reset Password dialog is displayed.
     a. Enter the new and confirm new passwords. The rules for the passwords are based the current account security settings.
     b. Optionally set **Change on first access** to `Yes` if you want to force the user to change the password the first time the user logs in to XClarity Administrator.
     c. Click **Reset**.
- If an external LDAP server is used, reset the password in Microsoft Active Directory.
- If an external SAML identity provider is used, reset the password in the identity provider.
- If you cannot log in to XClarity Administrator using another supervisor account or if another supervisor account does not exist, you can reset the password for a local user with recovery or supervisor authority by mounting an ISO image that contains a configuration file with the new password. For more information, see Password for a local recovery or supervisor user is forgotten in the XClarity Administrator online documentation.

Unlocking a user

You can unlock a user account that is locked out of Lenovo XClarity Administrator. A user account can become temporarily locked if the user attempts too many logins that are not valid.

About this task

The user-account security settings control the amount of time that must pass before a user that was locked out can attempt to log back in again. If the **Lockout period after maximum login failures** setting is set to `0`, the user account remains locked until the administrator explicitly unlocks it. For more information about the lockout period for maximum login failures, see Changing the user-account security settings.

You can also permanently disable or enable a user account. For more information, see Enabling or disabling a user.

Note: You must have Supervisor authority to unlock a user account.

Tip: You can use XClarity Administrator to unlock user accounts that are managed using the local authentication server. You cannot unlock user accounts in an external authentication server by using the XClarity Administrator.

Procedure

To unlock a user account, complete the following steps.

- If the local authentication server is used:
  1. From the XClarity Administrator menu bar, click **Administration → Security**.
  2. Click **Local Users** under the Users and Groups section to display the Users Management page.
  3. Select the user account from the table.
  4. Click the **All Actions → Unlock Account for Selected User**.
- If an external LDAP server is used, unlock the user account in Microsoft Active Directory.
- If an external SAML identity provider is used, unlock the user account in the identity provider.

Monitoring active users

You can determine who is logged in to the Lenovo XClarity Administrator web interface from the Dashboard page.

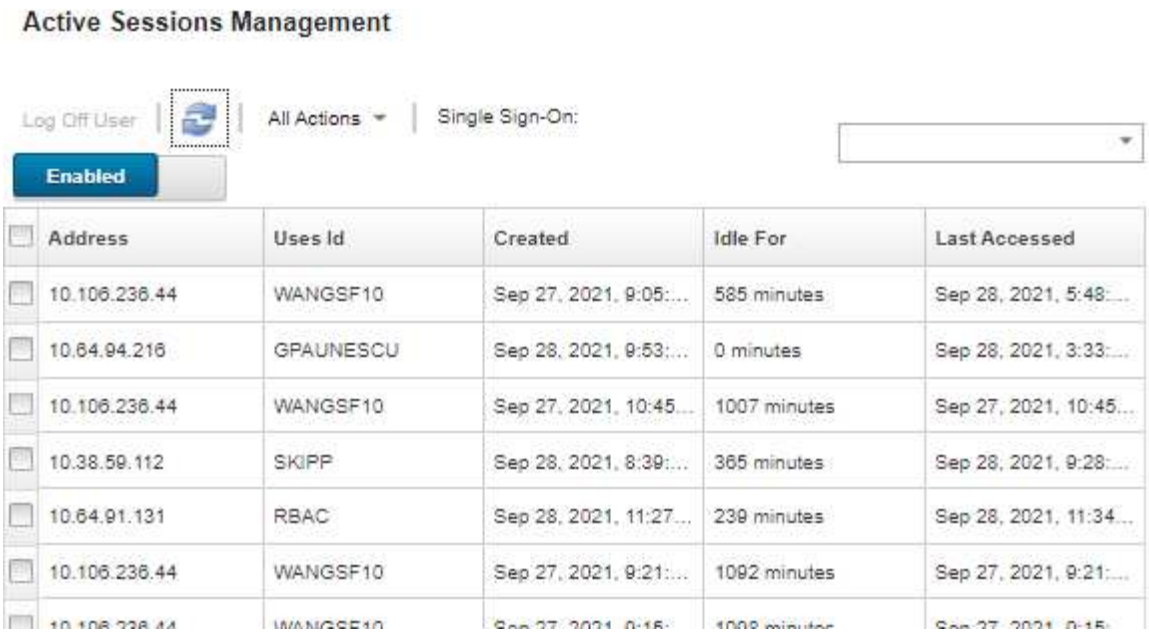
Procedure

- You can get find a list of active users and their IP addresses by clicking **Dashboard** from the XClarity Administrator menu bar.

  The active user sessions are listed in the Activity section.

- You can get find a list of all active users (other than the current user) and their IP addresses by clicking **Administration → Security** from the XClarity Administrator menu bar, and then clicking **Active Sessions**.

  Note: In XClarity Administrator v2.2 and later, user sessions that are inactive for more than specific amount of time are logged out automatically. You can set the inactivity period by clicking **Administration → Security** from the XClarity Administrator menu bar, clicking Account Security Settings, and then adjusting the **Web inactivity session timeout** value. Note that the change does not affect active user sessions. It only affects user sessions that start after the setting is changed.



Managing stored credentials

Stored credentials are used to manage authorization and access to chassis and servers that are managed by Lenovo XClarity Administrator using local authentication.

Before you begin

You must have **lxc-supervisor** or **lxc-security-admin** authority to create, modify, or delete stored credentials.

About this task

A stored credential must be a local user account on a device or a user account in an Active Directory server.

If you choose to manage devices using local authentication instead of XClarity Administrator managed authentication, you must select a stored-credentials account during the management process.

Important: XClarity Administrator does not validate the user name and password that you specify for the stored credential. It is your responsibility to ensure that specified information corresponds to an active user account on the local device or Active Directory (if the managed device is configured to use Active Directory for authentication).

Attention: The stored credentials must have supervisor access or sufficient authority to make configuration changes on the device. If you attempt to manage a server with stored credentials that do not have sufficient authority on the device, the manage process might succeed but additional administrative inventory actions on the device might fail due to access-denied errors, which could lead to perceived connectivity problems with the device.

Procedure

To add a stored credential to XClarity Administrator, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**. The Security page is displayed.

Step 2. Click **Stored Credentials** under the Managed Authentication section to display the Stored Credential page.

Step 3. Click the **Create** icon ( ) to create a stored credential. The Create New Stored Credentials dialog is displayed

Step 4. Fill in the following information in the dialog.
- Enter a user name and optional description for the stored credential.
- Enter and then confirm the password for the stored credential.
- Optionally enter and then confirm the password for the RECOVERY_ID stored recovery credentials.

Step 5. Click **Create Stored Credential**.

After you finish

The stored-credential account is displayed in the Stored Credential table. The table shows the associated ID and description for each stored-credential account.

From the Stored Credentials page, you can perform the following actions on a selected stored-credential account:

- Modify the user name, password, and description for a stored-credential account by clicking the **Edit** icon ( ).

  Note: If you manage a device using a stored credential and enable managed authentication, you cannot edit the stored credential.

- Delete the stored-credential account by clicking the **Delete** icon ( ).

To resolve stored credentials that have become expired or invalid, see Resolving expired or invalid stored credentials for a server.

Managing roles and role groups

A *role* is used to control user access to resources and limit the actions that users can perform on those resources. A *role group* is a collection of one or more roles and is used to assign those roles to multiple users. The roles that you configure for a role group determine the level of access that is granted to each user that is a member of that role group. Each Lenovo XClarity Administrator user must be a member of at least one role group.

Creating a custom role

A *role* is a set of *privileges*, or permissions to perform a specific action. Lenovo XClarity Administrator includes several predefined (default) roles. You can also create custom roles that enforce a unique set of privileges that users can perform

Before you begin

You must have **lxc-supervisor** or **lxc-security-admin** authority to perform this task.

About this task

To create a custom role, select one or more predefined roles that are closest in scope to the role that you want to create, and then clear the individual privileges that you want to restrict. This ensures that you get all of the intended privileges and that the role is constructed correctly with dependent privileges.

Some XClarity Administrator privileges depend on corresponding management-module privileges to perform actions on managed devices (see Management module v1 privileges and Management module v2 privileges). An XClarity Administrator privilege might allow you to request an action on a managed device, but the device will deny the request if you do not have the corresponding privileges for the CMM, IMM, or XCC. For example, if you create a custom role to perform power actions on managed devices, you would add the **lxc-inventory-modify-device-power-state** privilege and:

- For a ThinkSystem server in a rack, add the **mm-power-and-restart-access-v1** privilege.
- For an entire Flex System chassis (including devices in the chassis), add the **mm-power-and-restart-access-v1** privilege.
- For a ThinkSystem server in a chassis, add **mm-power-and-restart-access-v1**, **mm-blade-operator-v2**, and the **mm-blade-#-scope-v2** privilege that matches the target server.

All roles contain read-only privileges. No custom role can be more restrictive than the **lxc-operator** role.

If a user is does not have privileges to perform specific actions, menu items, toolbar icons, and buttons that perform those actions are disabled (greyed out).

XClarity Administrator provides a role group for each predefined role, using the same name as the role. Consider creating a role group for new roles that you create. For more information about role groups, see Creating a custom role group.

- **lxc-supervisor**. Users that are assigned this role can access, configure, and perform all available operations on the management server and all managed devices.Users that are assigned this role always have access to all managed devices. You cannot restrict access to devices for this role.
- **lxc-admin**. Users that are assigned this role can modify non-security related settings and perform all non-security related operations on the management server, including the ability to update and restart the management server. This role also provides the ability to view all configuration and status information about the management server and managed devices.
- **lxc-security-admin**. Users that are assigned this role can modify security settings and perform security-related operations on the management server and managed devices. This role also provides ability to view all configuration and status information about the management server and managed devices.

  Users that are assigned this role always have access to all managed devices. You cannot restrict access to devices for this role.
- **lxc-hw-admin**. Users that are assigned this role can modify non-security settings and perform non-security related operations on managed devices, including the ability to update and restart managed devices. This role also provides the ability to view all configuration and status information about the management server and all managed devices.
- **lxc-fw-admin**. Users that are assigned this role can create firmware policies and deploy those policies to managed devices. Users that are not assigned this role can only view policy information.

- **lxc-os-admin**. Users that are assigned this role can download and deploy operating systems and device-driver updates to managed servers. Users that are not assigned this role can only view operating-system and device-driver information.
- **lxc-service-admin**. Users that are assigned this role can collect and download service files for XClarity Administrator and managed devices. Users that are not assigned this role can collect but not download service data.
- **lxc-hw-manager**. Users that are assigned this role can discover new devices and place those devices under the management control of the XClarity Administrator. This role prohibits users from performing operations or modifying configurations settings on the management server and managed devices beyond those operations that are necessary to discover and manage new devices.
- **lxc-operator**. Users that are assigned this role can view all configuration and status information about the management server and managed devices. This role prohibits users from performing operations or modifying configurations settings on the management server and managed devices.
- **lxc-recovery**. Users that are assigned this role can modify security settings and perform security-related operations on the management server. These users can also authenticate directly to the XClarity Administrator even if the authentication method is set to external LDAP server. This role provides a recovery mechanism in case a communication error occurs with the external LDAP server that uses the "Login Credentials" configuration.

  Users that are assigned this role always have access to all managed devices. You cannot restrict access to devices for this role.

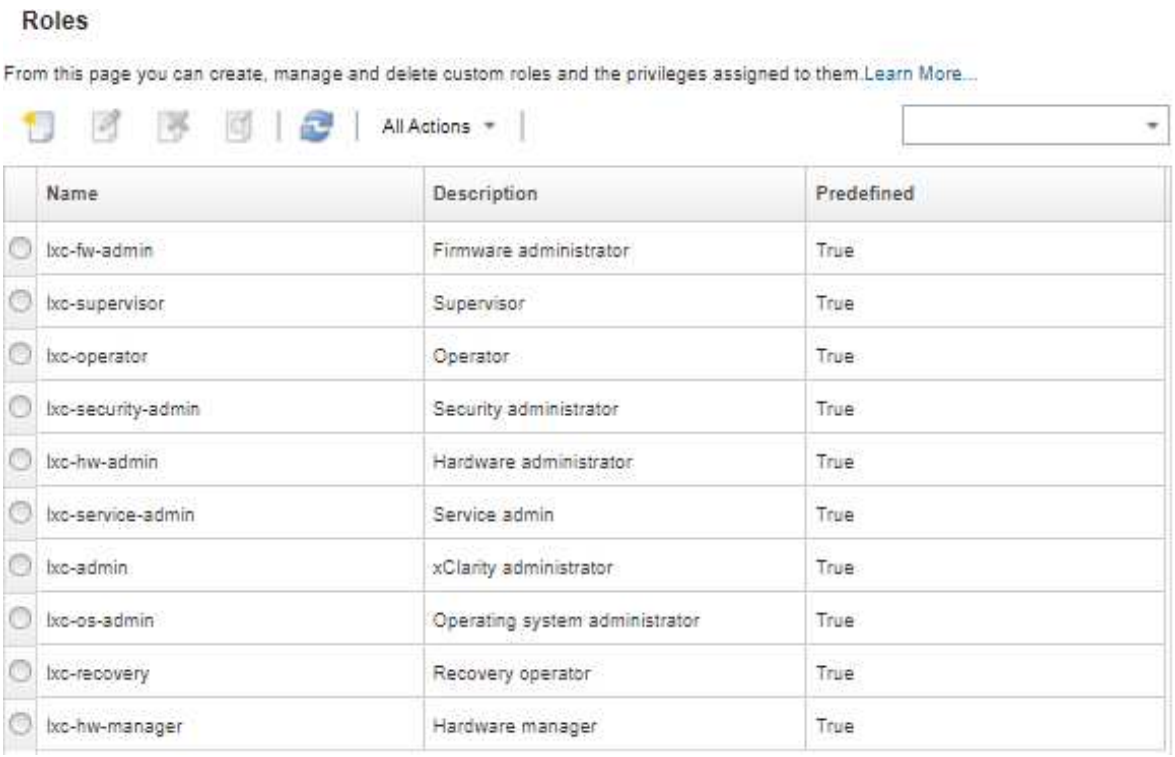
The following predefined roles are *reserved* and cannot be used to create new role groups or assigned to new users.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procedure

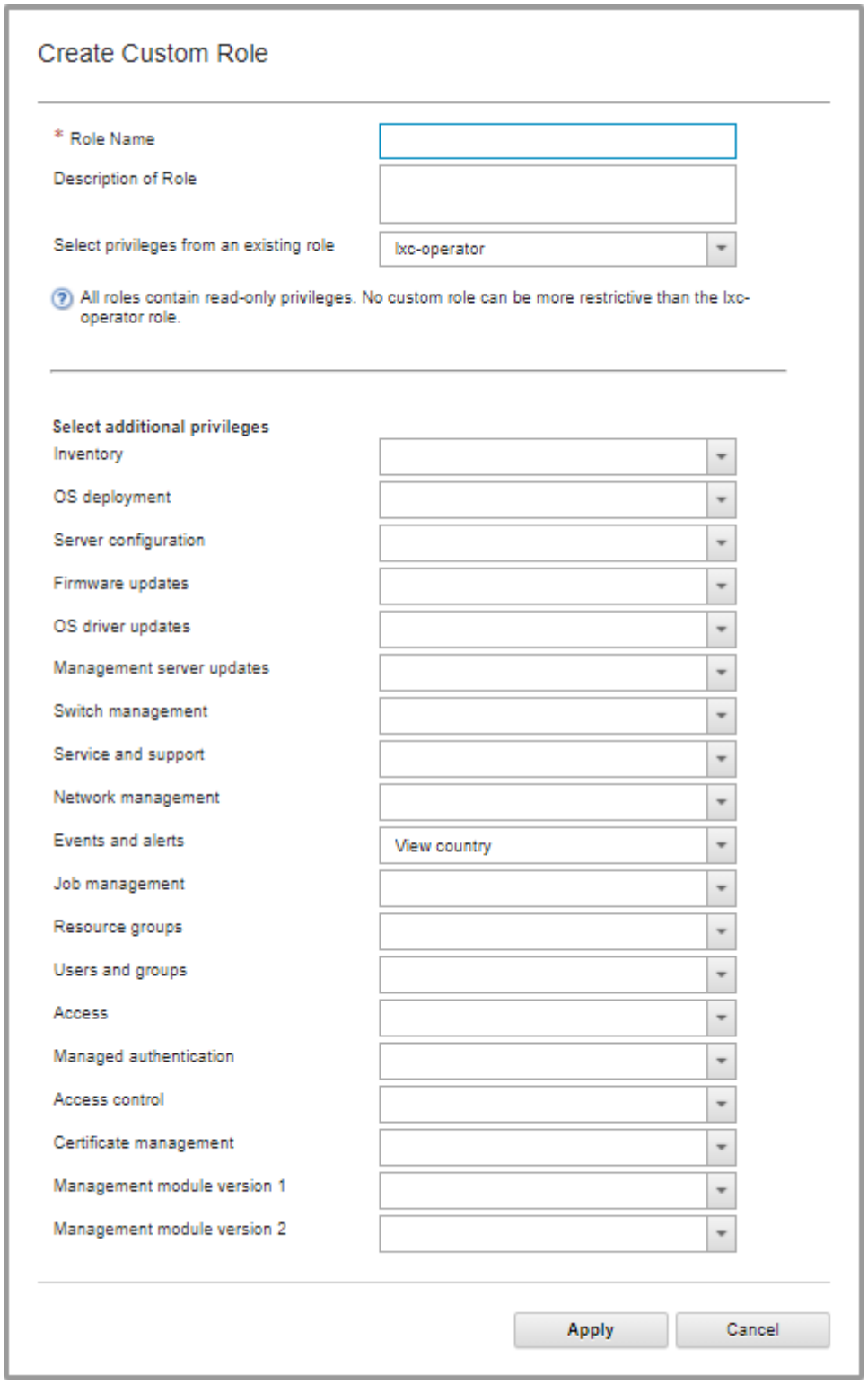
To create a custom role, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Roles** under the Users and Groups section to display the Roles Management page.



Step 3. Click the **Create** icon ( ) to create a role. The Create Custom Role dialog is displayed.



Step 4. Enter a role name and description.

Step 5. Optional: Select a predefined role to use as a starting point for this custom role.

If you select an existing role, the privileges that are associated with that role are selected in the dialog.

Step 6. Modify the privileges for this new role by selecting or clearing privileges from the **Select additional privileges** drop-down menus.

Note: If you select all privileges in specific category, and privileges are added to that category when you update or upgrade XClarity Administrator, the new privileges are automatically added to the custom role

Step 7. Click **Create**. The new role is added to the table on the Role Management page.

Results

You can also perform the following actions.

- View the privileges associated with a specific role by selecting the role and clicking the **View** icon ( ).
- Rename or edit the custom role by clicking the **Edit** icon ( ). When you edit a custom role, you can change selected privileges, the description, and list of users that are associated with the role.

  Note: You cannot modify a predefined role
- Delete the predefined or custom role by clicking the **Delete** icon ( ).
- Add or remove roles from a role group (see Adding and removing multiple users from a role group).
- Restore all predefined roles that were deleted by clicking **All Actions → Restore Default Roles**.

Predefined privileges

Lenovo XClarity Administrator provides a set of *privileges* (permissions) that allow a user to perform a specific action. The privileges are organized into categories based on the type of action.

Access privileges

These privileges provide permissions to modify cryptographic and SSL/TLS modes.

Privilege name	Privilege description	default roles
lxc-sec-apply-crypto-settings	Apply cryptography settings	lxc-recovery, lxc-security-admin, lxc-supervisor

Access control privileges

These privileges provide permissions to control access to resources.

Privilege name	Privilege description	default roles
lxc-sec-modify-resource-access-control	Edit resource access control settings	lxc-recovery, lxc-security-admin, lxc-supervisor

Certificate management privileges

These privileges provide permissions to manage security certificates in Lenovo XClarity Administrator.

Privilege name	Privilege description	dDefault roles
lxc-sec-add-external-certificates	Add an external certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-add-trusted-certificates	Add a trusted certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-certificate-signing	Generate certificate signing request	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilege name	Privilege description	dDefault roles
lxc-sec-delete-external-certificates	Delete an existing external certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-trusted-certificates	Delete an existing certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-ca	Download certificate authority root certificate	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-server-certificate	Download server certificate	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-certificate-revocation-list	Modify or replace certificate revocation list	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-ca	Regenerate certificate authority root certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-download-ca	Regenerate certificate authority root certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-server-certificate	Regenerate server certificate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-resolve-untrusted-certificates	Resolve untrusted certificates	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-upload-server-certificate	Upload server certificate	lxc-recovery, lxc-security-admin, lxc-supervisor

Monitoring and events privileges

These privileges provide permissions to manage events and alerts.

Privilege name	Privilege description	Default roles
lxc-event-audit	Manage event and audit logs	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	Create and modify event forwarders	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-monitoring-create-edit-push-services	Create and modify push services	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-event-forwarders	Delete event forwarders	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-push-services	Delete push services	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-set-event-thresholds	Set event thresholds	lxc-admin, lxc-hw-admin, lxc-supervisor

Firmware updates privileges

These privileges provide permissions to manage and apply firmware updates and UpdateXpress System Packs.

Privilege name	Privilege description	default roles
lxc-fwUpdates-apply-assign-policy	Assign firmware compliance policy to devices	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-apply-perform-updates	Perform firmware updates	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-create-policies	Create, copy, edit, and import firmware compliance policies	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-delete-policies	Delete compliance policies	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-delete-packages	Delete firmware update packages	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-download-packages	Download and import firmware update packages and refresh catalog of firmware update packages	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-export-packages	Export firmware update packages	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

Resource group privileges

These privileges provide permissions to use resource groups.

Privilege name	Privilege description	Default roles
lxc-resource-create-edit-group	Create and modify resource groups	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-resource-delete-group	Delete resource groups	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

Inventory privileges

These privileges provide permissions to discover and manage devices, and view device inventory.

Privilege name	Privilege description	default roles
lxc-dm-manage-device	Manage Chassis, Servers, Storage and Switches	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-dm-modify-ip-settings	Enable or disable checking for duplicate IP addresses in the same subnet	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-power-state	Modify canisters, cmms, nodes, storage and switches power state	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-properties	Modify cabinets, canisters, chassis, cmms, nodes, storage and switches properties	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	Modify predicted failure alerts (PFA) configuration settings	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Jobs management privileges

These privileges provide permissions to manage jobs (tasks).

Privilege name	Privilege description	Default roles
lxc-tasks-remove-jobs	Delete jobs	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-tasks-schedule-jobs	Schedule jobs	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Managed authentication privileges

These privileges provide permissions to manage authentication, including stored credentials.

Privilege name	Privilege description	default roles
lxc-sec-delete-stored-credentials	Delete stored credentials	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-stored-credentials	Edit existing stored credentials	lxc-recovery, lxc-security-admin, lxc-supervisor

Management module v1 privileges

These privileges are associated with the LDAP permission bits (bitstrings) that are enforced by management modules for rack servers and entire Flex System chassis (including all devices in that chassis).

Lenovo XClarity Administrator does not enforce these permissions. The permissions are enforced by the managed devices that use an XClarity Administrator use account.

If the device is managed using *managed authentication* (using the local authentication server for authentication), the local authentication server uses these permissions to indicate to the managed devices which permissions to grant to the user when logging in to the device.

You would configure these same permissions in an external LDAP server. When using an external LDAP server with XClarity Administrator, ensure that you add groups in the external LDAP server with names that match the role group names in XClarity Administrator and that the external LDAP users are added to one or more of those groups. External LDAP users must be part of an LDAP group with a name that matches an XClarity Administrator role group that contains roles associated with the management module bits strings. XClarity Administrator uses these groups to tie the external LDAP users to the role groups in XClarity Administrator and to the bits strings that are enforced by the management module. Then, when a user logs into a managed device using an external LDAP user account, the management module knows whether to grant the user supervisor or operator privileges.

Note: Management module v1 privileges are not supported for FlexSystem switches that do not have Secure IOM enabled, RackSwitch switches, Storage devices, and ThinkServer servers.

For information about the LDAP permission bits for each management module, see the online documentation.

- Configuring LDAP in the CMM and CMM2 online documentation
- Configuring LDAP in the IMM and IMM2 online documentation
- Configuring LDAP in the XCC online documentation

Privilege name	Privilege description	default roles
mm-advanced-adaptor-configuration-v1	Advanced adaptor configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-basic-configuration-v1	Basic configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Privilege name	Privilege description	default roles
mm-clear-event-logs-v1	Clear event logs	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v1	Deny always	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-networking-and-security-v1	Networking and security	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-power-and-restart-access-v1	Power/restart access for servers and Flex switches	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-access-v1	Remote control access for servers	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	Remote console and virtual media access for servers	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-supervisor-v1	Supervisor access	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-user-account-management-v1	User management	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

Management module v2 privileges

These privileges are associated with the LDAP permission bits (bitstrings) that are enforced by management modules for individual FlexSystem and ThinkSystem devices in a chassis (chassis, servers and switches with Secure IOM enabled).

Lenovo XClarity Administrator does not enforce these permissions. The permissions are enforced by the managed devices that use an XClarity Administrator use account.

If the device is managed using *managed authentication* (using the local authentication server for authentication), the local authentication server uses these permissions to indicate to the managed devices which permissions to grant to the user when logging in to the device.

You would configure these same permissions in an external LDAP server. When using an external LDAP server with XClarity Administrator, ensure that you add groups in the external LDAP server with names that match the role group names in XClarity Administrator and that the external LDAP users are added to one or more of those groups. External LDAP users must be part of an LDAP group with a name that matches an XClarity Administrator role group that contains roles associated with the management module bits strings. XClarity Administrator uses these groups to tie the external LDAP users to the role groups in XClarity Administrator and to the bits strings that are enforced by the management module. Then, when a user logs into a managed device using an external LDAP user account, the management module knows whether to grant the user supervisor or operator privileges.

Notes:

- You must also specify management module v1 privileges for the entire chassis (seeManagement module v1 privileges).
- Management module v2 privileges are not supported for FlexSystem switches that do not have Secure IOM enabled.

- For Lenovo ThinkSystem chassis, ensure that IMM2 is set up to allow the custom role to have “Node administration.” If you want the custom role to have control of all devices in the Lenovo ThinkSystem chassis, ensure that IMM2 is set up to allow the custom role to have “Node X scope” as well

For information about the LDAP permission bits for each management module, see the online documentation.
- Configuring LDAP in the CMM and CMM2 online documentation
- Configuring LDAP in the IMM and IMM2 online documentation
- Configuring LDAP in the XCC online documentation

Privilege name	Privilege description	Default roles
mm-blade-1-scope-v2	Node 1 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-2-scope-v2	Node 2 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-3-scope-v2	Node 3 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-4-scope-v2	Node 4 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-5-scope-v2	Node 5 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-6-scope-v2	Node 6 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-7-scope-v2	Node 7 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-8-scope-v2	Node 8 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-9-scope-v2	Node 9 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-10-scope-v2	Node 10 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-11-scope-v2	Node 11 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-12-scope-v2	Node 12 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-13-scope-v2	Node 13 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-14-scope-v2	Node 14 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-administration-v2	Node administration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-configuration-v2	Node configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-operator-v2	Blade operator	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-remote-presence-v2	Node remote presence	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Privilege name	Privilege description	Default roles
mm-chassis-administration-v2	Chassis administration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-configuration-v2	Chassis configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-log-management-v2	Chassis log account management	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-operator-v2	Chassis operator	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-chassis-scope-v2	Chassis scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-user-account-management-v2	User management	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v2	Deny always	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-io-module-1-scope-v2	I/O module 1 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-2-scope-v2	I/O module 2 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-3-scope-v2	I/O module 3 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-4-scope-v2	I/O module 4 scope	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-administration-v2	Switch administration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-configuration-v2	Switch configuration	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-operator-v2	Switch operator	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-supervisor-v2	Supervisor access	lxc-admin, lxc-hw-admin, lxc-supervisor

Management server privileges

These privileges provide permissions to update management server.

Privilege name	Privilege description	default roles
lxc-mgmtserverupdates-delete-updates	Delete management server updates	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-download-updates	Download and import management server updates and refresh management server catalog	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-perform-updates	Perform management server updates	lxc-admin, lxc-fw-admin, lxc-supervisor

Network management privileges

These privileges provide permissions to configure network settings.

Privilege name	Privilege description	Default roles
lxc-network-edit	Modify network access	lxc-admin, lxc-supervisor

OS deployment privileges

These privileges provide permissions to manage and deploy operating systems.

Privilege name	Privilege description	Default roles
lxc-osdeploy-create-edit-remote-file-server	Create and edit a remote file server entry	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	Create, import, export, and edit OS images and custom files	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-os-files	Delete OS images and custom files	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-remote-file-server	Delete a remote file server entry	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-global-settings	Edit information in global settings dialog **Note:** Changing global IP-assignment settings affects the network settings; therefore, to make changes to the global IP-assignment settings, you must also have also have **lxc-osdeploy-edit-settings-and-deploy-os-images** privileges.	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	Modify deployment settings and deploy OS images to one or more servers	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

OS driver updates privileges

These privileges provide permissions to manage and apply OS device-driver updates.

Privilege name	Privilege description	default roles
lxc-osDriverUpdates-apply-assign-uxsp	Assign OS device drivers UXSP to devices	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	Check OS authentication	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	Check OS device driver compliance	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	Perform OS device driver updates	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	Delete OS device driver update packages	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	Download and import OS device driver update packages and refresh OS device driver UXSP catalog	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Users and groups privileges

These privileges provide permissions to manage user accounts and groups.

Privilege name	Privilege description	default roles
lxc-sec-apply-saml-settings	Apply SAML settings	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-role-groups	Delete a role group	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-roles	Delete a role	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-users	Delete a user	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-edit-account-settings	Modify account security settings	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-ldap-settings	Apply LDAP settings	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-role-groups	Modify a role group	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-roles	Modify a role	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-users	Modify a user	lxc-recovery, lxc-security-admin, lxc-supervisor

Server configuration privileges

These privileges provide permissions to provision or preprovision servers using Configuration Patterns.

Privilege name	Privilege description	Default roles
lxc-cp-edit-management-ip	Modify management IP addresses for chassis	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-edit-preferences	Set Configuration Patterns Preferences	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-address-pools	Manage Address Pools	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-patterns	Manage Patterns	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-placeholders	Manage Placeholders	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-profiles	Deploy patterns, deploy placeholder to chassis and manage profiles	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-other-server-config	Reset local storage and apply Intel Optane DCPMM security operation	lxc-admin, lxc-hw-admin, lxc-supervisor

Service privileges

These privileges provide permissions to define support contacts for each managed device, collect and send service files to Lenovo Support, set up automatic notification to service providers when certain serviceable events occur on specific devices, view service-ticket status and warranty information, and collect and forward service data.

Privilege name	Privilege description	Default roles
lxc-ss-alter-backup-credentials	Modify backup FFDC credentials	lxc-admin, lxc-hw-admin, lxc-service-admin, lxc-supervisor
lxc-ss-call-home	Perform Call Home	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-recovery-password	Change service recovery password	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-tickets	Modify service tickets	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-remove-service-tickets	Delete service tickets	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-run-service-forwarders	Run service forwarders	lxc-admin, lxc-hw-admin, lxc-supervisor

Switch configuration privileges

These privileges provide permissions to configure switches and backup and restore switch configuration data.

Privilege name	Privilege description	default roles
lxc-netcfg-template-management	Create, modify, delete, and deploy switch-configuration templates, and delete a switch-configuration deployment	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-config-management	Backup, restore, delete, export, and import switch configuration-data files	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-port-management	Modify switch port status	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Creating a custom role group

A *role group* is a set of roles and a set of users that are members of the same set of roles. The level of access that is granted to each user in the role group is based on the roles that are assigned to that role group. XClarity Administrator provides the following predefined role groups, which correspond to each of the predefined roles. You can also create custom role groups.

About this task

Each XClarity Administrator user must be a member of at least one role group.

The following role groups are predefined in XClarity Administrator.

- **LXC-SUPERVISOR**. Includes the **lxc-supervisor** role.
- **LXC-ADMIN**. Includes the **lxca-admin** role.
- **LXC-SECURITY-ADMIN**. Includes the **lxc-security-admin** role.
- **LXC-HW-ADMIN**. Includes the **lxc-hw-admin** role.
- **LXC-FW-ADMIN**. Includes the **lxc-fw-admin** role.
- **LXC-OS-ADMIN**. Includes the **lxc-os-admin** role.
- **LXC-SERVICE-ADMIN**. Includes the **lxc-service-admin** role.
- **LXC-HW-MANAGER**. Includes the **lxc-hw-manager** role.

- **LXC-OPERATOR**. Includes the **lxc-operator** role.
- **LXC-RECOVERY**. Includes the **lxc-recovery** role.

The following predefined roles are *reserved* and cannot be used to create new role groups or assigned to new users.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procedure

To create a role group, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Role Groups** under the Users and Groups section to display the Group Management page.

Step 3. Click the **Create** icon ( ) to create a role group. The Create New Role Group dialog is displayed.

Step 4. Enter a group name and description.

Note: **Tip:** For the group name, you can use letters, numbers, white space, underscore, dashes, and periods.

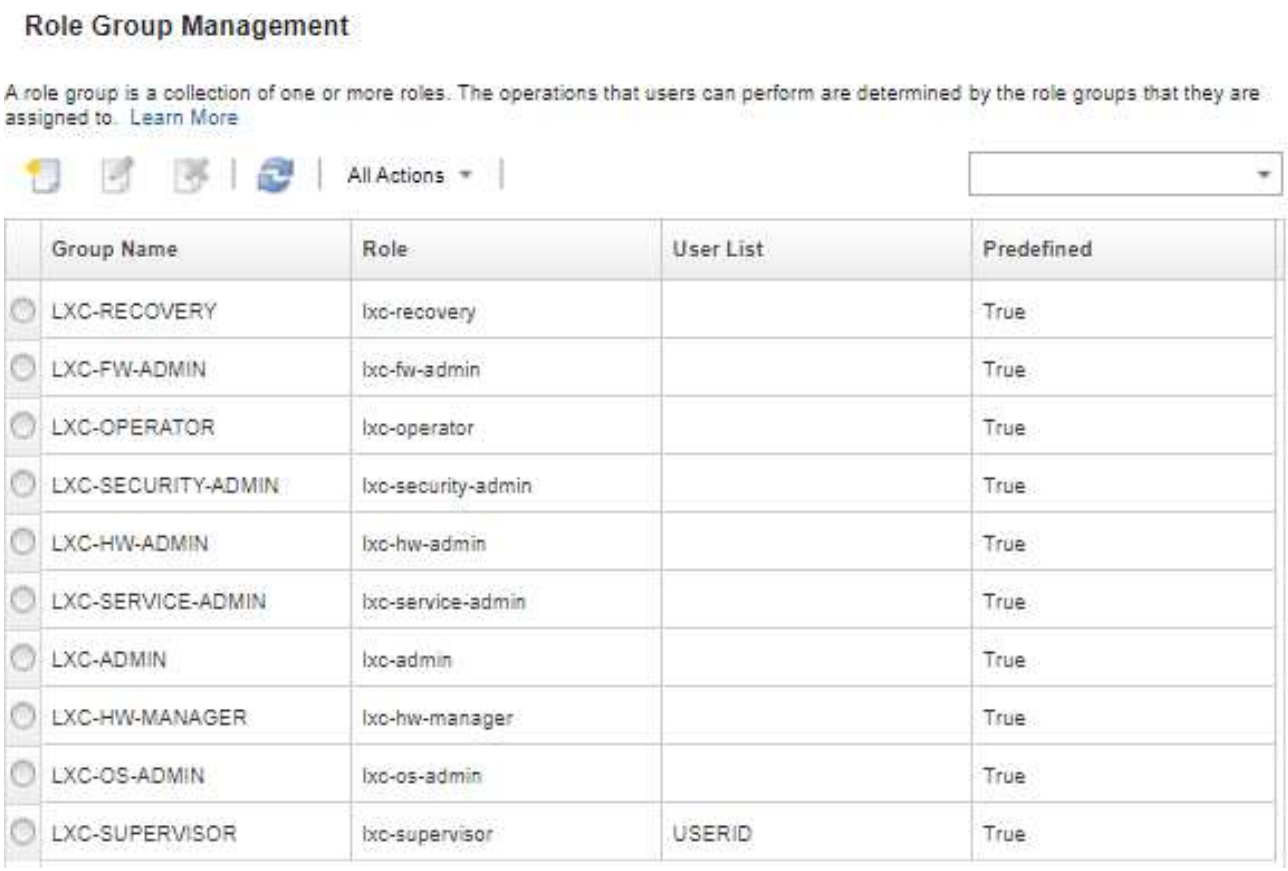
Step 5. Select one or more roles to assign to this role group.

Step 6. Select one or more users as members of this role group.

Step 7. Click **Create**. The new role group is added to the table on the Group Management page.

Results

The role group is displayed in the Role Groups table. The table shows the associated authorization roles and the members for each role group.



After you create a role group, you can perform the following actions on a selected role group:

- Add or remove roles that are assigned to this role group by clicking the **Edit** icon ( ).
- Add or remove users as members of the role group (see “Adding and removing multiple users from a role group” on page 55).
- Export information about the role groups, including access permissions, by clicking **All Actions → Export as CSV**.
- Delete the role group by clicking the **Delete** icon ( ).You cannot delete predefined role groups.

After a role group is created, edited, or deleted, the change is immediately provisioned to each managed device.

Adding and removing multiple users from a role group

You can change membership in a role group by adding or removing multiple users.

Procedure

Complete the following steps to add and remove users from a role group.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Role Groups** under the Users and Groups section to display the Group Management page.

Step 3. Click the **Edit** icon ( ) modify the role group. The Edit Role Group dialog is displayed.

Step 4. Click the **User List** drop-down list, and select the users to include or clear user to exclude from this role group.

Step 5. Click **Save**. The **User List** column displays the current user membership in the role group.

Managing access to devices

Access-control to devices is disabled by default and does not take effect until you enable it

When devices are initially managed by Lenovo XClarity Administrator, a predefined set of role groups have permission to access the devices by default. This predefined set is empty by default until it is configured.

You change the role groups that can access specific managed devices. When permission is given to certain role groups, only users that are members of those role groups can see and act on those specific devices.

Controlling access to specific devices

When devices are initially managed by Lenovo XClarity Administrator, a predefined set of role groups have permission to access the devices by default. You change the role groups that can access specific managed devices. When permission is given to certain role groups, only users that are members of those role groups can see and act on those specific devices.

Before you begin

Only users with **lxc-supervisor**, **lxc-security-admin**, or **lxc-recovery** authority can perform this action.

About this task

Access control is set on individual devices. It is not set for containers, such as racks and resource groups.

For components in a chassis or enclosure, users must have at least read-only access to the chassis or enclosure to the view components in that chassis or enclosure. If users do not have at least read-only access to the chassis or enclosure, those users might see the components in some views but are not guaranteed to see them in all views.

Users with **lxc-supervisor** authority can view and take actions on all resources regardless of whether they are in a role group that has specifically been given access to that resource. You cannot remove access to any resources for the **lxc-supervisor** role group.

If a user is not a member of a role group that has access to a specific managed device, the user cannot see or act on that specific device. This includes launching the management controller web interface through Lenovo XClarity Administrator. For Flex and System x devices, users also cannot directly log in to a CMM or management controller for which they do not have access.

The default access-control settings are used to set access permissions on devices when they are initially managed by XClarity Administrator and when resetting access permissions for a specific device to the default settings. Changing the default access-control settings does not automatically change access permissions on devices that are already managed.

Important:

- If a user is a member of more than one role group, and the role groups are assigned to different devices, then the actions that the user is allowed to perform on each device might be different. For example, if the user is a member of default role groups LXC-FW-ADMIN and LXC-OS-ADMIN, and if LXC-FW-ADMIN is granted access to Server A but LXC-OS-ADMIN has not been granted access to Server A, then that user would be able to update the firmware on Server A but would not be able to deploy an operating system to Server A. If LXC-OS-ADMIN had been granted access to Server B but LXC-FW-ADMIN had not been granted access to server B, then that same user would be able to deploy an operating system to Server B but would not be able to update the firmware on Server B.
- When limiting access to a device that has a parent resource (such as a server or switch in a Flex chasis), a user must have at least read-only permissions to the parent resource to interact fully with the device. If a

user has at least read-only access to the device but not the parent, the user will not able be see the device inventory views, but might be able to see about the device in some views, such as jobs and events.

For example, you can create a role group for the parent and assign that role group the **lxc-operator** role. Include all users who should be able to access any of the children (such as a server or switch in a Flex chasis), in that role group. Then, include that role group as one of the groups that has access to the parent.

Procedure

Complete the following procedures to control access to specific devices by associating role groups with those devices.

Step 1. From the main Lenovo XClarity Administrator menu, click **Administration → Security**.

Step 2. Click **Resource View** in the left navigation pane. The Resource View page is displayed.

You can sort the table columns to make it easier to find specific devices. In addition, you can select a device type in the **Resource Type** drop-down menu, select a role group in the **Role Groups** drop-down menu, select a resource group in the **Resource Groups**drop-down menu, and enter text (such as a resource name or type) in the **Filter** field to list only those devices that meet the selected criteria.

Step 3. Select one or more devices to which you want to control access.

Step 4. Click the **Edit** icon ( ). The Edit Resource dialog is displayed with the target devices listed in the **Resource Name** field.

Step 5. From the **Role Groups** drop-down list, select the role groups for which you want to allow access to the target devices.

Note: If the device has a parent resource (for example, a server or switch in a Flex chassis), you can specify access for both the device (right column) and the parent resource (left column).

Step 6. Set **Public Access** to `No`. This means that only users that are members of the selected role groups can access the target devices.

Step 7. Click **Save**.

Step 8. After you finish assigning permissions, click click the **Disabled** toggle to change **Resource Access Control** to enabled.

You can enable resource-access control at any time, either before or after configuring access to specific devices. When this setting is enabled, the configuration displayed in the table takes effect, including denying non-supervisor users access to any devices that do not have any groups configured to access them.

After you finish

You can also control access to devices by performing the following actions:

- Change the permissions to the default role groups and public access setting by clicking the **Edit** icon ( ) and then clicking **Rest to Defaults**.
- Change the default role group and public access setting (see Changing the default permissions.).
- Disable resource-access control by clicking the **Enabled** toggle to change **Resource Access Control** to disabled. This means that all role groups can access all managed devices.

Disabling resource-access control

You disable access control for all devices or specific devices so that all users can view and act on those devices.

About this task

Only users with **lxc-supervisor**, **lxc-security-admin**, or **lxc-recovery** authority can perform this action.

Procedure

Complete the following steps to disable resource-access control.

- For all managed devices
  1. From the main Lenovo XClarity Administrator menu, click **Administration → Security**.
  2. Click **Resource View** in the left navigation pane. The Resource View page is displayed.
  3. Click the **Enabled** toggle to change **Resource Access Control** to disabled.
- For specific managed devices
  1. From the main XClarity Administrator menu, click **Administration → Security**.
  2. Click **Resource View** in the left navigation pane. The Resource View page is displayed.

     You can sort the table columns to make it easier to find specific devices. In addition, you can select a device type in the **Resource Type** drop-down menu, select a role group in the **Role Groups** drop-down menu, select a resource group in the **Resource Groups** drop-down menu, and enter text (such as a resource name or type) in the **Filter** field to list only those devices that meet the selected criteria.
  3. Select one or more devices to which you want to change access.
  4. Click the **Edit** icon ( ). The Edit Resource dialog is displayed with the selected devices listed in the **Resource Name** field.
  5. Set **Public Access** to `Yes`. This means that all role groups can access the target devices regardless of the roles groups that are listed in the **Role Groups** drop-down list.
  6. Click **Save**.

Changing the default permissions

There are two settings that determine whether role groups can access devices when they are initially managed by Lenovo XClarity Administrator: public access and role groups. The public-access setting determines whether all or only a specific set of role groups can access the target devices. By default, this setting is set to `Yes`, which means that all role groups can access the target devices. You can change the default behavior by changing the public-access setting to `No` and then selecting the set of role groups that can access the target devices

About this task

Only users with **lxc-supervisor**, **lxc-security-admin**, or **lxc-recovery** authority can perform this action.

Users with the **lxc-supervisor**, **lxc-security-admin**, or **lxc-recovery** authority can access all managed devices. You cannot remove access to any device for these role groups.

The default access-control settings are used to set access permissions on devices when they are initially managed by XClarity Administrator and when resetting access permissions for a specific device to the default settings. Changing the default access-control settings does not automatically change access permissions on devices that are already managed.

Procedure

Complete the following procedures to change the default access controls.

Step 1. From the main XClarity Administrator menu, click **Administration → Security**.

Step 2. Click **Resource View** in the left navigation pane. The Resource View page is displayed.

You can sort the table columns to make it easier to find specific devices. In addition, you can select a device type in the **Resource Type** drop-down menu, select a role group in the **Role Groups** drop-down menu, select a resource group in the **Resource Groups**drop-down menu, and enter text (such as a resource name or type) in the **Filter** field to list only those devices that meet the selected criteria.

Step 3. Click **All Actions → Edit Default Resources**. The Edit Default Resources dialog is displayed.

Step 4. From the **Role Groups** drop-down list, select the role groups that you want to define as the default set.

Step 5. Select the default **Public Access** setting.

- **Yes**. When a device is initially managed, all role groups can access that device regardless of the roles groups that are listed in the **Role Groups** drop-down list.
- **No**. When a device is initially managed, only role groups that are listed in the **Role Groups** drop-down list can access that device by default.

Step 6. Click **Save**.

Implementing a secure environment

It is important that you evaluate the security requirements in your environment, understand all security risks, and minimize those risks. Lenovo XClarity Administrator includes several features that can help you secure your environment. Use the following information to help you implement the security plan for your environment.

About this task

Important: You are responsible for the evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls for your system environment. Implementing the security features that are described in this section does not secure your environment completely.

Consider the following information when you are evaluating the security requirements for your environment:

- The physical security of your environment is important; limit access to rooms and racks where systems-management hardware is kept.
- Use a software-based firewall to protect your network hardware and data from known and emerging security threats such as viruses and unauthorized access.
- Do not change the default security settings for the network switches and pass-thru modules. The manufacturing default settings for these components disable the use of unsecure protocols and enable the requirement for signed firmware updates.
- The management applications for the CMMs, baseboard management controllers, FSPs, and switches permit only signed firmware-update packages for these components to ensure that only trusted firmware is installed.
- Only the users who are authorized to update firmware components should have firmware-update authority.
- At a minimum, ensure that critical firmware updates are installed. After making any changes, always back up the configuration.
- Ensure that all security-related updates for DNS servers are installed promptly and kept up to date.
- Instruct your users to not accept any untrusted certificates. For more information, see Working with security certificates.

- Tamper-evident options are available for the Flex System hardware. If the hardware is installed in an unlocked rack or located in an open area, install the tamper-evident options to deter and identify intrusions. See the documentation that comes with your Flex System products for more information about the tamper-evident options.
- Where possible and practical, place the systems-management hardware in a separate subnet. Typically, only administrators should have access to the systems-management hardware, and no basic users should be given access.
- When you choose passwords, do not use expressions that are easy to guess, such as “password” or the name of your company. Keep the passwords in a secure place, and ensure that access to the passwords is restricted. Implement a password policy for your company.

  Important: Always change the default user name and password. Strong password rules should be required for all users.
- Establish power-on passwords for users as a way to control who has access to the data and setup programs on the servers. See the documentation that comes with your servers for more information about power-on passwords.
- Use the various authorization levels that are available for different users in your environment. Do not allow all users to work with the same supervisor user ID.
- Ensure that your environment meets the following NIST 800-131A criteria to support secure communications:
  - Use Secure Sockets Layer (SSL) over the TLS v1.2 protocol.
  - Use SHA-256 or stronger hashing functions for digital signatures and SHA-1 or stronger hashing functions for other applications.
  - Use RSA-2048 or stronger, or use NIST approved Elliptic Curves that are 224 bits or stronger.
  - Use NIST-approved symmetric encryption with keys at least 128 bits in length.
  - Use NIST-approved random-number generators.
  - Where possible, support Diffie-Hellman or Elliptic Curve Diffie-Hellman key-exchange mechanisms.

  For more information about cryptography settings, see Configuring cryptography settings. For more information about NIST settings, see Implementing NIST SP 800-131A compliance.

Changing the user-account security settings

The user-account security settings control the password complexity, account lockout, and web session inactivity timeout. You can change the values of the settings.

Procedure

Complete the following steps to override the user-account security settings that are in place.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Click **Account Security Settings** under the Users and Groups section to display the Users Management page.

Step 3. For each of the following setting that needs to change, select the new value.

Table 1. Account Security settings

Security setting	Description	Allowed values	Default values
Password expiration period	Amount of time, in days, that a user can use a password before it must be changed. Smaller values reduce the amount of time for attackers to guess passwords If set to **0**, passwords never expire. **Note:** This setting applies only when the user accounts are managed using the local authentication server. They are not used when the external authentication server is used.	**0 – 365**	**90**
Password expiration warning period	Amount of time, in days, before the password expiration date that users begin to receive warnings about the impending expiration of the user password If set to **0**, users are never warned. **Note:** This setting applies only when the user accounts are managed using the local authentication server. They are not used when the external authentication server is used.	**0 –** *maximum password expiration setting*	**5**
Minimum password reuse cycle	Minimum number of times that a user must enter a unique password when changing the password before the user can start to reuse passwords If set to **0**, users can reuse passwords immediately.	**0 – 10**	**5**
Minimum password change interval	Minimum amount of time, in hours, that must elapse before a user can change a password again after it was previously changed. The value specified for this setting cannot exceed the value specified for the password expiration period. If set to **0**, users can change passwords immediately.	**0 – 1440**	**24**
Maximum number of login failures	Maximum number of times that a user can attempt to log in with an incorrect password before the user account is locked out. The number specified for the lockout period after maximum login failures determines how long the user account is locked out. Accounts that are locked cannot be used to gain access to the system even if a valid password is provided. If set to **0**, accounts are never locked. The failed login counter is reset to zero after a successful login.	**0 – 100**	**20**

Table 1. Account Security settings (continued)

Security setting	Description	Allowed values	Default values
Lockout period after maximum login failures	Minimum amount of time, in minutes, that must pass before a user that was locked out can attempt to log back in again If set to **0**, the account remains locked until an administrator explicitly unlocks it. A setting of 0 might make your system more exposed to serious denial of service attacks, where deliberate failed login attempts can leave accounts permanently locked. **Tip:** Any user with the role of Supervisor can unlock a user account. For more information, see Unlocking a user. **Note:** This setting applies only when the user accounts are managed using the local authentication server. They are not used when the external authentication server is used.	**0 – 2880**	**60**
Web inactivity session timeout	Amount of time, in minutes, that a user session that is established with XClarity Administrator can be inactive before the user is logged out If set to **0**, the web session never expires. **Note:** When changing this value, only user sessions that start after the setting is changed are affected.	**0 – 1440**	**1440**
Minimum password length	Minimum number of characters that can be used to specify a valid password	**8 – 20**	**8**

Table 1. Account Security settings (continued)

Security setting	Description	Allowed values	Default values
Number of complexity rules that must be followed when creating a new password	Number of complexity rules that must be followed when creating a new password Rules are enforced starting with rule 1, and up to the number of rules specified. For example, if the password complexity is set to 4, then rules 1, 2, 3 and 4 must be followed. If the password complexity is set to 2, then rules 1 and 2 must be followed. XClarity Administrator supports the following password complexity rules. • (1) Must contain at least one alphabetic character, and must not have more than two sequential characters, including sequences of alphabetic characters, digits, and QWERTY keyboard keys (for example, “abc”, “123”, and “asd” are not allowed). • (2) Must contain at least one number (0 - 9). • (3) Must contain at least *two* of the following characters. – Uppercase alphabetic characters (A – Z) – Lowercase alphabetic characters (a – z) – Special characters ; @ _ ! ' $ & + • (4) Must not repeat or reverse the user name. • (5) Must not contain more than two of the same characters consecutively (for example, “aaa”, “111”, and “...” are not allowed). If set to **0**, passwords are not required to comply with any complexity rules.	**0 – 5**	**4**
Maximum active sessions for a specific user	Maximum number of active sessions for a specific user that is allowed at any given time If set to **0**, the number of allowed active sessions for a specific user is unlimited.	**1 – 20**	**3**
Force user to change password on first access	Indicates whether a user is required to change the password when the user logs in to XClarity Administrator for the first time	**Yes** or **No**	**Yes**

Step 4. Click **Apply**.

After you finish

When successfully saved, the new settings take effect immediately. If you change the setting for web inactivity session timeout, active sessions are affected.

If you change password policies, those policies are enforced the next time a user logs in or changes the password.

Configuring cryptography settings

Cryptographic management is composed of communication modes and protocols that control the way that secure communications are handled between Lenovo XClarity Administrator and the managed systems.

About this task

The *cryptographic mode* determines how secure communications are handled between XClarity Administrator and all managed systems. If secure communications are implemented, it sets the encryption-key lengths to be used.

Note: Regardless of the cryptography mode that you select, NIST-approved Digital Random Bit Generators are always used, and only 128-bit or longer keys are used for symmetric encryption.

When you change the cryptographic mode in the XClarity Administrator, the cryptographic mode for all CMMs and baseboard management controllers in the managed devices are changed to the same setting automatically. Consider the following implications of changing the cryptographic mode:

- If you switch from compatibility mode to NIST SP 800-131A mode and the current certificate authority on the managed CMMs and baseboard management controllers use RSA-2048/SHA-1 (the default), an RSA-2048/SHA-256 certificate is regenerated on each managed chassis and server. This causes a mismatch between the newly generated server certificates on the CMMs and baseboard management controllers and the server certificate that is stored in the XClarity Administrator trust store. To resolve this issue, go to the Chassis page and Servers page, and click **All Actions → Resolve Untrusted Certificate** for each device (see Resolving an untrusted server certificate in the XClarity Administrator online documentation).
- Not all Flex switches support NIST SP 800-131A mode. If a Flex switch does support NIST SP 800-131A mode, you might need to change the configuration for the switches through the Flex switch interface. For information about support for NIST SP 800-131A and about switching Flex switches between compatibility mode and NIST SP 800-131A mode, see the product documentation that is available for the Flex switches. For more information, see CMM Reset in the Flex Systems online documentation.

Procedure

To change the cryptography settings, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security**.

Step 2. Choose one of the following the cryptographic modes to use for secure communications:

- **Compatibility**. This mode is the default. It is compatible with older firmware versions, browsers, and other network clients that do not implement strict security standards that are required for compliance with NIST SP 800-131A.
- **NIST SP 800-131A**. This mode is designed to comply with the NIST SP 800-131A standard. XClarity Administrator is designed to always use strong cryptography internally and, where available, to use strong cryptography network connections. However, in this mode, network connections using cryptography that is not approved by NIST SP 800-131A is not permitted, including rejection of Transport Layer Security (TLS) certificates that are signed with SHA-1 or weaker hash.

  If you select this mode:

  – For all ports other than port 8443, all TLS CBC ciphers and all ciphers that do not support Perfect Forward Secrecy are disabled.

  – Event notifications might not be successfully pushed to some mobile-device subscriptions (see Forwarding events to mobile devices). External services, such as Android and iOS, present certificates that are signed with SHA-1, which is an algorithm that does not conform to the stricter requirements of NIST SP 800-131A mode. As a result, any connections to these services might fail with a certificate exception or a handshake failure.

  For more information about NIST SP 800-131A compliance, see Implementing NIST SP 800-131A compliance.

Step 3. Choose the minimum TLS protocol version to use for client connections to other servers (such as the LDAP client). There are two options:

- **TLSv1.2**. Enforces TLS v1.2 or later cryptography protocols on both XClarity Administrator and all managed endpoints used.

Step 4. Choose the minimum TLS protocol version to use for server connections (such as the web server). There are two options:

- **TLSv1.2**. Enforces TLS v1.2 or later cryptography protocols on both XClarity Administrator and all managed endpoints used.

Step 5. Choose the minimum TLS protocol version to use for the XClarity Administrator operating-system deployment and OS device-driver updates. There are two options:

- **TLSv1.2**. TLS v1.2 or later can be used.

  Only operating systems with an installation process that supports TLS 1.2 and stronger cryptographic algorithms can be deployed and updated through XClarity Administrator.

Step 6. Choose the devices to which you want to apply changes.
- **Apply to management server only**.
- **Apply to managed devices only**
- **Apply to management server and managed devices**

  When you apply the cryptographic-settings changes to managed devices, XClarity Administrator provisions the new settings to all managed devices and attempts to resolve any new certificates on those devices.

Step 7. If you applied the cryptographic-settings changes to the management server, restart XClarity Administrator (see Restarting XClarity Administrator).

After you finish

If you receive an alert that the server certificate is not trusted for a managed device, see Resolving an untrusted server certificate.

Working with security certificates

Lenovo XClarity Administrator uses SSL certificates to establish secure, trusted communications between XClarity Administrator and its managed devices (such as chassis and service processors in the System x servers) as well as communications with XClarity Administrator by users or with different services. By default, XClarity Administrator, CMMs, and baseboard management controllers use XClarity Administrator-generated certificates that are self-signed and issued by an internal certificate authority.

Before you begin

This section is intended for administrators that have a basic understanding of the SSL standard and SSL certificates, including what they are and how to manage them. For general information about public key certificates, see X.509 webpage in Wikipedia and Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC5280) webpage.

About this task

The default self-signed server certificate, which is uniquely generated in every instance of XClarity Administrator, provides sufficient security for many environments. You can choose to let XClarity Administrator manage certificates for you, or you can take a more active role and customize or replace the server certificates. XClarity Administrator provides options for customizing certificates for your environment. For example, you can choose to:

- Generate a new pair of keys by regenerating the internal certificate authority and/or the end server certificate that uses values that are specific to your organization.
- Generate a certificate signing request (CSR) that can be sent to your choice of certificate authority to sign a custom certificate that can then be uploaded to XClarity Administrator to be used as end-server certificate for all its hosted services
- Download the server certificate to your local system so that you can import that certificate into your web browser's list of trusted certificates.

XClarity Administrator provides several services that accept incoming SSL/TLS connections. When a client, such as a managed device or a web browser, connects to one of these services, XClarity Administrator provides its *server certificate* to be identified by the client attempting the connection. The client should maintain a list of certificates that it trusts. If XClarity Administrator's server certificate is not included in the client's list, the client disconnects from XClarity Administrator to avoid exchanging any security sensitive information with an untrusted source.

XClarity Administrator acts as a client when communicating with managed devices and external services. When XClarity Administrator connects to a device or external service, the device or external service provides its server certificate to be identified by XClarity Administrator. XClarity Administrator maintains a list of certificates that it trusts. If the *trusted certificate* that is provided by the managed device or external service is not listed, XClarity Administrator disconnects from the managed device or external service to avoid exchanging any security sensitive information with an untrusted source.

The following category of certificates is used by XClarity Administrator services and are supposed to be trusted by any client connecting to it.

- **Server Certificate**. During the initial boot, a unique key and self-signed certificate are generated. These are used as the default Root Certificate Authority, which can be managed on the Certificate Authority page in the XClarity Administrator security settings. It is not necessary to regenerate this root certificate unless the key has been compromised or if your organization has a policy that all certificates must be replaced periodically (see Regenerating or restoring the Lenovo XClarity Administrator self-signed server certificate).

  Also during the initial setup, a separate key is generated and a sever certificate is created and signed a certificate is created that is signed by the internal certificate authority. This certificate used as the default XClarity Administrator server certificate. It automatically regenerated each time XClarity Administrator detects that its networking addresses (IP or DNS addresses) have changed to ensure that the certificate contains the correct addresses for the server. It can be customized and generated on demand (see Regenerating or restoring the Lenovo XClarity Administrator self-signed server certificate).

  You can choose to use an externally-signed server certificate instead of the default self-signed server certificate by generating a certificate signing request (CSR), having the CSR signed by an private or commercial certificate Root Certificate Authority, and then importing the full certificate chain into XClarity Administrator (see Deploying customized server certificates to Lenovo XClarity Administrator).

  If you choose to use the default self-signed server certificate, it is recommended that you import the server certificate in your web browser as a trusted root authority to avoid certificate error messages in your browser (see Importing the Certificate Authority certificate into a web browser).
- **OS Deploy Certificate**. A separate certificate is used by the operating-system deployment service to ensure that the operating-system installer can connect securely to deployment service during the operating-system installation process. If the key has been compromised, you can regenerate it by restarting the management server.

The following category (trust stores) of certificates are used by XClarity Administrator clients.

- **Trusted Certificates**.

This trust store manages certificates that are used to establish a secure connection to local resources when XClarity Administrator acts as a client. Examples of local resources are managed devices, local software when forwarding event and an external LDAP server.

- **External-Services Certificates**. This trust store manages certificates that are used to establish a secure connection with external services when XClarity Administrator acts as a client. Examples of external services are online Lenovo Support services that are used to retrieve warranty information or create service tickets, external software (such as Splunk) to which events can be forwarded, and Apple and Google push-notification servers if Lenovo XClarity Mobile push notifications are enabled for an iOS or Android device. It contains preconfigured, trusted certificates from Root Certificate Authorities from certain commonly trusted and world-known certificate-authority providers, such as Digicert and Globalsign).

  When you configure XClarity Administrator to use a feature that requires a connection to another external service, refer to the documentation to determine if you need to manually add a certificate to this trust store.

  Note that certificates in this trust store are not trusted when establishing connections for other services (such as LDAP) unless you also add them to the main Trusted Certificates trust store. Removing certificates from this trust store prevents successful operation of these services.

XClarity Administrator supports PKCS 1.5 RSA-2048/SHA-256 certificate signatures and ECDSA p256/SHA-256 signatures in all product configurations. Other algorithms such as SHA-1 stronger or SHA hashes might be supported depending on your configuration. Consider the selected cryptographic mode in XClarity Administrator (see Configuring cryptography settings) and the capabilities of other software and devices in your environment. ECDSA certificates that are based on some elliptic curves (including p256), but not all elliptic curves, are supported on the Trusted Certificates page and in the signing chain of the XClarity Administrator certificate but *are not* currently supported for use by the XClarity Administrator server certificate.

Note: Only PKCS 1.5 RSA-2048/SHA-256 signatures are supported. RSA-PSS signatures are not supported at this time.

Installing a customized, externally signed server certificate

You can choose to use a server certificate that was signed by a private or commercial certificate authority (CA).

Before you begin

Ensure that the Root Certificate Authority is one that is generated by your organization and used to sign certificates within that organization or one that a commonly trusted and world-known (see List of Trusted Certifying Authorities webpage).

Ensure that the algorithms for the keys and signatures of the Root CA cert are supported. Only PKCS 1.5 RSA-2048/SHA-256 signatures are supported. RSA-PSS signatures are not supported at this time.

Ensure that all managed devices have the latest firmware installed before starting any task that might impact connections between the managed devices. To upgrade firmware on managed devices, see Updating firmware on managed devices.

Ensure that XClarity Administrator is successfully communicating with all managed devices by clicking **Hardware** and then clicking the device type (Chassis or Server). A page is displayed with a tabular view of all managed devices of that type. If any device has a status of “Offline,” ensure that network connectivity is working between the management server and the device, and resolve untrusted server certificates if needed (see Resolving an untrusted server certificate).

About this task

When you install a customized, externally-signed server certificate in XClarity Administrator or a baseboard management-controller or CMM, you must provide the certificate bundle that contains the entire CA signing chain.

When you install a customized server certificate in a chassis or server that is not managed by XClarity Administrator, install the certificate bundle on the CMM before installing it on all management controllers in the CMM.

When you install a customized server certificate to a managed chassis, you first add the CA signing chain to the XClarity Administrator trust store, install the server certificate on every management controller and CMM, and then upload the server certificate to XClarity Administrator. Note that this can easily be bypassed by trusting/adding all Root CA Certificates but not every certificate chain from every managed device. The number of imported certificates should be equal to the number of Root CA certificates (Root CA certificates + all intermediary CA certificates). For more information, see Deploying customized server certificates to managed devices.

You must add the CA root certificate and all intermediate certificates, one at a time, to the XClarity Administrator trust store. The order does not matter. Each certificate must be installed once, so if all devices use the same CA and intermediate certificates, then the CA and each intermediate certificate must be installed in the XClarity Administrator trust store one time. If more than one CA or an intermediate CA is used, ensure that each unique CA root certificate or intermediate certificate that is used in the signing chain of a managed device is imported the following these steps.

Tip: If the new server certificate has not been signed by a trusted third party, the next time that you connect to XClarity Administrator, your browser displays a security message and dialog prompting you to accept the new certificate into the browser. To avoid the security messages, you can import a downloaded server certificate into your web browser's list of trusted certificates. For more information about importing server certificates, see Importing the Certificate Authority certificate into a web browser.

Deploying customized server certificates to Lenovo XClarity Administrator

You can choose to generate a certificate signing request (CSR) for signing by your organization’s certificate authority or a third-party certificate authority. The CSR creates a full certificate chain that you can import and use in place of the unique default internally signed certificates.

Before you begin

Ensure that the certificate details include following requirements.

- Key Usage must contain
  - Key Agreement
  - Digital Signature
  - Key Encipherment
- Enhanced Key Usage must contain
  - Server Authentication (1.3.6.1.5.5.7.3.1)
  - Client Authentication (1.3.6.1.5.5.7.3.2)

About this task

Attention: If NIST SP 800-131A is enabled (see Implementing NIST SP 800-131A compliance) and you are using or plan to use custom or externally signed certificates in an NIST, all certificates in the chain must be based on SHA-256 hashing functions.

When the server certificate is uploaded, XClarity Administrator attempts to provision the new CA certificate to all managed devices. If the provisioning process succeeds, XClarity Administrator begins using the new server certificate immediately. If the process fails, error messages are provided that direct you to correct any problems manually before applying the newly imported server certificate. After the errors are corrected, complete the installation of the previously uploaded certificate.

Note: If XClarity Administrator was already using a certificate signed by the same root authority, the CA does not need to be sent to devices, and XClarity Administrator begins to use the certificate immediately.

After uploading a certificate in XClarity Administrator v1.1.0 and earlier, the web server restarted and automatically terminated all browser sessions. XClarity Administrator v1.1.1 and later begin using the new certificate without terminating existing sessions. Any new sessions are established using the new certificate. To see the new certificate in use, restart your web browser.

Procedure

To generate and deploy a customized externally signed server certificate to Lenovo XClarity Administrator, complete the following steps.

Step 1. Create and download a certificate signing request (CSR) for XClarity Administrator.

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

b. Click **Server Certificate** under the Certificate Management section to display the Server Certificate page.

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

d. Fill in the fields for the request.
- Country or Region
- State or Province
- City or Locality
- Organization
- Organization Unit (optional)
- Common Name

Attention: Select a common name that matches the IP address or hostname that XClarity Administrator uses to connect to the managed device. Failure to select the correct value might result in connections that are not trusted.

e. Customize the Subject Alternative Names (SANs) that are added to the X.509 “subjectAltName” extension when the CSR is generated.

By default, XClarity Administrator automatically defines Subject Alternative Names (SANs) for the CSR based on the IP address and hostname that are discovered by the XClarity Administrator guest operating system's network interfaces. You can customize, delete, or add to these SAN values.

The name that you specify must be valid for the selected type:
- **directoryName** (for example, `cn=lxca-example,ou=dcg,dc=company,dc=com`)
- **dNSName** (for example, `lxca-example.dcg.company.com`)
- **ipAddress** (for example, `192.0.2.0`)
- **registeredID** (for example, `1.2.3.4.55.6.5.99`)
- **rfc822Name** (for example, `example@company.com`)
- **uniformResourceIdentifier** (for example, `https://lxca-dev.dcg.company.com/example`)

Note: All SANs that are listed in the table are validated, saved, and added to the CSR only after you generate the CSR in the next step.

f. Click **Generate CSR File**. The server certificate is displayed in the Certificate Signing Request dialog.

g. Click **Save to File** to save the server certificate to the host server.

Step 2. Provide the CSR to a trusted certificate authority (CA). The CA signs the CSR and responds with a server certificate.

Step 3. Upload the externally signed server certificate to XClarity Administrator. The certificate content must be a bundle containing the CA's root certificate, any intermediate certificates, and the server certificate.

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

b. Click **Server Certificate** under the Certificate Management section.

c. Click the **Upload Certificate** tab.

d. Click **Upload Certificate** to display the Upload Certificate dialog.

e. Specify a certificate bundle file in PEM, DER or PKCS7 format, or paste the certificate bundle in PEM format.

f. Click **Upload** to upload the server certificate and store the certificate in the XClarity Administrator trust store.

Deploying customized server certificates to managed devices

You can deploy customized server certificates to managed devices by uploading and installing the externally-signed certificate bundle using the CMM and management controller for those devices.

Before you begin

Ensure that the latest firmware is installed on all managed devices (see Updating firmware on managed devices).

When generating a certificate signing request (CSR) for custom certificates, ensure that you select a common name that matches the IP address or hostname that is used to identify the device. Failure to select the correct value might result in connections that are not trusted.

Ensure that you obtain a certificate bundle that contains the entire signing chain, from the end-server certificate to the root (base) certificate of the trusted CA that can be used to verify the complete certificate chain of trust.

Do not change the Lenovo XClarity Administrator server certificate while a managed device is "Offline." You must repair the connection before modifying Lenovo XClarity Administrator, otherwise additional steps might be required to repair the connectivity issues (see Resolving an untrusted server certificate).

About this task

This section contains recommendations for ensuring continued successful communication between Lenovo XClarity Administrator and the managed devices. For detailed instructions about how to generate a CSR and import a signed certificate, see your device documentation.

If Lenovo XClarity Administrator is managing one or more chassis, rack servers, and tower servers, and the default Lenovo XClarity Administrator internally signed certificates are currently installed on Lenovo XClarity Administrator and the managed devices, you can deploy customized server certificate.

If the externally signed server certificate is installed on the device *before* the you attempt to manage the device by Lenovo XClarity Administrator, no additional steps are needed. To deploy a custom server

certificate to devices that are managed under Lenovo XClarity Administrator management, you must perform one of the following steps to ensure continued connectivity between the management server and the managed devices.

Procedure

Complete one of the following options to deploy the customized externally signed server certificate to managed chassis or servers.

- If Lenovo XClarity Administrator uses a certificate that is signed by the same certificate authority as the managed devices, perform the steps in Deploying customized server certificates to Lenovo XClarity Administrator *before* installing the certificates on managed devices. Installing the Lenovo XClarity Administrator certificate chain from the same CA first ensures that the certificate chain is in the Lenovo XClarity Administrator trust store and that Lenovo XClarity Administrator is able to trust the devices after the externally signed certificates are installed there.
- Add the externally signed certificates in the CA signing chains to the Lenovo XClarity Administrator trust store.

  You must add the CA root certificate and all intermediate certificates, one at a time, to the Lenovo XClarity Administrator trust store. The order does not matter. Each certificate must be installed once, so if all devices use the same CA and intermediate certificates, then the CA and each intermediate certificate must be installed in the Lenovo XClarity Administrator trust store one time. If more than one CA or an intermediate CA is used, ensure that each unique CA root certificate or intermediate certificate that is used in the signing chain of a managed device is imported the following these steps.

  Note: Do not add the end, non-CA server certificates during these steps.

  Perform the following steps for each certificate in the bundle.

  1. From the Lenovo XClarity Administrator menu bar, click **Administration → Security** to display the Security page.
  2. Click **Trusted certificates** under Certificate Management in the left navigation.
  3. Click the **Create** icon ( ) to display the Add Certificate dialog.
  4. Specify a certificate file in PEM or DER format, or paste the certificate in PEM format.
  5. Click **Create** to create the certificate.

  After the CA signing chain is installed, Lenovo XClarity Administrator trusts connections to CIM servers on the CMM and management controller on which the externally signed server certificate is installed.
- Import the externally signed certificates into the managed devices.

  Note: If the necessary certificates are not present in the Lenovo XClarity Administrator trust store, connectivity is lost between Lenovo XClarity Administrator and the managed device. Perform the steps in Resolving an untrusted server certificate to repair the connection.

  Important: This option involves temporary connectivity loss; therefore, one of the previous options is recommended.

Regenerating or restoring the Lenovo XClarity Administrator self-signed server certificate

You can generate a new certificate authority or server certificate to replace current self-signed certificates or to reinstate a Lenovo XClarity Administrator-generated certificate if XClarity Administrator currently uses a customized externally-signed server certificate. The new self-signed server certificate is then used by the authentication, HTTPS, and CIM servers on the XClarity Administrator. It is also automatically provisioned to all managed devices.

Before you begin

When you regenerate or upload the XClarity Administrator certificate, XClarity Administrator is restarted.

If a new CA certificate is generated, the new CA certificate is automatically deployed to the trust store in each CMM and baseboard management controller in all managed chassis, rack servers, and tower servers to maintain trusted authentication-server connections. If an error occurs while deploying the CA root certificate, download it from the Certificate Authority page and import it manually into the trust store of any managed devices to which it was not successfully provisioned before generating a new server certificate.

If you plan to regenerate the CA certificate, reserve time to regenerate the CA, resolve any provisioning errors, and regenerate the server certificate within a short period of time.

After generating a new CA root certificate, communication errors might occur, or you might not be able to log in to a device until after the server certificate is regenerated and signed.

Important: For XClarity Administrator v1.1.1 and earlier, you must import the CA root certificate into the trust store of each CMM and management controller. See the documentation for the CMM and management controller for more information about importing the CA root certificate

Procedure

Complete the following steps to restore a self-signed server certificate on XClarity Administrator.

Note: The server certificate that is currently in use on XClarity Administrator, whether self-signed or externally-signed, remains in use until new server certificate is regenerated and signed.

Step 1. Optional: **Optional:** Generate a new CA root certificate.

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

b. Click **Certificate Authority** under the Certificate Management section.

c. Click **Regenerate Certificate Authority Root Certificate**.

If the CA key and certificate are successfully regenerated, then a dialog is displayed showing the status of jobs to provision that certificate as an LDAP trusted certificate to all CMMs and management controllers (for Converged, NeXtScale, and System x servers). This dialog as well as the job monitoring page shows the success or failure of each of those provisioning jobs.

If any of the provisioning jobs fail, complete the following steps to download the CA root certificate, then manually import the root certificate as a trusted LDAP certificate in any device for which the job failed.

Step 2. Optional: **Optional:** Download the CA root certificate to the host system and import it into your web browser.

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

b. Click **Certificate Authority** under the Certificate Management section.

c. Click **Download Certificate Authority Root Certificate**. The current CA root certificate is displayed in the Certificate Authority Root Certificate dialog.

d. Click **Save to File** to save the CA root certificate to the host system.

e. Follow the instructions for your web browser and the web browser of other users who will access XClarity Administrator to import the certificate as a trusted root authority.

Step 3. Regenerate a new server certificate and sign the certificate with the new CA root certificate.

a. From the Security page, click **Server Certificate** under the Certificate Management section.

b. Click the **Regenerate Server Certificate** tab.

c. Fill in the fields in the Regenerate Server Certificate page:
   - Country or Region
   - State or Province
   - City or Locality
   - Organization
   - Organization Unit
   - Common Name
   - Not valid before date
   - Not valid before time
   - Not valid after date
   - Not valid after time

d. Click **Regenerate Certificate**.

e. If regenerating self-signed certificates on the managed CMMs and management controllers (for Converged, NeXtScale, ThinkSystem, and System x servers), after regenerating the certificate on each device, import the new device certificate into the XClarity Administrator trust store (see Resolving an untrusted server certificate). Alternatively, you can manually download the certificate from the device and import it into XClarity Administrator on the Trusted Certificates page.

For XClarity Administrator v1.1.0 and earlier, the web server restarts and automatically terminates all browser sessions after regenerating a certificate. For XClarity Administrator v1.1.1 and later, XClarity Administrator begins using the new certificate without terminating existing sessions. New sessions are established using the new certificate. To see the new certificate in use, restart your web browser.

Step 4. If regenerating self-signed certificates on the managed CMMs and management controllers (for Converged, NeXtScale, ThinkSystem, and System x servers), after regenerating the certificate on each device, import the new device certificate into the XClarity Administrator trust store (see Resolving an untrusted server certificate). Alternatively, you can manually download the certificate from the device and import it into XClarity Administrator on the Trusted Certificates page.

Resolving an untrusted server certificate

The server certificate that is used to establish a secure connection to a managed device can become untrusted. If the problem is due to a down-level version of the device CA root certificate or device self-signed certificate in the Lenovo XClarity Administrator trust store, XClarity Administrator can resolve the untrusted server certificate.

About this task

If a managed device becomes untrusted, XClarity Administrator prevents communication with that device, preventing you from performing management or inventory operations on that device.

Procedure

To resolve an untrusted server certificate for a managed device, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware**, and then click the device type (**Chassis**, **Server**, **Storage**, or **Switch**). A page is displayed with a tabular view of all managed devices of that type.

Step 2. Select a specific device in the “Offline” state.

Step 3. Click **All Actions → Security → Resolve Untrusted Certificates**.

Step 4. Click **Install Certificate**.

XClarity Administrator retrieves the current certificate from the target device. If that certificate is different from the trusted certificate for that device in the XClarity Administrator trust store, the new certificate is placed in the XClarity Administrator trust store, overriding the previous certificate for that device.

If this does not resolve the issue, ensure that network connectivity is working between XClarity Administrator and the device.

Downloading the server certificate

You can download a copy of the current server certificate, in PEM or DER format, to your local system. You can then import the certificate into your web browser or another applications (such as Lenovo XClarity Mobile or Lenovo XClarity Integrator).

Procedure

Complete the following steps to download the server certificate.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

Step 2. Click **Server Certificate** under the Certificate Management section. The Server Certificate page is displayed.

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

Step 4. Click **Download Certificate**.

Step 5. Click **Save as der** or **Save as pem** to save the server certificate as a DER or PEM file on your local system.

Importing the Certificate Authority certificate into a web browser

To avoid security warning messages from your web browser when you access Lenovo XClarity Administrator, you can download a copy of the current Certificate Authority (CA) certificate, in PEM or DER format, to your local system, and then import that certificate into your web browser's list of trusted certificates.

About this task

XClarity Administrator supports PKCS 1.5 RSA-2048/SHA-256 certificate signatures and ECDSA p256/SHA-256 signatures in all product configurations. Other algorithms such as SHA-1 stronger or SHA hashes might be supported depending on your configuration. Consider the selected cryptographic mode in XClarity Administrator (see Configuring cryptography settings) and the capabilities of other software and devices in your environment. ECDSA certificates that are based on some elliptic curves (including p256), but not all elliptic curves, are supported on the Trusted Certificates page and in the signing chain of the XClarity Administrator certificate but *are not* currently supported for use by the XClarity Administrator server certificate.

Note: Only PKCS 1.5 RSA-2048/SHA-256 signatures are supported. RSA-PSS signatures are not supported at this time.

Procedure

To download the server certificate, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

Step 2. Click **Certificate Authority** under the Certificate Management section. The Certificate Authority page is displayed.

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

Step 4. Click **Save as der** or **Save as pem** to save the server certificate as a DER or PEM file on your local system.

Step 5. Import the downloaded certificate into the list of trusted root authority certificates for your browser.

- **Firefox:**
  1. Open the browser, and click **Tools → Options → Advanced**.
  2. Click the **Certificates** tab.
  3. Click **View certificates**.
  4. Click **Import**, and browse to the location where the certificate was downloaded.
  5. Select the certificate, and click **Open**.
- **Internet Explorer:**
  1. Open the browser and click **Tools → Internet Options → Content**.
  2. Click **Certificates** to see a list of all certificates that are currently trusted.
  3. Click **Import** to display the Certificate Import wizard.
  4. Complete the wizard to import the certificate.

Adding and replacing a certificate revocation list

A *certificate revocation list* is a list of certificates that have been revoked and are no longer trusted. A certificate might be revoked if it was incorrectly issued from by the CA or if its key is compromised, lost, or stolen.

Procedure

Complete the following steps to add a new certificate revocation list or to replace an existing certificate revocation list.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Security** to display the Security page.

Step 2. Click **Certificate Revocation Lists** under Certificate Management in the left navigation. The Certificate Revocation Lists page is displayed with a list of all certificate revocation lists.

Step 3. Click **Add / Replace CLR** to add a certificate revocation list, or select a certificate revocation list and click the **Add / Replace CLR** to replace the CRL.

Step 4. Specify a certificate revocation list file, in PEM or DER format, or paste the certificate in PEM format.

Step 5. Click **Create** to create the certificate revocation list.

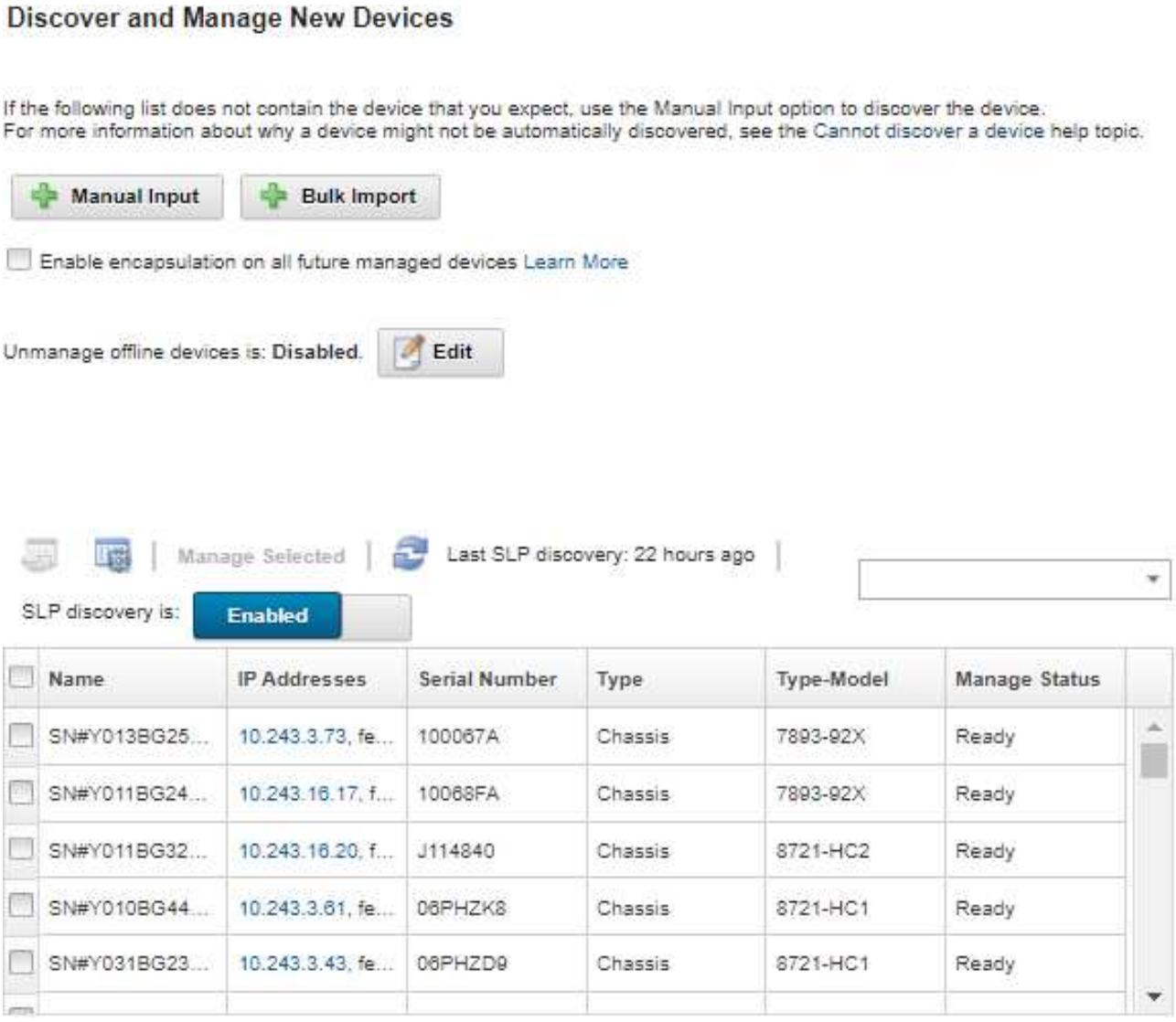
Enabling encapsulation

When you manage Lenovo chassis and servers in Lenovo XClarity Administrator, you can configure Lenovo XClarity Administrator to change the firewall rules for the devices so that incoming requests are accepted only from Lenovo XClarity Administrator. This is referred to as *encapsulation*. You can also enable or disable encapsulation on chassis and servers that are already managed by Lenovo XClarity Administrator.

When enabled on devices that support encapsulation, Lenovo XClarity Administrator changes the device encapsulation mode to “encapsulationLite,” and changes the firewall rules on the device to limit incoming requests from only this Lenovo XClarity Administrator.

When disabled, the encapsulation mode is set to “normal”. If encapsulation was previously enabled on the devices, the encapsulation firewall rules are removed.

You can enable or disable encapsulation globally for all devices during the management process by selecting the **Enable encapsulation on all future managed devices** checkbox on the Discover and Manage New Devices page. The encapsulation is disabled by default.



You can also enable or disable encapsulation individually for specific managed devices at any time by navigating to the device summary page, selecting the device, and clicking **Actions → Enable Encapsulation** or **Actions → Disable Encapsulation**.

Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.

Note: Encapsulation is not supported on switches, storage devices, and non-Lenovo chassis and servers.

Implementing NIST SP 800-131A compliance

If you must be compliant with NIST SP 800-131A, you can begin to work toward a fully compliant environment using Lenovo XClarity Administrator.

About this task

The National Institute of Standards and Technology Special Publication 800-131A (NIST SP 800-131A) specifies the way that secure communications should be handled. The standard strengthens algorithms and increases key lengths to improve security. The NIST SP 800-131A standard requires that users be configured for strict enforcement of the standard.

Notes: The following Flex System components do not currently support NIST SP 800-131A. Communications between XClarity Administrator or the CMM and these components are not compliant:

- Flex System EN4023 10 Gb Scalable Switch
- Flex System EN6131 40 Gb Ethernet Switch
- Flex System FC3171 8 Gb SAN Switch
- Flex System FC5022 16 Gb SAN Scalable Switch
- Flex System IB6131 Infiniband Switch

Note: When an SAML identity provider is used for authentication, XClarity Administrator uses SHA-1 to sign the signature in the metadata. Using the SHA-1 algorithm for digital signatures is not NIST SP 800-131A compliant.

Procedure

To implement NIST SP 800-131A compliance, complete the following steps.

Step 1. Ensure that your devices meet the following criteria:

- Use Secure Sockets Layer (SSL) over the TLS v1.2 protocol.
- Use SHA-256 or stronger hashing functions for digital signatures and SHA-1 or stronger hashing functions for other applications.
- Use RSA-2048 or stronger, or use NIST approved Elliptic Curves that are 224 bits or stronger.
- Use NIST-approved symmetric encryption with keys at least 128 bits in length.
- Use NIST-approved random-number generators.
- Where possible, support Diffie-Hellman or Elliptic Curve Diffie-Hellman key-exchange mechanisms.

Step 2. Configure the cryptographic settings on Lenovo XClarity Administrator. There are two settings that are related to NIST SP 800-131A compliance:

- The *SSL/TLS mode* specifies the protocols that are to be used for secure communications. The XClarity Administrator supports a setting of **TLS 1.2 Server and Client** to restrict the cryptography protocol to TLS 1.2 on XClarity Administrator and all managed devices.
- If secure communications are implemented, the *cryptographic mode* sets the encryption key lengths that are to be used. You can set the cryptographic mode as **NIST SP 800-131A**. However, you might not be able to deploy some operating systems through XClarity Administrator because some operating-system installers do not support the restricted settings. To support operating system deployment, you can choose to allow an exception for operating-system deployment.

When you change any cryptographic settings, XClarity Administrator provisions the new settings to all managed devices and attempts to resolve any new certificates on those devices.

Note: You must manually restart XClarity Administrator after cryptographic settings are changed for the changes to take effect and to restore any lost services (see Restarting XClarity Administrator).

For more information about these settings, see Configuring cryptography settings.

Step 3. Use a web browser that supports the TLS1.2 protocol and SHA-256 hashing functions, and enable those settings in your web browser.

Note: If you use or plan to use custom or externally signed certificates, all certificates in the chain must be based on SHA-256 hashing functions.

Step 4. Use encrypted protocols for all communications. Do not enable unencrypted protocols, such as Telnet, FTP, and VNC for remote communications with XClarity Administrator managed devices.

Using VMware Tools

The VMware Tools package is installed in the virtual machine's guest operating system when you install Lenovo XClarity Administrator in VMware ESXi-based environments. This package provides a subset of the VMware tools that support optimized virtual-appliance backup and migration while preserving application state and continuity.

For information about using the VMware Tools, see Using the VMware Tools Configuration Utility in the VMware vSphere Documentation Center website.

Configuring network access

When you initially set up Lenovo XClarity Administrator, you configure up to two network interfaces. In addition, you must specify which of those interfaces is to be used to deploy operating systems. After the initial setup, you can modify these settings.

Before you begin

Attention:

- Changing the XClarity Administrator IP address after managing devices might cause the devices to be placed in offline state in XClarity Administrator. Ensure that all devices are unmanaged before changing the IP address.
- You can enable or disable checking for duplicate IP addresses in the same subnet by clicking the **Duplicate IP address checking** toggle. It is disabled by default. When enabled, XClarity Administrator raises an alert if you attempt to change the IP address of XClarity Administrator or manage a device that has the same IP address as another device that is under management or another device found in the same subnet.
- When running XClarity Administrator as a virtual appliance, if the network interface for the management network is configured to use the Dynamic Host Configuration Protocol (DHCP), the management-interface IP address might change when the DHCP lease expires. If the IP address changes, you must unmanage the chassis, rack and tower servers, and then manage them again. To avoid this problem, either change the management interface to a static IP address, or ensure that the DHCP server configuration is set so that the DHCP address is based on a MAC address or that the DHCP lease does not expire.
- If you *do not* intend to use XClarity Administrator to deploy operating system or update OS device drivers, you can disable Samba and Apache servers by changing the network interface to use the **discover and manage hardware only** option. Note that the management server is restarted after changing the network interface.
- When running XClarity Administrator as a container:
  - You can only enable or disable duplicate IP address checking, modify the network interface roles, and modify proxy settings. All other network settings (including IP address, gateway, and DNS) are defined in the container setup.
  - Ensure that a macvlan network is set up on the host system.

About this task

XClarity Administrator has two separate network interfaces that can be defined for your environment, depending on the network topology that you implement. For virtual appliances, these networks are named eth0 and eth1. For containers, you can choose custom names.

- When only one network interface (eth0) is present:
  - The interface must be configured to support the device discovery and management (such as server configuration and firmware updates). It must be able to communicate with the CMMs and Flex switches in each managed chassis, the baseboard management controller in each managed server, and each RackSwitch switch.
  - If you intend to acquire firmware and OS device-driver updates using XClarity Administrator, the network interface must be connected to the Internet, preferably through a firewall. Otherwise, you must manually import updates into the repository.
  - If you intend to collect service data or use automatic problem notification (including Call Home), the interfaces must be connected to the Internet, preferably through a firewall.
  - If you intend to deploy operating-system images and update OS device drivers, the interface must have IP network connectivity to the server network interface that is used to access the host operating system.

    Note: If you implemented a separate network for OS deployment and OS device-driver updates, you can configure the second network interface to connect to that network instead of the data network. However, if the operating system on each server does not have access to the data network, configure an additional interface on the servers to provide connectivity from the host operating system to the data network for OS deployment and OS device-driver updates, if needed
- When two network interfaces (eth0 and eth1) are present:
  - The first network interface (typically the Eth0 interface) must be connected to the management network and configured to support the device discovery and management (including server configuration and firmware updates. It must be able to communicate with the CMMs and Flex switches in each managed chassis, the management controller in each managed server, and each RackSwitch switch.
  - The second network interface (typically the eth1 interface) can be configured to communicate with an internal data network, a public data network, or both.
  - If you intend to acquire firmware and OS device-driver updates using XClarity Administrator, the interface that you use for the management network must be connected to the Internet, preferably through a firewall. Otherwise, you must import updates into the repository.
  - If you intend to collect service data or use automatic problem notification (including Call Home and Lenovo Upload Facility), at least one of the network interfaces must be connected to the Internet, preferably through a firewall.
  - If you intend to deploy operating-system images and update device drivers, you can choose to use either eth1 or eth0 interface. However, the interface that you use must have IP network connectivity to the server network interface that is used to access the host operating system.

    Note: If you implemented a separate network for OS deployment and OS device-driver updates, you can configure the second network interface to connect to that network instead of the data network. However, if the operating system on each server does not have access to the data network, configure an additional interface on the servers to provide connectivity from the host operating system to the data network for OS deployment and OS device-driver updates, if needed
  - Other XClarity Administrator functions (including discovery and hardware management, server configuration, firmware downloads and updates, service-data collection, automatic problem notification, and warranty data retrieves) can be performed from either interface.

The following table shows possible configurations for the XClarity Administrator network interfaces based on the type of network topology that has been implemented in your environment. Use this table to determine how to define each network interface.

Table 2. Role of each network interface based on network topology

Network topology	Role of interface 1 (eth0)	Role of interface 2 (eth1)
Converged network (management and data network with support for OS deployment and OS device-driver updates)	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval • OS deployment • OS device-driver updates	None
Separate management network with support for OS deployment and OS device-driver updates and data network	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval • OS deployment • OS device-driver updates	Data network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval
Separate management network and data network with support for OS deployment and OS device-driver updates	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval	Data network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval • OS deployment • OS device-driver updates
Separate management network and data network without support for OS deployment and OS device-driver updates	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval	Data network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval
Management network only (OS deployment and OS device-driver updates is not supported)	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval	None

For more information about XClarity Administrator network interfaces including IPv6 address limitations, see Network considerations in the XClarity Administrator online documentation.

Procedure

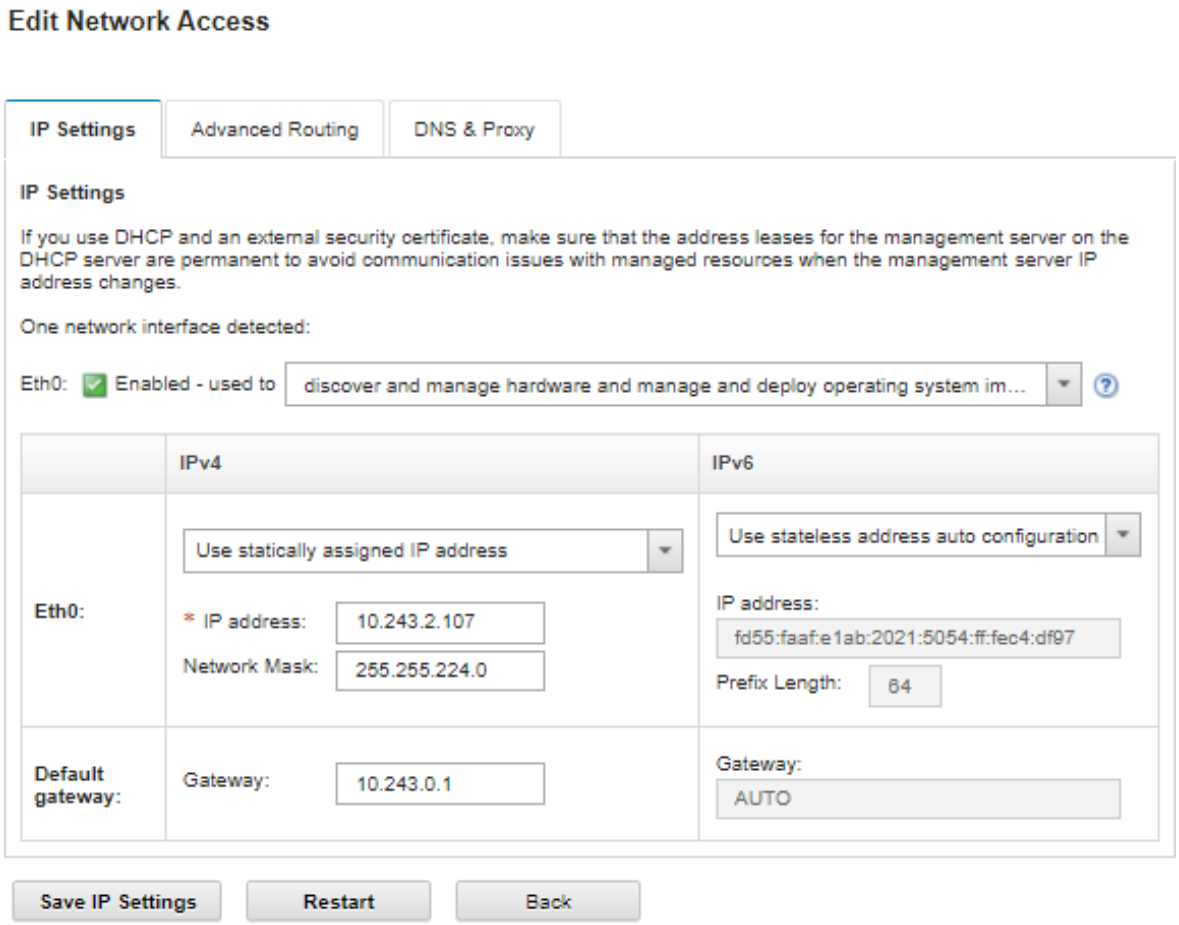
To configure network access, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Network Access**. The current network settings are displayed.

Step 2. Optionally enable checking for duplicate IP addresses in the same subnet by clicking the **Duplicate IP address checking** toggle.

When enabled, XClarity Administrator raises an alert if you attempt to change the IP address of XClarity Administrator or manage a device that has the same IP address as another device that is under management or another device found in the same subnet.

Step 3. Click **Edit Network Access** to display the Edit Network Access page.



Step 4. If you intend to deploy operating-systems and update OS device drivers using XClarity Administrator, choose the network interface to use for managing operating systems.

- If only one interface is defined for XClarity Administrator, choose whether that interface is to be used to discover and manage hardware only, or whether it is also to be used to manage operating systems.
- If two interfaces are defined for XClarity Administrator (Eth0 and Eth1), determine which interface is to be used to manage operating systems. If you choose “None”, you *cannot* deploy operating-system images or update OS device drivers to managed servers from XClarity Administrator.

Step 5. (XClarity Administrator as a virtual appliance only) Modify the IP Settings.

a. For the first interface, specify the IPv4 address, IPv6 address, or both.

- **IPv4**. You must assign an IPv4 address to the interface. You can choose to use a statically assigned IP address or obtain an IP address from a DHCP server.
- **IPv6**. Optionally, you can assign an IPv6 address to the interface using one of the following assignment methods:
  - Use statically assigned IP address
  - Use stateful address configuration (DHCPv6)
  - Use stateless address auto configuration

  Note: For information about IPv6 address limitations, see IPv6 configuration limitations in the XClarity Administrator online documentation.

b. If a second interface is available, specify the IPv4 address, the IPv6 address, or both.

Note: The IP addresses that are assigned to this interface must be in a different subnet from the IP addresses that are assigned to the first interface. If you choose to use DHCP to assign IP addresses for both interfaces (Eth0 and Eth1), the DHCP server must not assign the same subnet for the IP addresses of the two interfaces.

- **IPv4**. You can choose to use a statically assigned IP address or obtain an IP address from a DHCP server.
- **IPv6**. Optionally, you can assign an IPv6 address to the interface using one of the following assignment methods:
  - Use statically assigned IP address
  - Use stateful address configuration (DHCPv6)
  - Use stateless address auto configuration

c. Specify the default gateway.

If you specify a default gateway, it must be a valid IP address and must use the same network mask (the same subnet) as the IP address for one of the network interfaces (Eth0 or Eth1). If you use a single interface, default gateway must be on the same subnet as network interface.

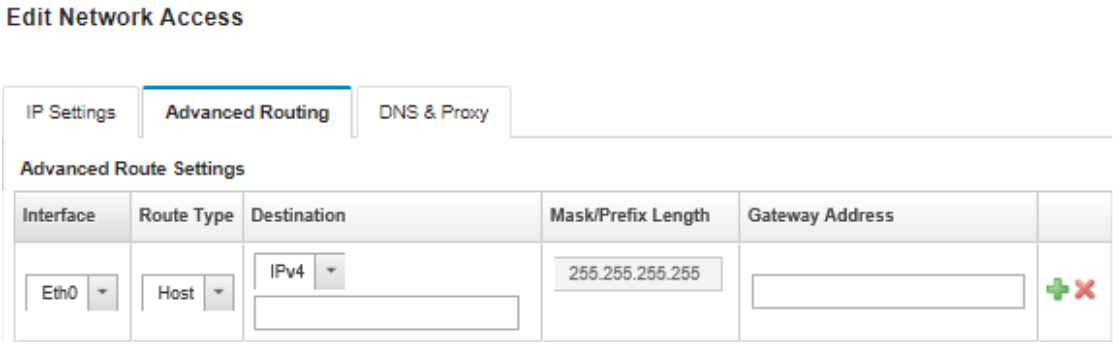
Tip: The default gateway must use the same network mask (the same subnet) as at least one enabled interface. Therefore, if you assign the default gateway to be on the same subnet as the second interface and then change the IP address assignment method or disable the second interface, the default gateway might not be reachable.

If either interface uses DHCP to obtain an IP address, the default gateway also uses DHCP.

d. Click **Save IP Settings**.

Step 6. (XClarity Administrator as a virtual appliance only) Optionally, modify the advanced settings.

a. Click the **Advanced Routing** tab.



b. Specify one or more route entries in the **Advanced Route Settings** table to be used by this interface.

To define one or more route entries, complete the following steps.

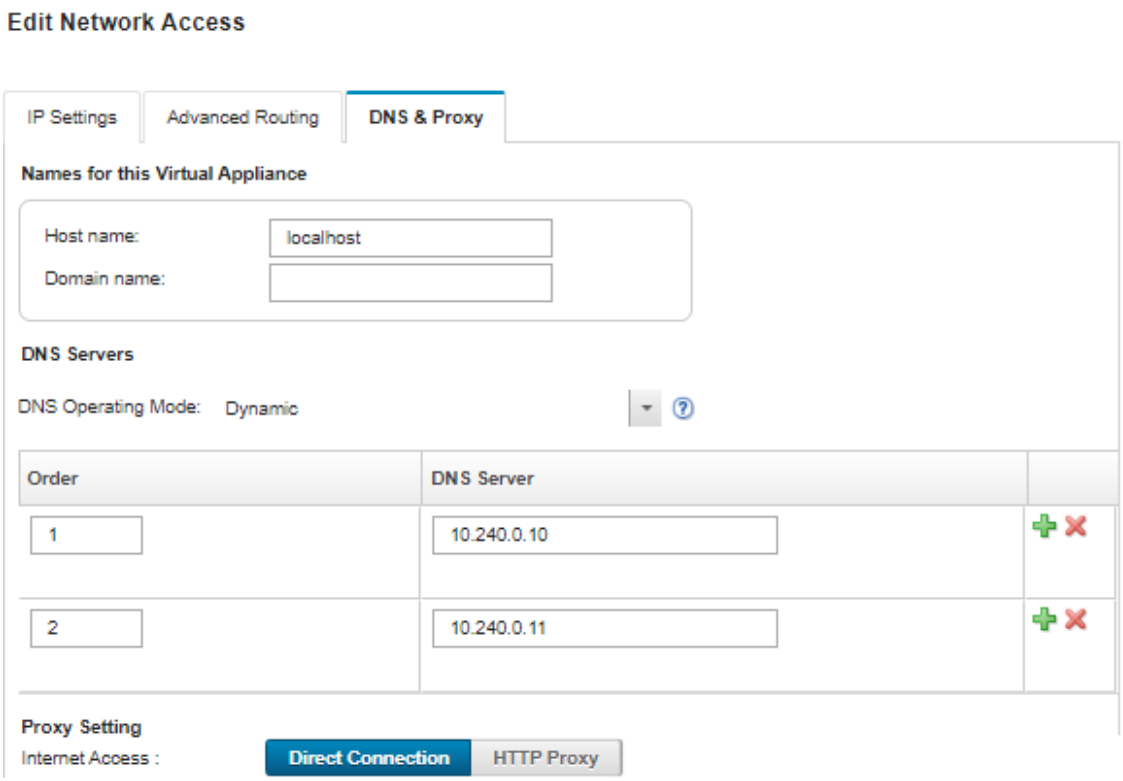
1. Choose the interface.
2. Specify the route type, which can be a route to another host or to a network.
3. Specify the destination host or network address to which you are directing the route.
4. Specify the subnet mask for the destination address.
5. Specify the gateway address to which packets are to be addressed.

c. Click **Save Advanced Routing**.

Step 7. Optionally, modify the DNS and proxy settings.

When XClarity Administrator is setup as a container, only proxy settings can be modified form the web interface. The DNS settings are defined in the container.

a. Click the **DNS & Proxy** tab.



b. Specify the hostname and domain name to be used for XClarity Administrator.

c. Select the DNS operating mode. This can be **Static** or **DHCP**.

Note: If you choose to use a DHCP server to obtain the IP address, any changes that you make to the **DNS Server** fields are overwritten the next time XClarity Administrator renews the DHCP lease.

d. Specify the IP address of one or more Domain Name System (DNS) servers to be used, and the priority order for each.

e. Specify whether to access the Internet using a direct connection or an HTTP proxy (if XClarity Administrator has access to the Internet).

Notes: If using a HTTP proxy, ensure that the following requirements are met.

- Ensure that the proxy server is set up to use basic authentication.
- Ensure that the proxy server is set up as a non-terminating proxy.
- Ensure that the proxy server is set up as a forwarding proxy.

- Ensure that load balancers are configured to keep sessions with one proxy server and not switch between them.

If you choose to use an HTTP proxy, complete the required fields:

1. Specify the proxy server hostname and port.
2. Choose whether to use authentication, and specify the user name and password if required.
3. Specify the proxy test URL.
4. Click **Text Proxy** to verify that the proxy settings are configured and working correctly.

f. Click **Save DNS & Proxy**.

Step 8. Click **Restart** to restart the management server.

Step 9. Click **Test Connection** to verify the network settings.

Setting the date and time

You can set the date and time to be used for Lenovo XClarity Administrator.

Before you begin

You must use at least one (and up to four) Network Time Protocol (NTP) server to synchronize the time stamps for all events that are received from managed devices with XClarity Administrator.

Tip: The NTP server must be accessible over the management network (typically the Eth0 interface). Consider setting up the NTP server on the host where XClarity Administrator is running.

If you change the time on the NTP server, it might take a while for XClarity Administrator to synchronize with the new time.

Attention: The XClarity Administrator virtual appliance and its host must be set to synchronize to the same time source to prevent inadvertent time mis-synchronization between XClarity Administrator and its host. Typically, the host is configured to have the its virtual appliances time-sync to it. If XClarity Administrator is set to synchronize to a different source than its host, you must disable the host time synchronization between XClarity Administrator virtual appliance and its host.

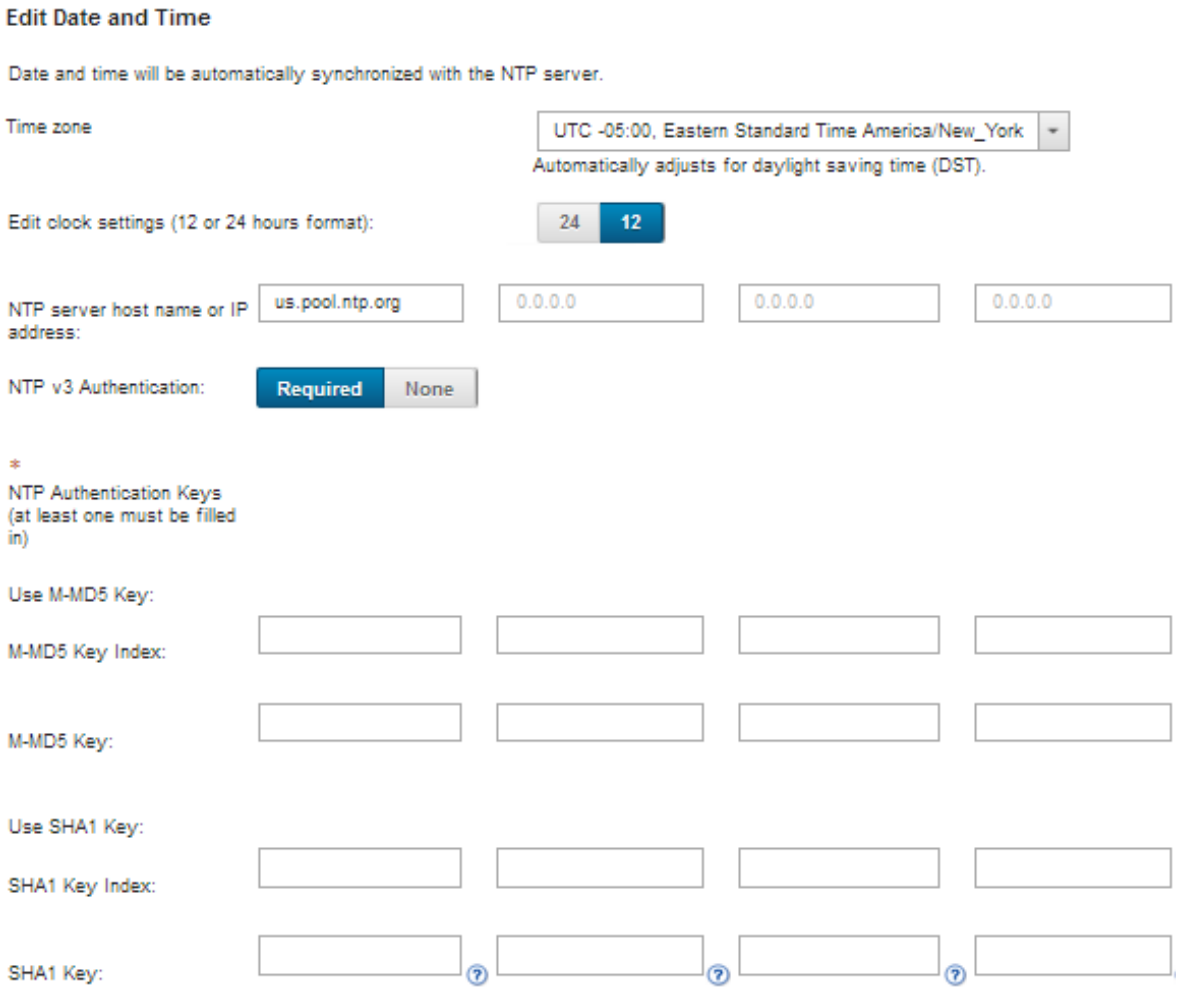
- For ESXi, following instructions on the VMware – Disabling Time Synchronization webpage.
- For Hyper-V, from Hyper-V Manager, right-click the XClarity Administrator virtual machine, and then click **Settings**. In the dialog, click **Management > Integration Services** in the navigation pane, and then clear **Time synchronization**.

Procedure

Complete the following steps to set the date and time for XClarity Administrator.

Step 1. From the XClarity Administrator menu bar, click **Administration → Date and Time**. The Date and Time page is displayed. This page shows the current date and time for XClarity Administrator.

Step 2. Click **Edit Date and Time** to display the Edit Date and Time page.



Step 3. Fill in the date and time dialog.

1. Choose the time zone where the host for XClarity Administrator is located.

   If the selected time zone observes daylight saving time (DST), the time is automatically adjusted for DST.
2. Choose to use a 12-hour or 24-hour clock.
3. Specify the hostname or IP address for each NTP server within your network. You can define up to four NTP servers.
4. Select **Required** to enable NTP v3 authentication, or select **None** to use NTP v1 authentication between XClarity Administrator and the NTP servers within your network.

   You can use v3 authentication if the managed Flex System CMMs and baseboard management controllers have firmware that require v3 authentication, and if NTP v3 authentication is required between XClarity Administrator and one or more NTP servers within your network
5. If you enabled NTP v3 authentication, set the authentication key and index for each applicable NTP server. You can specify an M-MD5 key, SHA1 key, or both. If both M-MD5 or SHA1 keys are specified, XClarity Administrator pushes either M-MD5 or SHA1 key to the managed Flex System CMMs and management controllers that support it. The XClarity Administrator uses the key to authenticate to the NTP server
   - For the M-MD5 key, specify an ASCII string that includes only upper and lower case letters (a-z, A-Z), digits (0–9) and the following special characters @# .

- For the SHA1 key, specify a 40-character ASCII string, including only 0–9 and a-f.
- The specified key index and authentication key must match the key ID and password values that is set on the NTP server. For example, if the key index of the entered SHA1 key in the NTP server is 5, the specified key index of the XClarity Administrator SHA1 key is also 5. For information about setting the key ID and password, see your NTP server documentation.
- You must specify the key for each NTP server that uses v3 authentication, even if two or more NTP servers use the same key.
- If you enable v3 authentication but do not provide an authentication key and index for an NTP server, v1 authentication is used by default.
- If you specified multiple NTP servers, the NTP servers must be either all v3-authenticated or all v1-authenticated. A mix of v3-authenticated or and v1-authenticated NTP servers was not supported.
- If you specified multiple NTP servers with v3-authentication, the key indices must be unique if the keys are not the same. For example, NTP server 1 and 2 cannot have the SHA1 key index of 1 if the SHA1 keys are different in the NTP server 1 and 2. You must reconfigure one of the NTP servers to accept the key with a different key index than the other NTP server; otherwise, that last defined key that was associated with a key index will be configured for all NTP servers with the same key index.

Step 4. Click **Save**.

Setting inventory preferences

You can set inventory preferences for managed devices, including the property to use to display the device name.

Procedure

Complete the following steps to set the inventory preferences for managed devices.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Inventory Preferences**. The Inventory Preferences page is displayed.

Step 2. Select the property to use for the device name that is displayed in the Lenovo XClarity Administrator user interface. You can select one of the following properties.
- **Predefined sequence (default)**
- **User-defined name**
- **DNS hostname**
- **Hostname**
- **IPv4 address**
- **Serial number**

If **Predefined sequence** is selected, the device name that is displayed is chosen based on the sequence of properties in the previous list. For example, if a device has a user-defined name, that name is displayed. If a device does not have a user-defined name, then the DNS host name is displayed. If a device does not have a user-defined name or DNS host name, the hostname is displayed.

Note: Selecting a value other than the default changes that the name that is displayed in the Lenovo XClarity Administrator user interface for all devices to the selected property. The user-defined name that is assigned to the device does not change.

Step 3. Optionally click **Enable** to choose to sort grids (tables) using the value that is selected for the device name.

Step 4. Select the rack numbering order preference, either top to bottom (for example, 1 – 52) or bottom to top (for example, 52 – 1).

Note: Changing the number order preference does not change the location of a device in the rack.

Step 5. Click **Apply**.

After you finish

You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level (see Setting threshold preferences for generating alerts and events).

Setting threshold preferences for generating alerts and events

You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level.

Procedure

Complete the following steps to forward specific service files to the service provider.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts** to display the Alerts page.

Step 2. Click the **Threshold Settings** icon ( ) to display the Threshold Settings dialog.

Step 3. Modify the warning or critical thresholds for the remaining life of SSDs in ThinkSystem and ThinkServer servers.

Remaining life of SSDs is calculated using vendor SMART counters. The default values are 30% for the warning threshold and 20% for the critical threshold.

Step 4. Select the **Enabled** toggle to generate an alert and event when each threshold is reached.

Step 5. Click **Apply**.

Setting up automatic problem notification to Lenovo Support (Call Home)

You can create a service forwarder that automatically sends service data for any managed device to Lenovo Support using the Call Home when certain serviceable events, such as an unrecoverable memory, are received from specific managed devices so that the issue can be addressed. This service forwarded is named “Default Call Home.”

Lenovo is committed to security. When enabled, Call Home automatically contacts Lenovo to open a service ticket and sends in service data collected from a managed device when that device reports a hardware failure or when you choose to initiate a manual Call Home. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later; your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel.

Before you begin

Attention: You must accept the Lenovo Privacy Statement before you can transfer data to Lenovo Support.

Ensure that all ports that are required by Lenovo XClarity Administrator (including ports that are required for Call Home) are available before you enable Call Home. For more information about ports, see Port availability in the XClarity Administrator online documentation.

Ensure that a connection exists to the Internet addresses that are required by Call Home. For information about firewalls, see Firewalls and proxy servers in the XClarity Administrator online documentation.

If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is configured to use basic authentication and is set up as a non-terminating proxy. For more information about setting up the proxy, see Configuring network accessConfiguring network access in the XClarity Administrator online documentation.

About this task

A *service forwarder* defines information about where to send the service data files when a serviceable event occurs. You can define up to 50 service forwarders.

Note: For XClarity Administrator v2.3 and later, service requests are no longer routed directly to IBM. When Call Home is enabled, service requests are first routed to the Lenovo Support, and then forwarded to IBM, if appropriate for certain devices.New DNS names and IP addresses are required to use Call Home to route service requests to Lenovo Support in for XClarity Administrator v2.3.0 and later. The old DNS names and IP addresses are no longer required to use Call Home; however, they are needed to retrieve status for open service tickets that were submitted prior to updating to v2.3.0.

If a Call Home service forwarder is not configured, you can manually open a service ticket and send service files to the Lenovo Support Center by following the instructions on the New Service Request webpage. For information about collecting and downloading service files, see Downloading XClarity Administrator diagnostic files and Collecting and downloading diagnostic files for a device in the XClarity Administrator online documentation.

If a Call Home service forwarder is configured but not enabled, you can *manually* open a service ticket using the Call Home function to collect and transfer service files to the Lenovo Support Center at any time. For more information, see Opening a service ticket in the XClarity Administrator online documentation.

When a Call Home service forwarder is configured and enabled, XClarity Administrator *automatically* opens a service ticket and transfers service files to the Lenovo Support Center when a serviceable event occurs so that the issue can be addressed.

Note: When a Call Home service forwarder is enabled in Lenovo XClarity Administrator, Call Home is disabled on each managed device to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices or if you intend to disable Call Home in XClarity Administrator, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time. For information about re-enabling Call Home on all managed devices when the service forwarder for Call Home is disabled, see Re-enabling call home on all managed devices in the XClarity Administrator online documentation..Although XClarity Administrator supports Call Home for ThinkAgile and ThinkSystem devices, the baseboard management controller for some ThinkAgile and ThinkSystem devices does not include Call Home support. Therefore, you cannot enable or disable Call Home on those devices themselves. Call Home can be enabled only for those devices at the XClarity Administrator level.

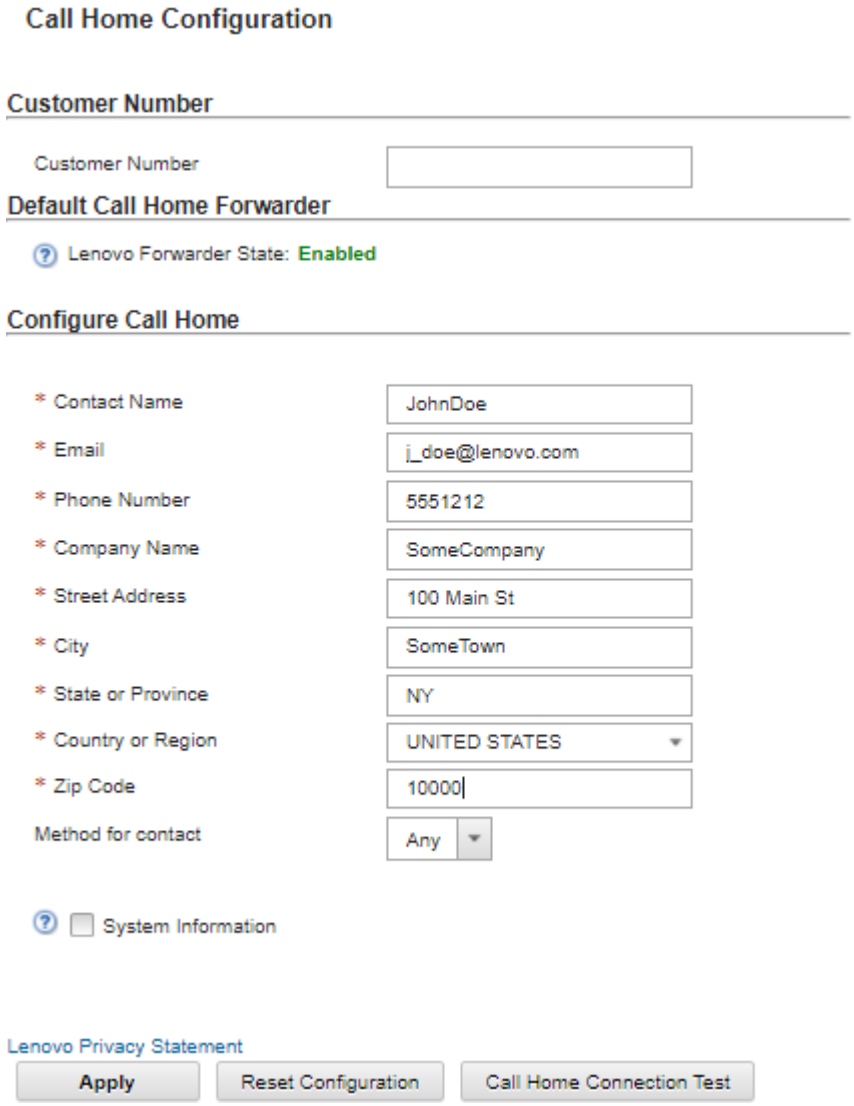
Call home is suppressed for repeated events for any device if a service ticket is open for that event on that device. Call Home is also suppressed for similar events for any ThinkAgile and ThinkSystem device if a service ticket is open for an event on that device. ThinkAgile and ThinkSystem events are 16-characters strings in the following format *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (for example, `806F010D0401FFFF`). Events are similar if they have the same reading type, sensor type, and entity ID. For example, if a service ticket is open for event 806F010D0401FFFF on a specific ThinkAgile or ThinkSystem device, any events that occur on that device with event IDs like *xx*`6F01`*xx*`04`*xxxxxx*, where *x* is any alphanumeric character, are suppressed.

For information about viewing service tickets that were opened automatically by a Call Home service forwarder, see Viewing problem records and status in the XClarity Administrator online documentation.

Procedure

Complete the following steps to setup a service forwarded for Call Home.

- Setup Call Home for all managed devices (current and future):
  1. From the XClarity Administrator menu bar, click **Administration → Service and Support**.
  2. Click **Call Home Configuration** in the left navigation to display the Call Home Configuration page.



  3. (Optional) Specify the default Lenovo customer number to use when reporting problems with XClarity Administrator.

     Tip: You can find your customer number in the proof-of-entitlement email that you received when you purchased Lenovo XClarity Pro.
  4. Fill in the contact and location information.
  5. Select the preferred method of contact by Lenovo Support.
  6. (Optional) Fill in the system information.
  7. Click **Apply**.

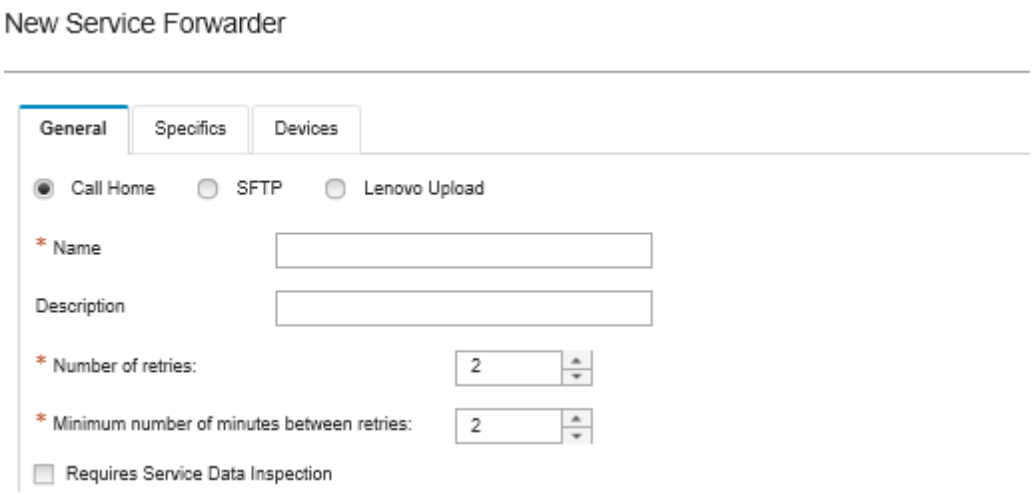
A Call Home service forwarder named “Default Call Home” is created for all managed devices using the specified contact information.

8. Enable and test the “Default Call Home” service forwarder.
   a. Click **Service Forwarder** in the left navigation to display the Service Forwarders page.
   b. Select **Enable** in the **Status** column for the “Default Call Home” service forwarder.
   c. Select the “Default Call Home” service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with the Lenovo Support Center.

      You can monitor the test progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

      Note: The service forwarder must be enabled before it can be tested

- Setup Call Home for specific managed devices:
  1. From the XClarity Administrator menu bar, click **Administration → Service and Support**.
  2. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.
  3. Click the **Create Service Forwarder** icon ( ) to display the New Service Forwarder dialog.
  4. Click the **General** tab.



     a. Select **Call Home** as the service forwarder:
     b. Enter the name of the service forwarder and a description.
     c. Specify the number of automatic-notification retries. The default is 2.
     d. Specify the minimum number of minutes between retries. The default is 2.
     e. (Optional) Click **Requires Service Data Inspection** if you want to inspect the service-data files before they are transferred, and optionally specify the e-mail address of the contact to be notified when service files must be inspected.
  5. Click the **Specific** tab, and fill in the contact and system information.

     Tip: To use the same contact and location information that is configured on the Call Home Configuration page, select **General Configuration** in the **Configuration** drop-down menu.
  6. Click the **Devices** tab, and select the managed devices and resource groups for which you want this service forwarder to forward service files.

     Tip: To forward service files for all managed devices (current and future), select the **Match all devices** checkbox.

7. Click **Create**. The service forwarder is added to the Service and Support page.
8. On the Service Forwarders page, select **Enable** in the **Status** column to enable the service forwarder.
9. Select the service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with the Lenovo Support Center.

   You can monitor the test progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

   Note: The service forwarder must be enabled before it can be tested.

After you finish

From the Service and Support page, you can also perform the following actions:

- If **Requires Service Data Inspection** is selected and a serviceable event was received from one of the managed devices that is associated with the service forwarder, you must inspect service files before the files are forwarded to the service provider. For more information, see Transferring diagnostic files to Lenovo Support in the XClarity Administrator online documentation.
- Determine whether Call Home is enabled or disabled on a managed device by clicking **Endpoint Actions** in the left navigation and verifying the state in the **Call Home Status** column.

  Tip: If "Unknown State" is displayed in the **Call Home Status** column, refresh the web browser to display the correct status.
- Define the support contact and location information for a specific managed device by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking the **Create Contact Profile** icon ( ) or **Edit Contact Profile** icon ( ). The contact and location information for the managed device is included in the service ticket that Call Home sends to the Lenovo Support Center. If unique contact and location information is specified for a managed device, that information is included in the service ticket. Otherwise, general information that is specified for the XClarity Administrator Call Home configuration (on the **Call Home Configuration** page or **Service Forwarders** page) is used. For more information, see Lenovo Support Center. For more information, see Defining the support contacts for a device in the XClarity Administrator online documentation.
- View service tickets that have been submitted to the Lenovo Support Center by clicking **Service Ticket Status** in the left navigation. This page lists service tickets that have been opened automatically or manually by a Call Home service forwarder, the status, and service files that were transmitted to the Lenovo Support Center. For more information, see Viewing problem records and status in the XClarity Administrator online documentation.
- Collect service data for a specific device by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking the **Collect Service Data** icon ( ). For more information, see Collecting and downloading diagnostic files for a device in the XClarity Administrator online documentation.
- Manually open a service ticket in the Lenovo Support Center, collect service data for a specific device, and send those files to the Lenovo Support Center by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking **All Actions → Perform Manual Call Home**.If the Lenovo Support Center requires additional data, the Lenovo Support might instruct you to recollect service data for that device or for another device.

  For more information, see Opening a service ticket in the XClarity Administrator online documentation.
- Re-enable Call Home on all managed devices by clicking **Endpoint Actions** in the left navigation, and then clicking **All Actions → Enable Call Home on all devices**.

  When a Call Home service forwarder is enabled in Lenovo XClarity Administrator, Call Home is disabled on each managed device to avoid duplicate problem records from being created. If you intend to

discontinue using XClarity Administrator to manage your devices or if you intend to disable Call Home in XClarity Administrator, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time.

For more information, see Re-enabling call home on all managed devices in the XClarity Administrator online documentation.

Setting up automatic problem notification to a preferred service provider

You can configure Lenovo XClarity Administrator to automatically send diagnostic files for a specific set of managed devices to your preferred service provider (including Lenovo Support using Call Home) when certain serviceable events are received from managed devices (such as an unrecoverable memory error) so that the issue can be addressed.

Before you begin

Attention: You must accept the Lenovo Privacy Statement before you can transfer data to Lenovo Support.

Ensure that all ports that are required by XClarity Administrator (including ports that are required for call home) are available before you setup a service forwarder. For more information about ports, see Port availability in the XClarity Administrator online documentation.

Ensure that a connection exists to the Internet addresses that are required by the service provider.

If you choose to use Lenovo Support, ensure that a connection exists to the Internet addresses that are required by Call Home. For information about firewalls, see Firewalls and proxy servers in the XClarity Administrator online documentation.

If XClarity Administrator accesses the Internet through an HTTP proxy, ensure that the proxy server is set up as a non-terminating proxy. For more information about setting up the proxy, see Configuring network accessConfiguring network access in the XClarity Administrator online documentation.

About this task

A *service forwarder* defines information about where to send the service data files when a serviceable event occurs. You can define up to 50 service forwarders

For each service forwarder, you can choose to automatically transfer service data to Lenovo Support (called *Call Home*), to the Lenovo Upload Facility, or to another service provider using SFTP. For information about setting up a service forwarder for Call Home, see Setting up automatic problem notification to Lenovo Support (Call Home) and Setting up automatic problem notification to a preferred service provider. For information about setting up a service forwarder for the Lenovo Upload Facility, see Setting up automatic problem notification to the Lenovo Upload Facility in the XClarity Administrator online documentation.

If a service forwarder is configured and enabled for SFTP, XClarity Administrator *automatically* transfers service files to the specified SFTP site for your preferred service provider.

Note: If multiple SFTP service forwarders are set up for the same device, only one of the service forwarders transfers service data. The address and port that is used depends on which service forwarder is triggered first.

Procedure

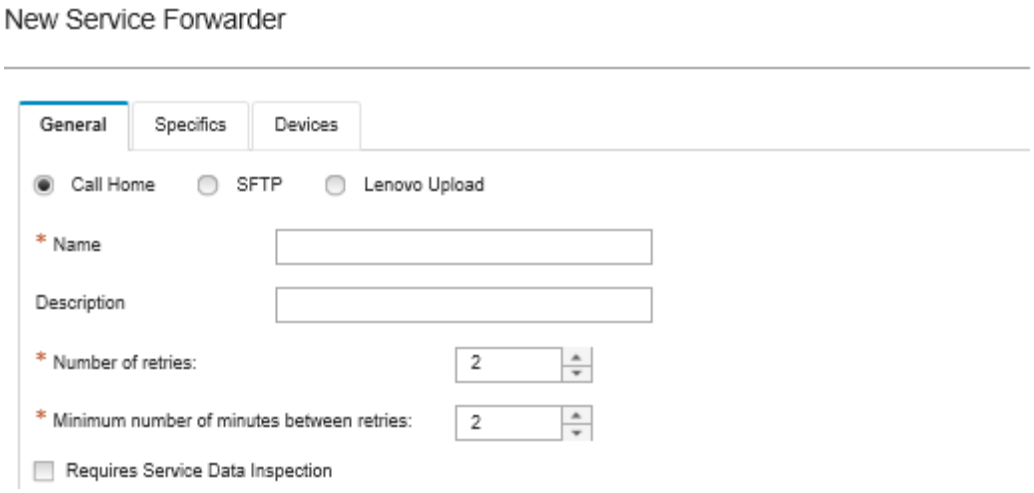
Complete the following steps to define and enable a service forwarder.

Step 1. From the XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.

Step 2. Click **Service Forwarders** in the left navigation to display the Service Forwarders page.

Step 3. Click the **Create Service Forwarder** icon ( ) to display the New Service Forwarder dialog.

Step 4. Click the **General** tab.



1. Select **SFTP** for the service forwarder:
2. Enter the name of the service forwarder and a description.
3. Specify the number of automatic-notification retries. The default is 2.
4. Specify the minimum number of minutes between retries. The default is 2.
5. (Optional) Click **Requires Service Data Inspection** if you want to inspect the service files before they are transferred, and optionally specify the e-mail address of the contact to be notified when service files must be inspected.

Step 5. Click the **Specific** tab, and fill in the following information:
- IP address and port number of the SFTP server
- User ID and password for authentication to the SFTP server

Step 6. Click the **Device** tab, and select the managed devices and resource groups for which you want this service forwarder to forward service data.

Tip: To forward service data for all managed devices (current and future), select the **Match all devices** checkbox.

Step 7. Click **Create**. The service forwarder is added to the Service and Support page

Step 8. On the Service and Support page, select **Enable** in the **Status** column to enable the service forwarder.

Step 9. Optional: To prevent serviceable events that are in the list of excluded events from automatically opening problem reports, select **No** next to the question **Do you want excluded events to open problem reports?**.

Step 10. Select the service forwarder, and click **Test Service Forwarders** to generate a test event for the service forwarder and verify that XClarity Administrator is able to communicate with each service provider.

Note: The service forwarder must be enabled before it can be tested.

After you finish

From the Service and Support page, you can also perform the following actions:

- If **Requires Service Data Inspection** is selected and a serviceable event was received from one of the managed devices that is associated with the service forwarder, you must inspect and service files before the files are forwarded to the service provider. For more information, see Inspecting diagnostic files in the XClarity Administrator online documentation.
- Modify the service-forwarder information by clicking **Service Forwarders** in the left navigation and clicking the **Edit Service Forwarder** icon ( ).
- Enable or disable a service provider by clicking **Service Forwarders** and selecting **Enable** or **Disable** in the **Status** column.
- Delete the service provider by clicking **Service Forwarders** and clicking the **Delete Service Forwarder** icon ( ).
- Define the support contact and location information for a specific managed device by clicking **Endpoint Actions** in the left navigation, selecting the device, and then clicking the **Create Contact Profile** icon ( ) or **Edit Contact Profile** icon ( ). The contact and location information for the managed device is included in the problem record that call home creates in the Lenovo Support Center. If unique contact and location information is specified for a managed device, that information is included in the problem record. Otherwise, general information that is specified for the XClarity Administrator call-home configuration (on the **Call Home Configuration** page or **Service Forwarders** page) is used. For more information, see Defining the support contacts for a device in the XClarity Administrator online documentation.
- Collect service data for a specific device by clicking **Endpoint Actions**, selecting the device, and then clicking the **Collect Service Data** icon ( ). For more information, see Collecting and downloading diagnostic files for a device in the XClarity Administrator online documentation.

For more information about these service and support tasks, see Working with service and support in the XClarity Administrator online documentation.

Connecting XClarity Administrator as a hub to the TruScale portal

You can connect Lenovo XClarity Administrator as a management hub to the Lenovo TruScale portal.

Before you begin

Attention: These configuration steps are intended only for Lenovo Service representatives.

Procedure

To connect XClarity Administrator to the TruScale portal, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Administration → Hub Configuration** to display the Hub Configuration page.

Step 2. Create a registration key by clicking **Generate Registration Request**. The Generate Registration Request dialog is displayed.

Step 3. Click **Copy to Clipboard** to copy the registration key, and then close the dialog.

Step 4. Click **Install Registration Key** to display the Install Registration Key dialog.

Step 5. Paste the registration key in the **Registration Key** field.

Step 6. Click **Submit**.

After you finish

You can uninstall the registration key by clicking **Reset Configuration**.

Backing up, restoring, and migrating system data and settings

You can use Lenovo XClarity Administrator to backup and restore system data and settings and imported files such as operating-system images, firmware updates, and OS device drivers.

Backing up Lenovo XClarity Administrator

If you already have backup procedures in place for virtual hosts, ensure that your procedures include Lenovo XClarity Administrator.

Before you begin

Attention: Ensure that you notify all active users before you initiate the backup procedure. XClarity Administrator is quiesced during the procedure to prevent data from being modified. Therefore, you cannot access XClarity Administrator while the backup procedure is running.

Download the Certificate Authority certificate from the XClarity Administrator virtual appliance and import the certificate into your web browser (see Importing the Certificate Authority certificate into a web browser).

Ensure that all running jobs are complete and that there are no pending jobs. If jobs are running, you can choose to stop the running jobs and continue creating the backup.

Ensure that the DNS servers are set up correctly; otherwise SMTP and NTP might not work correctly after the backup is restored.

Ensure that there is enough disk space available in the management server for the backup. If not, free up disk space by deleting XClarity Administrator resources, including previous backups, that are no longer needed (see Managing disk space) or choose to create a new backup without including operating-system images, firmware updates, and OS device drivers.

About this task

Always back up XClarity Administrator after performing the initial setup and after making significant configuration changes, including:

- Before you update XClarity Administrator
- When you manage new chassis or rack servers
- When you add users to XClarity Administrator
- When you create and deploy new Configuration Patterns

Ensure that you back up XClarity Administrator on a regular basis.

It is recommended that you download backups to your local system. If the host operating system shuts down unexpectedly, you might not be able to authenticate with XClarity Administrator after the host operating system is restarted. To resolve this problem, restore XClarity Administrator from the last backup on your local system (see Restoring Lenovo XClarity Administrator.).

Procedure

Complete the following steps to back up XClarity Administrator.

Step 1. From the XClarity Administrator menu bar, click **Administration → Back Up and Restore Data**. The Back Up and Restore Data page is displayed.

Step 2. Click the **Back Up** icon ( ). The Back Up Data and Settings dialog is displayed.

Step 3. Enter a description for this backup.

Step 4. Choose the location where you want to create the backup. This can be the local repository or a remote share.

The backup is created in the local repository by default. You can copy a backup from the local repository to a remote share by clicking the **Copy Backup** icon ( ).

If you choose a remote share, the backup is first created in the local repository. Then, the backup is copied to the selected remote share, and the local copy is deleted. For more information, see Managing remote shares.

Step 5. Optionally select to include operating-system images, firmware updates, and OS device drivers.

Step 6. Specify the encryption passphrase for the backup.

Attention: Record the encryption passphrase. The passphrase is needed to restore the backup to this or another XClarity Administrator instance. If you forget the passphrase, there is no way to recover it.

Step 7. Click **Back Up** to backup data and settings immediately, or click **Schedule** to schedule this backup to run at a later time.

Attention: If you choose to back up immediately, do not close or refresh the web browser tab or window before the process completes. Otherwise, the backup might not be generated.

Generating the backup might take a while. A progress bar shows the status of the job.

If you chose to create the backup on a remote share, you can monitor progress from the Jobs page (see Monitoring jobs).

If you schedule a backup, the management server is shut down temporarily during the backup process. After the management server comes back online, you can monitor the status of the backup process from the Jobs page.

Step 8. Log in to the XClarity Administrator to continue managing your devices.

After you finish

From the Back Up and Restore Data page, you can perform the following actions:

- Copy XClarity Administrator backups to or from a remote share clicking the **Copy Backup** icon ( ).
- Delete selected backups from the local repository or remote shares that are no longer needed by clicking the **Delete Backup** icon ( ).
- Restore system data and settings to this management server (see Restoring Lenovo XClarity Administrator).
- Import or export backups from the local system by clicking the **Import Backup** icon ( ) or **Export Backup** icon ( ), respectively.
- Push the selected backup to a new XClarity Administrator instance (see Migrating system data and settings to another XClarity Administrator instance).

Restoring Lenovo XClarity Administrator

You can use backed up data and settings to restore Lenovo XClarity Administrator to a previous state.

Before you begin

Attention: Ensure that you notify all active users before you initiate the backup procedure. XClarity Administrator is quiesced during the procedure to prevent data from being modified. Therefore, you cannot access XClarity Administrator while the backup procedure is running

Download the Certificate Authority certificate from the XClarity Administrator virtual appliance and import the certificate into your web browser (see Importing the Certificate Authority certificate into a web browser).

Ensure that all running jobs are complete and that there are no pending jobs.

You can restore a backup only to the same XClarity Administrator version that was used to create the backup.

About this task

Attention:

- All changes since when the backup was created will be lost.
- To restore data, the virtual appliance is reset to its original clean state. All current settings, device inventory and files (operating-system images, firmware updates, and OS device drivers) are deleted before restoring data in the backup. Data and settings in the backup are not mixed with the virtual appliance's current data and settings. If you choose not to restore device inventory, operating-system images, firmware updates, and OS device drivers, only the default XClarity Administrator data is present after the restore operation completes.

Restoring a backup does not delete backups in the XClarity Administrator instance.

Restoring a backup does not change data or settings on the managed devices. For example, if you unmanage a device and then restore a previous backup when the device was still managed on XClarity Administrator, you might have connectivity issues with that device after the restore operation is complete. Likewise, if you manage a device and then restore a previous backup when the device was still unmanaged, you might need to manually modify the device's configuration to undo its managed status or use the **Force** option when trying to manage it in XClarity Administrator again.

Procedure

Complete the following steps to restore XClarity Administrator.

Step 1. From the XClarity Administrator menu bar, click **Administration → Back Up and Restore Data**. The Back Up and Restore Data page is displayed.

Step 2. If you exported the backup package to your local system and deleted it from XClarity Administrator, complete the following steps.

a. From the Backup and Restore Data page, click the **Import Backup** icon ( ) to display the Import Backup dialog.

b. Click **Browse** to find the backup that you exported from a XClarity Administrator instance.

c. Click **Import** to upload the backup to the XClarity Administrator.

Importing the backup might take a while. A progress bar shows the status of the job.

Attention: If you close or refresh the web browser tab or window before the upload completes, the process might fail.

d. When the import is complete, specify the encryption passphrase for the backup.

Note: If you do not have the encryption passphrase, you will need to create a new backup in XClarity Administrator (see Backing up Lenovo XClarity Administrator).

Step 3. Select the backup to restore, and click the **Restore Backup** icon ( ). The Restore Data dialog is displayed.

Step 4. Specify the encryption passphrase for the backup.

Step 5. Click **Confirm**.

Step 6. In the Confirm Data Restore dialog, verify that the information in the dialog is correct.

Step 7. In the Restore Options dialog, optionally choose to import operating-system images, firmware updates, OS device drivers, network settings, and device inventory.

Attention: Ensure that you carefully read all warning that are displayed in this dialog.

Step 8. Click **Confirm** to begin data restore.

Restoring the data and settings might take a while. A progress bar shows the status of the job.

When the restore process is complete, you are redirected to the login page.

Attention: If you close or refresh the web browser tab or window before the process completes, process might fail.

Step 9. Log in to the XClarity Administrator to continue managing your devices.

Migrating system data and settings to another XClarity Administrator instance

You can migrate the backed-up system data and settings to a new Lenovo XClarity Administrator that is in the same or different network.

Before you begin

The target management server must be a *new* XClarity Administrator instance at the same version as the management server that was used to create the backup and must be in the Initial Setup wizard, with no steps completed. For more information, see Installing and setting up XClarity Administrator in the XClarity Administrator online documentation.

Ensure that you notify all active users before you initiate the backup procedure. XClarity Administrator is quiesced during the procedure to prevent data from being modified. Therefore, you cannot access XClarity Administrator while the backup procedure is running.

Download the Certificate Authority certificate from the XClarity Administrator, and import the certificate into your web browser (see Managing disk space in the XClarity Administrator online documentation).

Backups in the source management-server backup repository are not migrated to the target management server. Before migrating data and settings, export any backups you might need to your local system.

About this task

Any changes to the source management server after the backup was created is not migrated to the target management server.

Restoring a backup does not change data or settings on the managed devices. For example, if you unmanage a device and then restore a previous backup when the device was still managed on XClarity Administrator, you might have connectivity issues with that device after the restore operation is complete. Likewise, if you manage a device and then restore a previous backup when the device was still unmanaged,

you might need to manually modify the device's configuration to undo its managed status or use the **Force** option when trying to manage it in XClarity Administrator again.

Notes: When running XClarity Administrator as a container, the volumes that were created on the host for the one container can be used as volumes by another container. After the volumes are bound the to the new (target) container, they can no longer be used by initial (source) container.

1. Configuring the `docker-compose.yml` file for the target container to use the same IP address and container name as the source container.
2. Stop the source container using the following command.
   `docker-compose -p ${CONTAINER_NAME} down`
3. Start the target container using the following command, where <*env_filename*> is the name of the environment variables file. When the target container is started, the volumes are bound to the target XClarity Administrator container, and XClarity Administrator uses system data and settings from those volumes.
   COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <env_filename> up -d`

Procedure

Complete the following steps to restore XClarity Administrator.

Step 1. If the source and target XClarity Administrator are in the same network, complete the following steps.

a. From the XClarity Administrator menu bar, click **Administration → Back Up and Restore Data**. The Back Up and Restore Data page is displayed.

b. Click the **Push Backup** icon ( ) to display the Push Data dialog.

c. Specify the current IP address of the target XClarity Administrator.

d. Click **Continue** to upload the backup to the target XClarity Administrator.

Uploading the backup might take a while. A progress bar shows the status of the job.

Attention: If you close or refresh the web browser tab or window before the upload completes, the package might not be uploaded.

Step 2. If the source and target XClarity Administrator *are not* in the same network, complete the following steps

a. From the source XClarity Administrator menu bar, click **Administration → Back Up and Restore Data**. From the Back Up and Restore Data page, click the **Export Backup** icon ( ) to export the backup to the local system.

Exporting the backup might take a while.

b. Copy the exported backup from the source management server to a system in the same network as the target management server

c. From the Wizard page on the target XClarity Administrator, click the **Import Backup** icon ( ) to display the Import Data Package dialog.

d. Click **Browse** to find the backup that you exported from the source XClarity Administrator.

e. Click **Upload** to import the backup to the target XClarity Administrator.

Importing the backup might take a while. A progress bar shows the status of the job.

Attention: If you close or refresh the web browser tab or window before the upload completes, the process might fail.

Step 3. When the import is complete, specify the encryption passphrase for the backup.

Note: If you do not have the encryption passphrase, you will need to create a new backup in the source XClarity Administrator (see Backing up Lenovo XClarity Administrator.

Step 4. In the Confirm Data Restore dialog, verify that all information is correct.

Step 5. Click **Confirm** to begin loading system data and settings.

Step 6. In the Restore Options dialog, optionally choose to import operating-system images, firmware updates, OS device drivers, network settings, and device inventory.

Attention: Ensure that you carefully read all warning that are displayed in this dialog.

Step 7. If you chose to import network settings or device inventory, shut down the source management server from the source XClarity Administrator by clicking **Administration → Shutdown Management Server → Shutdown**.

Confirm that the source virtual appliance has shut down before continuing

Step 8. On the target XClarity Administrator, click **Confirm** to begin loading data and settings from the package

If you chose to import network settings, after migration is complete the IP addresses from the source XClarity Administrator are reassigned to the target XClarity Administrator.

Attention: If the source XClarity Administrator uses DHCP, you must bind the target XClarity Administrator MAC addresses to the corresponding source XClarity Administrator IP addresses on the DHCP server. Wait at least 15 minutes after the DHCP server is modified before continuing.

Step 9. Wait for the Load Data and Settings from Package progress bar to complete.

When the data-migration process is complete, you are redirected to the login page.

Attention: If you close or refresh the web browser tab or window before the upload completes, the process might fail.

Step 10. Log in to the target XClarity Administrator to continue managing your devices.

Managing disk space

You can manage the amount of disk space that is used by Lenovo XClarity Administrator by moving large data files that are not immediately needed to a remote share or by deleting resources that are no longer needed.

About this task

To determine how much disk space is currently being used, click **Dashboard** from the XClarity Administrator menu bar. The disk space usage on the repository and remote shares is listed in the XClarity Administrator Activity section.

Procedure

Complete one or more of the following steps to free up disk space by moving files to a remote share and deleting unneeded resources.

- **Delete unneeded resources**

  You can quickly delete files from the local repository that are no longer needed by completing the following steps.

1. From the XClarity Administrator menu bar, click **Administration → Disk Cleanup** to display the Disk Cleanup page.
2. Select the files that you want to delete. The section header identifies the amount of space that will be freed when the files are deleted.
   - **Operating system related files**

     You can delete OS Images, boot-option files, and software files.
   - **Firmware updates**

     You can delete payload files for all OS device drivers that are associated with UpdateXpress System Packs (UXSPs) and individual device drivers that are in the Downloaded state.

     You can delete payload files for individual firmware updates that are in the Downloaded state and are not used in a firmware-compliance policy.

     You can delete payload files for management-server updates that are in the Downloaded state.

     Note: When the firmware-updates repository is located on a remote share, you cannot use the disk-cleanup function to delete individual firmware updates and UXSPs.
   - **Service data files**

     When service event occurs on a device, service data is collected automatically for that device. Service data is automatically captured for the management server every time an exception occurs in the XClarity Administrator. It is recommended that you periodically delete these archives if XClarity Administrator and the managed devices are running without issues.

     When management-server updates are successfully applied, the update files are automatically removed from the repository.
3. Click **Delete Selected**.
4. Review the list of files that you selected, and click **Delete**.

- **Move firmware update packages to a remote repository**

  By default, Lenovo XClarity Administrator uses a local (internal) repository for storing firmware updates. You can free up disk space that is available to the XClarity Administrator local repository by using a mounted remote share over SSH File System (SSHFS) as a remote repository. You can then use firmware update files directly from the remote repository to maintain firmware compliance on your devices. For more information, see Using a remote repository for firmware updates.

  When you change the location of the firmware updates repository, you can choose to copy all firmware update from the original repository to the new repository.

  Firmware update files in the original repository *are not* automatically cleaned up after switching locations.

  Tip: The remote updates repository can be shared by multiple XClarity Administrator management servers.

  To move firmware updates to a remote firmware-updates repository, complete the following steps.

  1. Add a remote share to XClarity Administrator (see Managing remote shares).
  2. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.
  3. Click **All Actions → Switch Repository Location** to display the Switch Repository Location dialog.
  4. Select the remote share that you just created from the **Repository Location** drop down list.
  5. Select **Copy update packages from current repository the new repository** to copy firmware update files to the new repository location before switching the repository location.
  6. Click **OK**.

A job is created to copy firmware update packages to the new repository. You can monitor the job progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

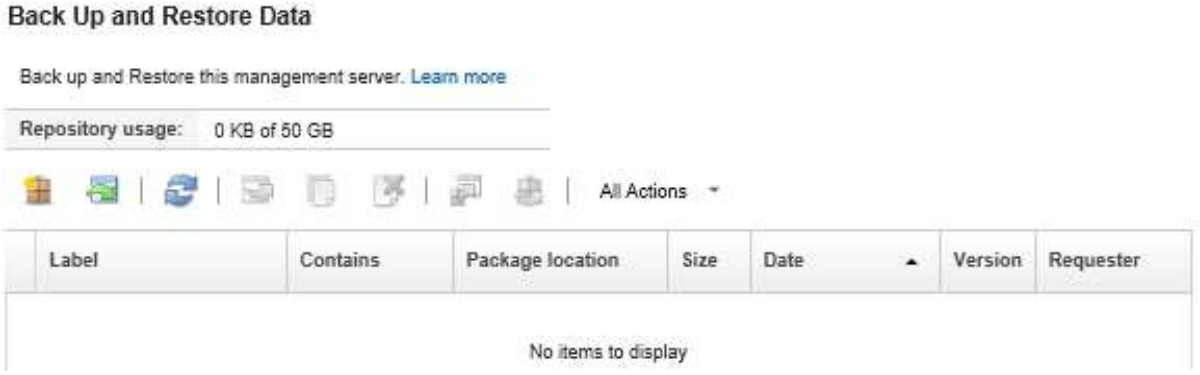
7. Clean up firmware update files in the local repository.
   a. Switch the location to the local repository by clicking **All Actions → Switch Repository Location**, select the **Local Repository** for the repository location, and then click **OK**.
   b. Click the **Individual Updates** tab, click the select-all checkbox in the table to select all firmware updates, and then click the **Delete full update packages** icon ( )
   c. Click the **UpdateXpress System Pack (UXSP)** tab, click the select-all checkbox in the table to select all UXSPs, and then click the **Delete UXSP and associated policy** icon ( )
   d. Switch the location back to the remote repository by clicking **All Actions → Switch Repository Location**, selecting the new remote repository for the repository location, and then clicking **OK**.

- **Move XClarity Administrator backups to a remote share**

  You can free up disk space that is available to the XClarity Administrator local repository by moving XClarity Administrator backups to a remote share. However, you cannot use the files directly on the remote share. To use the files, you must move them back to the XClarity Administrator local repository. For more information about remote shares, see Managing remote shares.

  Important: It is recommended that you download backups to your local system or copy backups to a remote share before deleting the backups in XClarity Administrator.

  1. From the XClarity Administrator menu bar, click **Administration → Back Up and Restore Data** to display the Back Up and Restore Data page.



  The **Package location** column identifies whether the backup is stored, either locally in the XClarity Administrator local repository or on a remote share.

  2. Select the backup, and click the **Copy Backup** icon ( ) to displays the Copy Backup dialog.
  3. Choose the remote share to store the backup.
  4. Click **Copy**.
  5. Monitor the copy progress on the Jobs page. When the copy is complete, select the backup again, and click the **Delete Backup** icon ( ) to display the Delete Backup dialog.
  6. Select “Local” for the location.
  7. Click **Delete**.

Managing remote shares

You can mount remote shares and then move large data files, such as Lenovo XClarity Administrator backups and firmware updates, from the local repository to the remote share to manage disk space that is available to management server.

Before you begin

When running XClarity Administrator as a container, remote shares are mounted to the container using the yml file during installation (see).

When running XClarity Administrator as a virtual appliance:

- You must have **lxc-supervisor** authority to mount or unmount a remote share.
- When using SSH key authentication to mount a remote share, you must import the SSH private key for the remote server to XClarity Administrator.

Ensure that you have a high speed and stable network between the file server and XClarity Administrator.

About this task

You must use separate remote shares to store XClarity Administrator backups and firmware updates.

You cannot use the XClarity Administrator backup files directly from the remote share. To use the backup files, you must move them back to the local repository.

Currently, only SSHFS is supported.

Procedure

To add a remote share when running XClarity Administrator as a virtual appliance, complete the following steps.

1. From the XClarity Administrator menu bar, click **Administration → Remote Share**. The Remote Share page is displayed.
2. Click the **Create** ( ) icon to create a remote share. The Create Remote Share dialog is displayed.
3. Specify the IP address of the file server that hosts the remote share.
4. Specify the stored credential to use to access the remote share.

   Tip: To create a stored credential, see Managing stored credentials.
5. Specify the mount point (local directory) on the management server to use for mounting the remote share.

   Important: The path must start with “/mnt”.
6. Specify the shared directory (remote server path) to mount as the remote share on the management server.
7. Click **Create**.

After you finish

- Unmount the remote share by selecting the remote share and clicking the **Delete** ( ) icon.
- Move XClarity Administrator backup files to and from a remote share (see Managing disk space).
- Configure XClarity Administrator to use a remote share as the firmware-updates repository (see Using a remote repository for firmware updates

Changing the language of the user interface

You can change the language of the user interface after you are logged in.

Procedure

From the Lenovo XClarity Administrator title bar, click the user-actions menu (

), and then click **Change language**. Select the language that you want to display, and then click **Close**.

Note: The help system displays in the same language that is set for the user interface.

Shutting down XClarity Administrator

When Lenovo XClarity Administrator shuts down, connectivity to Lenovo XClarity Administrator is lost.

Before you begin

You must have **lxc-supervisor** or **lxc-admin** authority to shut down an XClarity Administrator virtual appliance.

Ensure that no jobs are currently running. Any jobs that are currently running are canceled during the shutdown process. To view the jobs log, see Monitoring jobs.

Procedure

Complete the following steps to shut down Lenovo XClarity Administrator.

- **Containers**

  Run the following commands to stop the container.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  ```
- **Virtual appliances**
  1. From the Lenovo XClarity Administrator menu bar, click **Administration → Shut Down Management Server**.

     A confirmation dialog is displayed with a list of jobs that are currently running. When you shut down XClarity Administrator, the jobs are canceled.
  2. Click **Shut down**.

After you finish

To restart XClarity Administrator after a shutdown, see Restarting XClarity Administrator.

Restarting XClarity Administrator

You can restart Lenovo XClarity Administrator from the web interface or from the hypervisor after a shutdown.

Before you begin

You must have **lxc-supervisor** or **lxc-admin** authority to restart XClarity Administrator.

Ensure that no jobs are currently running. Any jobs that are currently running are canceled during the restart process. To view the jobs log, see Monitoring jobs.

About this task

There are certain situations when you are required to restart Lenovo XClarity Administrator:

- When regenerating a server certificate
- When uploading a new server certificate

Procedure

Complete one of the following procedures to restart Lenovo XClarity Administrator.

- **Containers**

  Run the following commands to stop and then start the container, where <*env_filename*> is the name of the environment variables file.

  ```
  docker-compose -p ${CONTAINER_NAME} down
  COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <env_filename> up -d
  ```

- **Virtual appliances**
  - Restart Lenovo XClarity Administrator from the web interface:
    1. From the Lenovo XClarity Administrator menu bar, click **Administration → Shut Down Management Server**.

       A confirmation dialog is displayed with a list of jobs that are currently running. When you restart Lenovo XClarity Administrator, the jobs are canceled.
    2. Click **Restart**.

       When Lenovo XClarity Administrator shuts down, connectivity to Lenovo XClarity Administrator is lost.
    3. Wait a few minutes for Lenovo XClarity Administrator to restart, and then log in again.
  - Restart Lenovo XClarity Administrator from the hypervisor after a shutdown:
    - Microsoft Hyper-V
      1. From the Server Manager Dashboard, click **Hyper-V**.
      2. Right-click the server, and click **Hyper-V Manager**.
      3. Right-click the virtual machine, and click **Start**. When the virtual machine is started, the IPv4 and IPv6 addresses are listed for each interface, as shown in the following example.

         The XClarity Administrator eth0 management port uses a DHCP IP address by default. At the end of the XClarity Administrator boot process, you can choose to set a static IP address for the eth0 management port by entering 1 when prompted, as shown in the example below. The prompt is available for 150 seconds, until the login prompt is displayed. To proceed to the login prompt without delay, enter x at the prompt.

         Important:

         - When changing the static IP address settings, you have a maximum of 60 seconds to enter the new settings. Ensure that you have the required IP information before continuing.
           - For IPv4 settings, you must have the IP address, subnet mask, and gateway IP address
           - For IPv6 settings, you must have the IP address and prefix length
         - If you are not using a DHCP server, you can use a configuration file to specify the IP settings for the XClarity Administrator eth0 management port. that you want to use to access the XClarity Administrator. For more information, see the “What to do next” section below.
         - If you change the IP address settings from the console, XClarity Administrator is restarted to apply the new settings.
         - No action is required to log in. Ignore the console login message. The console interface is not for customer use.

- You might see the message `TCP: eth0: Driver has suspect GRO implementation, TCP performance may be compromised` on the console. The performance of the virtual machine is not impacted, and you can ignore this warning.

Attention: Changing the IP address of the XClarity Administrator management port after managing devices might cause the devices to be placed in offline state in XClarity Administrator. If you choose to change the IP address after XClarity Administrator is up and running, ensure that all devices are unmanaged before changing the IP address.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

4. Log in to Lenovo XClarity Administrator (see Logging in to XClarity Administrator).

– VMware ESXi

1. Connect to the host through VMware vSphere Client.
2. Right-click the virtual machine, and click **Power → Power on**.
3. Click the **Console** tab. When the virtual machine is started, the IPv4 and IPv6 addresses are listed for each interface, as shown in the following example.

   The XClarity Administrator eth0 management port uses a DHCP IP address by default. At the end of the XClarity Administrator boot process, you can choose to set a static IP address for the eth0 management port by entering 1 when prompted, as shown in the example below. The prompt is available for 150 seconds, until the login prompt is displayed. To proceed to the login prompt without delay, enter x at the prompt.

   Important:

   - When changing the static IP address settings, you have a maximum of 60 seconds to enter the new settings. Ensure that you have the required IP information before continuing.
     – For IPv4 settings, you must have the IP address, subnet mask, and gateway IP address
     – For IPv6 settings, you must have the IP address and prefix length
   - If you are not using a DHCP server, you can use a configuration file to specify the IP settings for the XClarity Administrator eth0 management port. that you want to use to access the XClarity Administrator. For more information, see the “What to do next” section below.
   - If you change the IP address settings from the console, XClarity Administrator is restarted to apply the new settings.
   - No action is required to log in. Ignore the console login message. The console interface is not for customer use.

- You might see the message `TCP: eth0: Driver has suspect GRO implementation, TCP performance may be compromised` on the console. The performance of the virtual machine is not impacted, and you can ignore this warning.

Attention: Changing the IP address of the XClarity Administrator management port after managing devices might cause the devices to be placed in offline state in XClarity Administrator. If you choose to change the IP address after XClarity Administrator is up and running, ensure that all devices are unmanaged before changing the IP address.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

4. Log in to Lenovo XClarity Administrator (see Logging in to XClarity Administrator).

After you finish

When Lenovo XClarity Administrator restarts, it recollects inventory for each managed device. Wait approximately 30-45 minutes, depending upon the number of managed devices, before attempting firmware updates, configuration pattern deployments, or operating-system deployments.

Chapter 3. Monitoring devices and activities

You can monitor your devices and activities though the dashboard, alerts and audit logs, and jobs logs.

Viewing a summary of your environment

The Dashboard displays the status of all managed devices, an overview of all provisioning-related tasks, an information about Lenovo XClarity Administrator resources and activities.

Learn more: XClarity Administrator: Monitoring

Procedure

Step 1. From the XClarity Administrator menu bar, click **Dashboard**.

© Copyright Lenovo 2015, 2022

Step 2. Expand the hardware status, provisioning status, or the administrator activity section to obtain more information about each of these areas.

Viewing a summary of your hardware status

The Hardware Status area displays the status of all managed devices.

Procedure

To obtain more information about all of the devices of that type, click the number listed under the device type.

To view more information about only those devices of that type and status, click the icon or number beside each status icon.

- **Servers**. Displays the total number of servers (compute nodes, rack servers, and tower servers) that XClarity Administrator manages, and the number of servers with normal, warning, and critical status. For more information, see Viewing the status of a managed server.
- **Storage**. Displays the total number of storage devices that XClarity Administrator manages, and the number of storage devices with normal, warning, and critical status. For more information, see Viewing the status of storage devices.
- **Switches**. Displays the total number of RackSwitch and Flex System switches that XClarity Administrator manages, and the number of switches with normal, warning, and critical status. For more information, see Viewing the status of switches
- **Chassis**. Displays the total number of Flex chassis that XClarity Administrator manages, and the number of Flex chassis with normal, warning, and critical status. For more information, see Viewing the status of a managed chassis.
- **Racks**. Displays the number of racks that are created in XClarity Administrator, and the number of racks with devices that have the normal, warning, and critical as their highest status. For more information, see Viewing the status of devices in a rack.
- **Resource groups**. Displays the number of resource groups that XClarity Administrator manages and the number of resource groups with devices that have the normal, warning, and critical as their highest status. For more information, see Viewing the status of devices in a resource group.

To customize the hardware resources that are displayed on the dashboard, click the **Customize** icon ( ). You can choose the device types that you want to show or hide. You can also choose whether to aggregate servers into a single summary, display separate summaries for each type of server (rack and tower, Flex System, ThinkServer, and NeXtScale servers), or omit specific types of servers.

Viewing a summary of your provisioning status

The Provisioning Status area provides a summary of all tasks that are associated with provisioning devices.

Procedure

- **Configuration Patterns**. Displays details about the number of servers that have profiles, including the following statistics.

Note: When the management server is not license compliant, all values are 0 (see Installing the full-function enablement license in the XClarity Administrator online documentation).

- The number of servers that are compliant with their server profile. You can click the number to display the Configuration Patterns: Server Profiles page with a list of compliant servers.
- The number of servers that are not compliant with their server profile. You can click the number to display the Configuration Patterns: Server Profiles page with a list of non-compliant servers.
- The number of devices for which compliance status is unknown. You can click the number to display the Configuration Patterns: Server Profiles page with a list of servers with unknown compliance.

  Note: Compliance status is unknown, typically after a partial profile deployment, when Lenovo XClarity Administrator did not collect the configuration information from the sever. Refresh the server inventory or revisit the server-profile details page to force collecting configuration information from server.
- The number of servers that are assigned a server profile. You can click the number to display the Configuration Patterns: Server Profiles page with a list of servers with profiles.
- The number of servers that are not assigned a server profile. You can click the number to display the Configuration Patterns: Server Patterns page with a list of server patterns that can be deployed to servers without profiles.
- The number of server patterns that are currently being deployed.

To view trending data for configuration patterns, click **View Trending Data** (see Monitoring trends in provisioning status).

For more information about configuration patterns and server profiles, see Configuring servers using configuration patterns.

- **Operating System Images**. Displays details about operating-system deployments, including the following statistics.

  Note: When the management server is not license compliant, all values are 0 (see Installing the full-function enablement license in the XClarity Administrator online documentation).

  - The number of OS images in the repository. You can click the number to display the Deploy Operating Systems: Manage OS Images page with a list of operating systems.
  - The number of current OS deployments that are in progress. You can click the number to display the Deploy Operating Systems: Deploy OS Images page with a list devices for which an operating system is being installed.
- **Firmware Updates**. Displays details about firmware updates, including the following statistics.
  - The number of devices that are compliant. You can click the number to display the Firmware Updates: Apply / Activate page with a list of compliance devices.
  - The number of devices that are not compliant. You can click the number to display the Firmware Updates: Apply / Activate page with a list of non-compliance devices.
  - The number of devices that do not have an assigned firmware-compliance policy. You can click the number to display the Firmware Updates: Apply / Activate page with a list of devices without a compliance policy.

    From this page, you can assign each device a firmware-compliance policy by selecting a policy from the **Assigned Compliance Policy** column.
  - The number of devices for which updates are not supported. You can click the number to display the Firmware Updates: Apply / Activate page with a list of devices for which updates are not supported.
  - The number of updates that are in progress.
  - The number of devices with pending firmware. You can click the number to display the Firmware Updates: Apply / Activate page with a list of devices for which updates are pending activation.

To view trending data for firmware updates, click **View Trending Data** (see Monitoring trends in provisioning status).

For more information about firmware updates and compliance policies, see Updating firmware on managed devices.

Viewing a summary of Lenovo XClarity Administrator activity

The XClarity Administrator Activity area displays information about active jobs, active sessions, and system resources in XClarity Administrator.

Procedure

- **Jobs**. Displays the number of active jobs that are currently in progress. For more information about jobs, see Monitoring jobs.
- **Active Sessions**. Displays the user ID and IP address for each active XClarity Administrator session. For more information about users, see Managing user accounts.
- **Resource Usage**. Displays the processor usage, memory usage, and disk capacity on the host system and remote files shares. For more information about system resources, see Monitoring system resources.

Monitoring system resources

You can determine the processor usage, memory usage, and disk capacity on the host system from the Dashboard page.

Before you begin

The following *minimum requirements* must be met for XClarity Administrator. Depending on the size of your environment and your use of Configuration Patterns, additional resources might be required for optimal performance.

- Two virtual microprocessors
- 8 GB of memory
- 192 GB of storage for use by the XClarity Administrator virtual appliance.
- Display with a minimum resolution of 1024 pixels in width (XGA)

The following table lists the minimum recommended configurations for a given number of devices. Keep in mind that if you run the minimum configuration, you might experience longer than expected completion times for management tasks. For provisioning tasks such as operating system deployment, firmware updates, and server configuration, you might need to increase the resources temporarily.

Number of Managed Devices	Virtual CPU/Memory Configuration
0 - 100 devices	2 vCPUs, 8 GB RAM
100 - 200 devices	4 vCPUs, 10 GB RAM
200 - 400 devices	6 vCPUs, 12 GB RAM
400 - 600 devices	8 vCPUs, 16 GB RAM
600 - 800 devices	10 vCPUs, 20 GB RAM
800 – 1,000 devices	12 vCPUs, 24 GB RAM

Notes:

- A single XClarity Administrator instance can support a maximum of 1,000 devices.

- For the latest recommendations and additional performance considerations, see the XClarity Administrator: Performance Guide (White paper).
- Depending on the size of your managed environment and the pattern of use in your installation, you might need to add resources to maintain acceptable performance. If you frequently see processor usage in the system resources dashboard displaying high or very high values, consider adding 1-2 virtual processor cores. If your memory usage persists above 80% at idle, consider adding 1-2 GB of RAM. If your system is responsive at a configuration as defined in the table, consider running the VM for a longer period to assess system performance.
- For information about how to free up disk space by deleting XClarity Administrator resources that are no longer needed, see Managing disk space.

Procedure

From the Lenovo XClarity Administrator menu bar, click **Dashboard**.

The host-system resource usage is listed in the XClarity Administrator Activity section.

Processor

The usage measurement indicates the number of XClarity Administrator processes that are simultaneously accessing the processors on the host.

Tip: The usage measure might occasionally spike to High or Very High. If the usage remains at these level for more than 30 minutes, check the jobs log to see if long running jobs are in progress (see Monitoring jobs).

The total-capacity measurement indicates the number of processors that are available on the host.

Memory

The usage measurement indicates the amount of memory that is currently in use by XClarity Administrator.

The total-capacity measurement indicates the total amount of available memory on the host.

User Data

The usage measurement indicates the amount of disk space that is currently in use by XClarity Administrator on the host system.

The total-capacity measurement indicates the total amount of space (used and unused) that is allocated for user data, such as operating systems and firmware updates.

For more information about managing disk space, see Managing disk space.

Attention: If the allocated resources are insufficient to handle the current number of managed devices with good performance, consider increasing the resource allocation. For information about recommended hardware requirements based on the number of managed devices in your environment, see Supported host systems in the XClarity Administrator online documentation.

Monitoring trends in provisioning status

Lenovo XClarity Administrator regularly collects provisioning status, including compliance and active jobs for firmware updates and configuration patterns, for all managed devices so that you can monitor trends over a period of time.

About this task

You must have **lxc_admin** or **lxc-supervisor** authority to view trend data.

The following data is collected:

- **Firmware updates**
  - **Devices compliant**. Number of devices that are compliant with their assigned firmware-compliance policy
  - **Devices non-compliant**. Number of devices that are not compliant with their assigned firmware-compliance policy
  - **Devices without policies**. Number of devices that do not have an assigned firmware-compliance policy
  - **Devices not supported for updates**. Number of devices for which firmware updates are not supported
  - **Updates in progress**. Number of devices for which firmware updates are in progress
- **Configuration patterns**
  - **Servers with profiles**. Number of devices that have an assigned server profile
  - **Servers without profiles**. Number of devices that do not have an assigned server profile
  - **Servers compliant**. Number of devices that are compliant with their assigned server profile
  - **Servers non-compliant**. Number of devices that are not compliant with their assigned server profile
  - **Server patterns in progress**. Number of devices for which configuration-pattern updates are in progress

Procedure

Complete the following steps to view trends in provisioning status.

Step 1. From the XClarity Administrator menu bar, click **Dashboard** to display the Dashboard page.

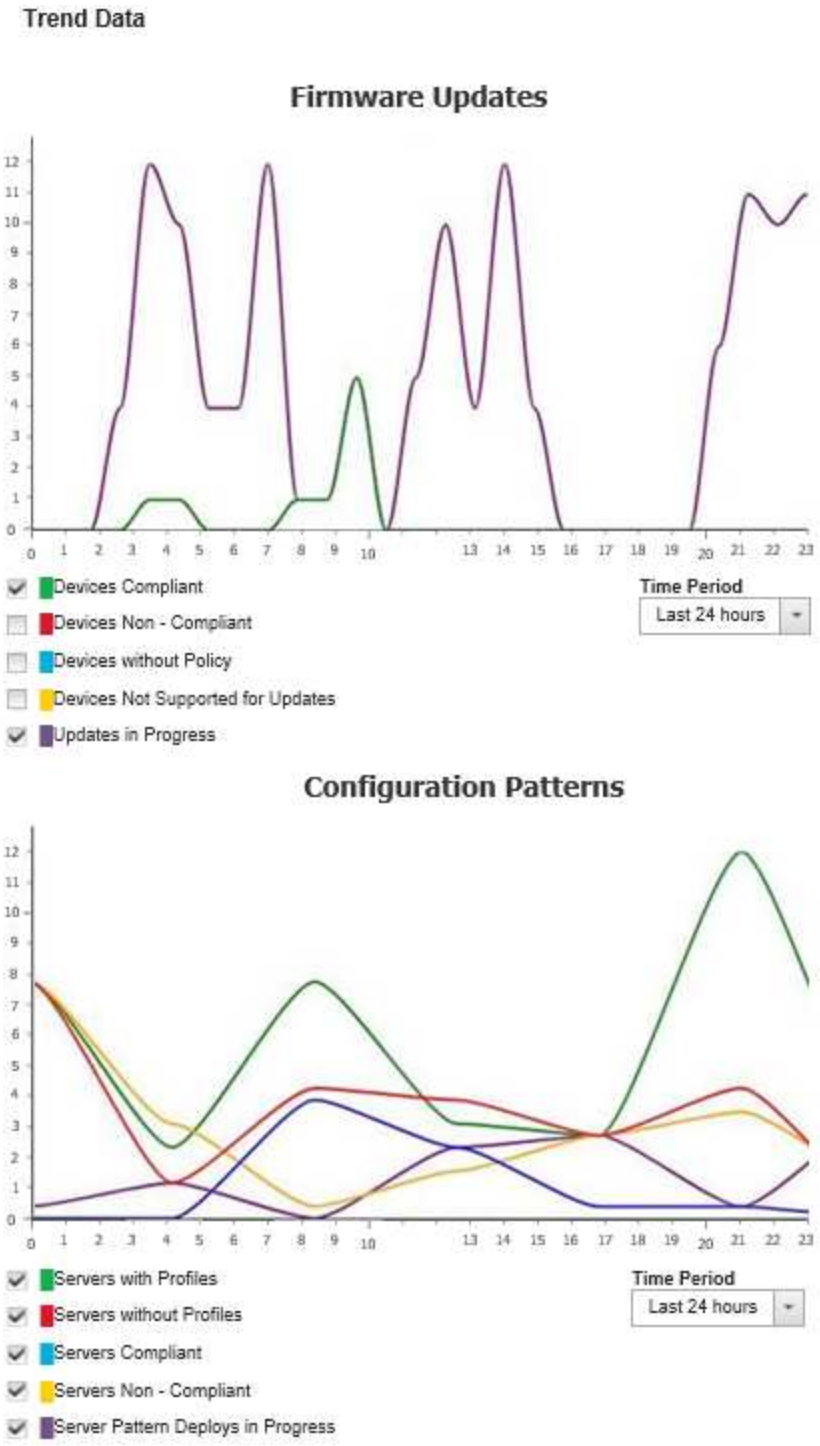
Step 2. Click the **Trending Data** link to display the Threshold Settings dialog.

Step 3. Clear or select the data that you want to view.

Step 4. Select the time period that you want to view.

- **24 hours**. Displays data for the last 24 hours. Each data point is an average over a 1-hour period.
- **1 month**. Displays data for the last 30 days. Each data point is an average over a 24-hour period.

The trend data is shown as a graph over the selected time period.



Monitoring historical metrics

Lenovo XClarity Administrator regularly collects metrics data for managed ThinkSystem and ThinkAgile devices, so that you can analyze the current state of your environment.

Before you begin

Historical metrics are supported for only ThinkSystem servers (except SR635, SR645, SR655 and SR665).

Only SSDs in ThinkAgile and ThinkSystem servers (except SR635 and SR655) running XCC firmware released after April 2019 are supported.

Onboard SATA drivers are not supported.

NVMe drives must support the NVMe Management Interface (NVMe-MI) specification.

About this task

The following metrics are collected.

- **SSD Monitoring** This report card includes the following statistics and graphs.
  - The total number of SSDs in the managed devices (based on the scope).
  - The number of SSDs that were analyzed
  - The number of SSDs that are not eligible for analysis
  - A circular graph that shows the number of devices with SSDs that have remaining life in a specific range.
    - Life remaining <= 10%. Number of SSDs with 10% or less life remaining
    - Life remaining 11 – 50%. Number of SSDs with 11 – 50% life remaining
    - Life remaining 51 – 100%. Number of SSDs more than 50% life remaining
- **System Utilization** This report card includes the following statistics and graphs.
  - The current processor usage, as a percentage
  - The current memory usage, as a percentage
  - A line graph that shows the processor and memory usage over time
- **Power Consumption** This report card includes the following statistics and graphs.
  - The current total power input for all power supplies, in watts
  - A line graph that shows the total power input over time
- **Device Temperature** This report card includes the following statistics and graphs.
  - The current maximum temperature of the inlet air, in Celsius
  - A line graph that shows the maximum temperature over time

You can hover over each colored line in the circular graph, each point in the line graph, or number next to each metric to get more information about the metric. You can show or hide metrics in the graph by clicking the color icon in the legend. You can also click any linked number or option in the **Settings** icon (in the upper right corner of the card to view a list of all devices that have metrics that fit the selected criteria.

Procedure

Complete the following steps to view the flow diagram for a specific activity.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Historical Metrics** to display the Historical Metrics page with report cards for each metric type.

Step 2. Set the scope to all or a specific group of devices.

Placing devices in maintenance mode

When a device is in maintenance mode, Lenovo XClarity Administrator excludes all events and alerts for that device from all pages on which events and alerts are displayed. Excluded alerts are still logged but are hidden from view.

About this task

Only events and alerts that were generated for a device while the device is in maintenance mode are excluded. Events and alerts were generated before the device was placed in maintenance mode are displayed.

Placing a managed device in maintenance and then back in service might cause inventory for that device to be out of date. If you see abnormalities, manually refresh the inventory from the device page by selecting the device and clicking **All Actions → Inventory → Refresh Inventory**.

Procedure

Complete one of the following steps to place devices in maintenance mode.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Administration → Service and Support**. The Service and Support page is displayed.

Step 2. Click **Endpoint Actions** in the left navigation to display the Endpoint Actions page.

Step 3. Select one or more devices to place in maintenance mode.

Step 4. Click **Actions → Maintenance** to display the Maintenance mode dialog.

Step 5. Select the date and time for taking the device out of maintenance mode and placing back in service.

Select **Indefinitely** if you do not want the device placed back in service.

Step 6. Click **Confirm**. The maintenance column in the table changes to Yes for that device.

After you finish

When you are done with maintenance on the device, you can put the device back in service by selecting the device and clicking **Actions → Maintenance**, and then clicking **Turn off maintenance** in the dialog. If you do not manually place the device back in service mode, it is placed in service mode automatically after the specified end date and time expires.

Working with alerts

Alerts are hardware or management conditions that require investigation and user action. Lenovo XClarity Administrator polls the managed devices asynchronously and displays alerts that are received from those devices.

Learn more: XClarity Administrator: Monitoring

About this task

Typically, when an alert is received, a corresponding event is stored in the event log. It is possible to have an alert without a corresponding event in the event log (even if the log wraps). For example, events that occur before you manage a chassis are not displayed in the event log. However, the alerts for the chassis are displayed in the alert log because Lenovo XClarity Administrator polls the CMM after the chassis has been managed.

Viewing active alerts

You can view a list of all active hardware and management alerts.

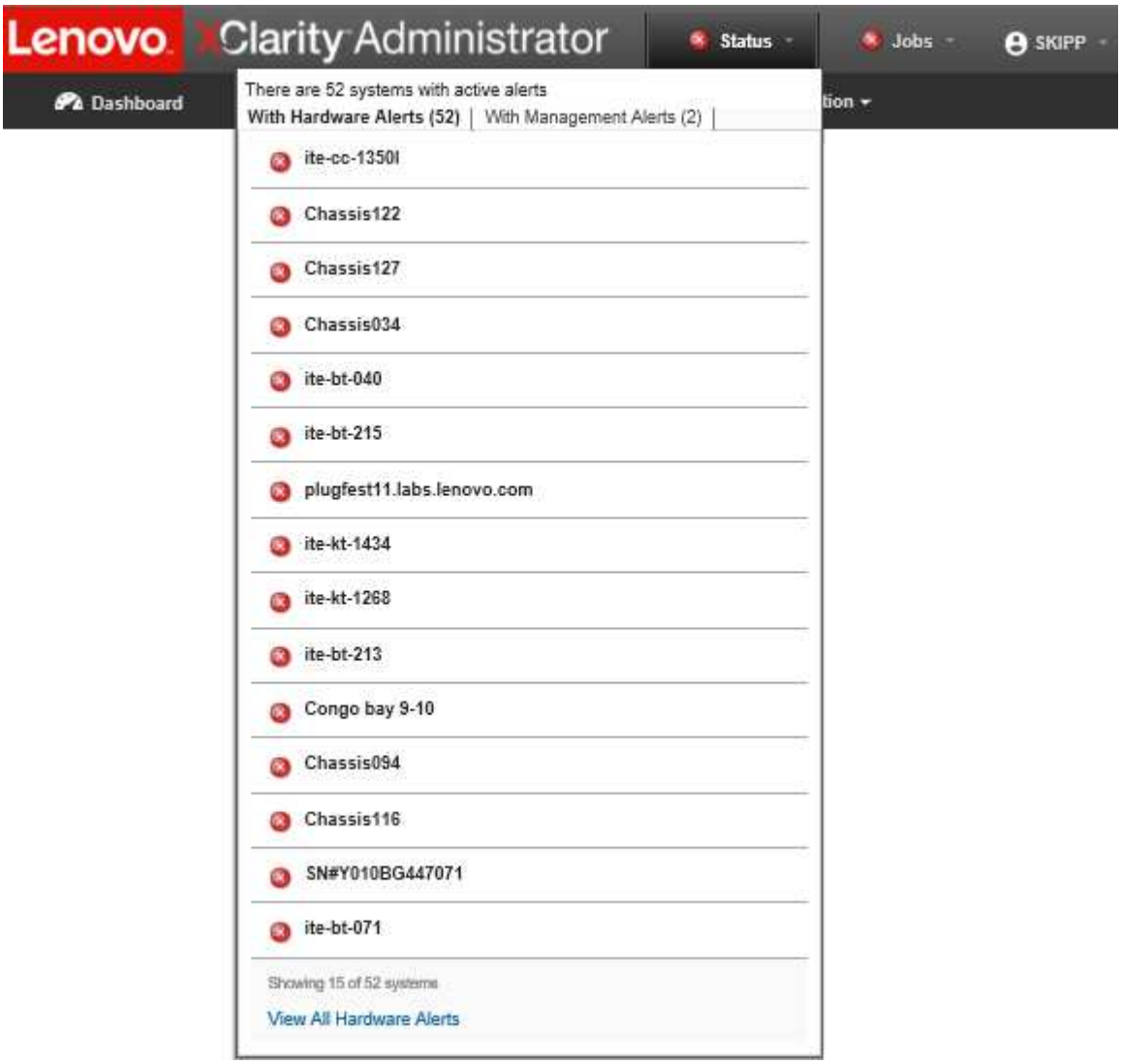
About this task

Note: Alerts for Lenovo Storage devices are presented only in English, even when the locale for Lenovo XClarity Administrator is set to another language. Use an external translation system to translate the messages manually, if needed.

Procedure

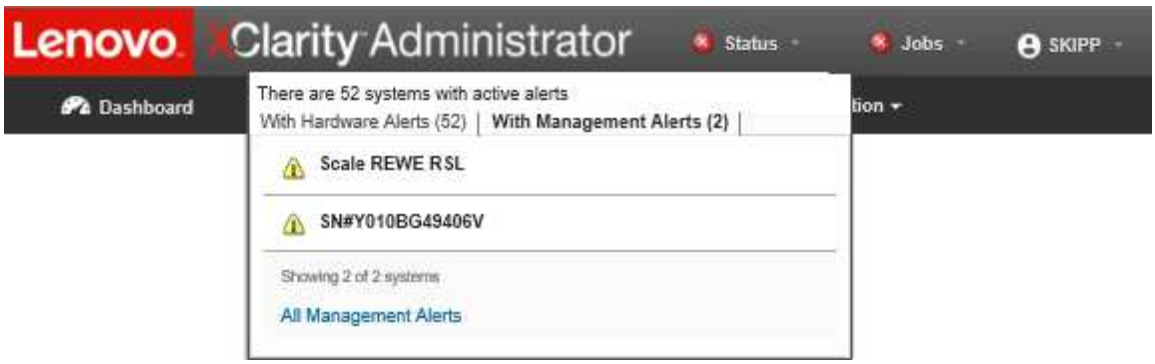
Complete one of these procedures to view the active alerts.

- To view only alerts for managed devices (known as *hardware alerts*):
  1. From the XClarity Administrator title bar, click the **Status** pull-down to display a summary of hardware and management alerts.
  2. Click the **With Hardware Alerts** tab to see a summary of alerts for each managed device.



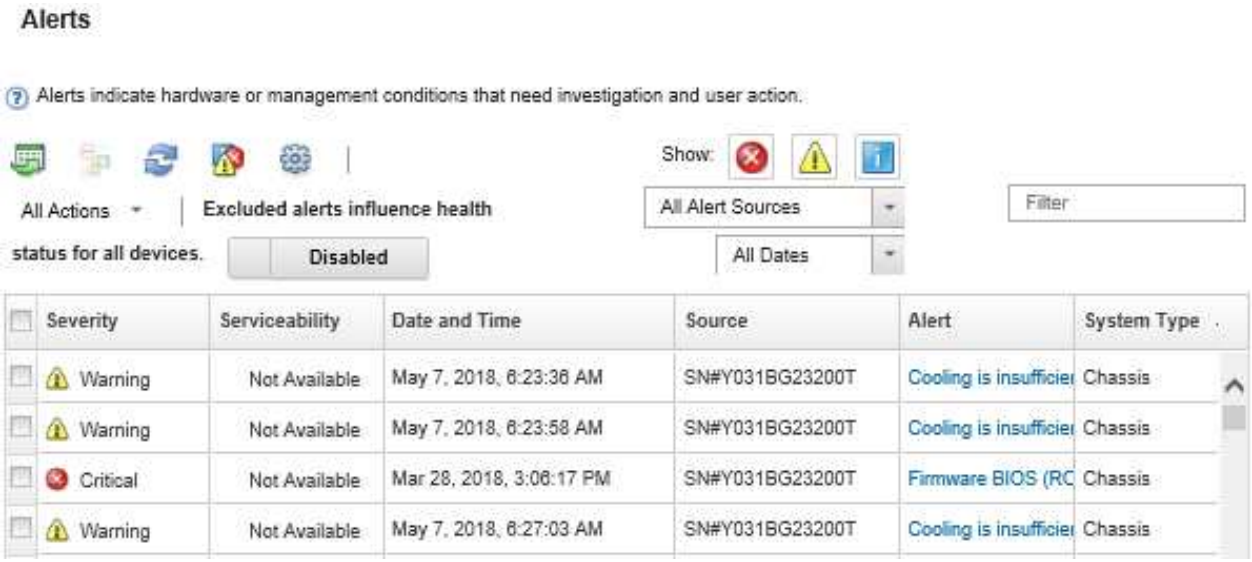
  3. Hover the cursor over a device that is listed under that tab to display a list of alerts for that device.
  4. Click the **All Hardware Alerts** link to display the Alerts page with a filtered list of all hardware alerts.
- To view only alerts from XClarity Administrator (known as *management alerts*):
  1. From the XClarity Administrator title bar, click the **Status** pull-down to display a summary of hardware and management alerts.

2. Click the **With Management Alerts** tab to see a summary of all CMM and XClarity Administrator alerts.



3. Hover the cursor over a device that is listed under that tab to display a list of alerts for that device.
4. Click the **All Management Alerts** link to display the Alerts page with a filtered list of all CMM and XClarity Administrator alerts.

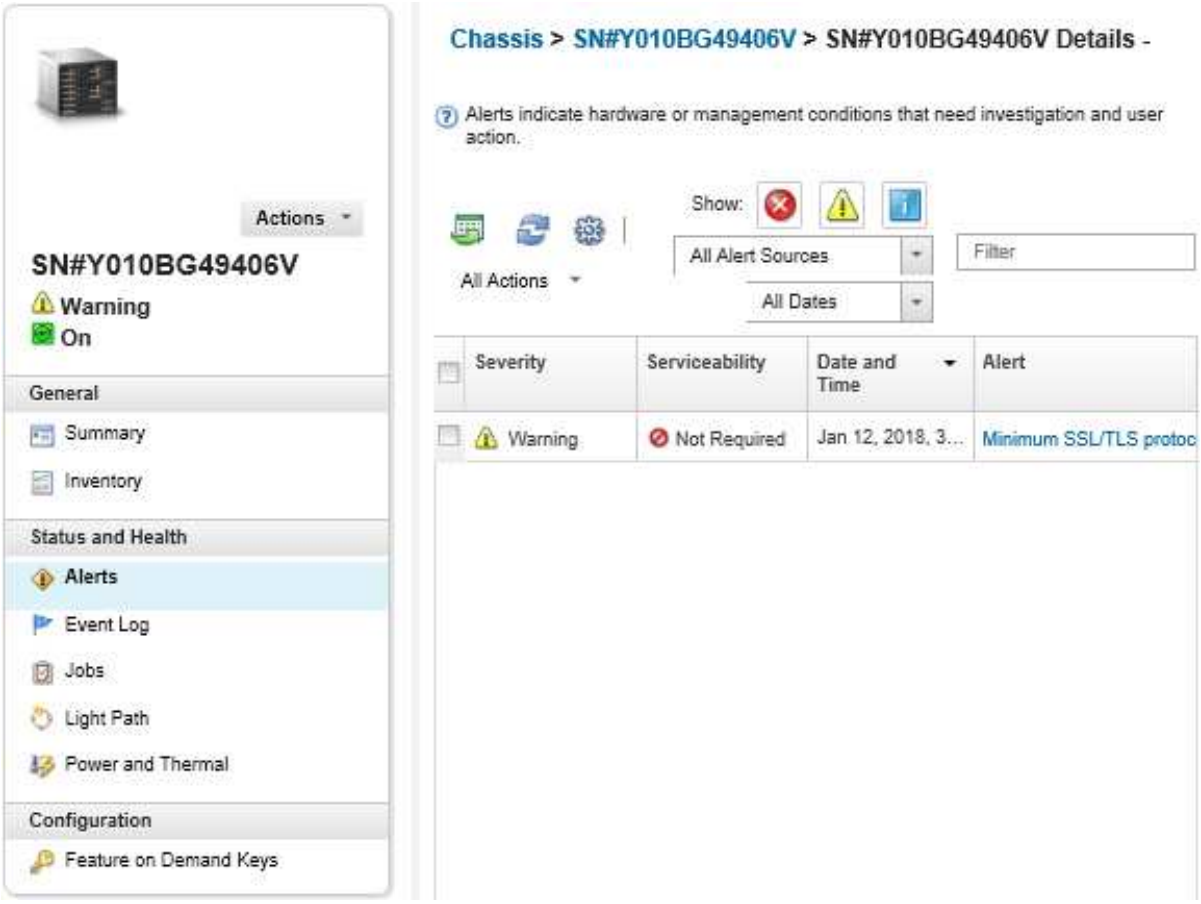
- To view all alerts in XClarity Administrator, click **Monitoring → Alerts** from the XClarity Administrator menu bar. The Alerts page is displayed with a list of all active alerts.



- To view alerts for a specific device:
  1. From the XClarity Administrator menu bar, click **Hardware**, and then click a device type. A page is displayed with a tabular view of all managed devices of that type. For example, click **Hardware → Servers** to display the Servers page.
  2. Click a specific device to display the Summary page for the device.
  3. Under Status and Health, click **Alerts** to display a list of all alerts associated with that device.

     Notes: The Serviceability column might show “Not Available” if:

     – The alert on the device occurred before XClarity Administrator started managing it
     – The event log has wrapped, and the event associated with that alert is no longer in the event log.



Results

From the Alerts page, you can perform the following actions:

- Refresh the list of alerts by clicking the **Refresh** icon ( ).

  Tip: If new alerts are detected, the alerts log refreshes automatically every 30 seconds.
- View information about a specific alert (including an explanation and user action) and about the device that is the source of the alert (such as the Universally Unique Identifier) by clicking the link in the **Alert** column. A dialog with information about the alert properties and details is displayed.

  Note: If the explanation and recovery actions for an alert are not displayed under the **Details** tab, go to Lenovo Flex System online documentation, and search for the alert ID (for example, `FQXHMSE0004G`). The website always provides the most up-to-date information.
- By default, excluded alerts do not influence the health status of managed devices. You can allow excluded alerts to influence the health status of managed devices from the Alerts page by clicking the toggle to enable **Excluded alerts influence health status for all devices**.
- You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level (see Setting threshold preferences for generating alerts and events).
- Export the alerts log by clicking the **Export as CSV** icon ( ).

  Note: The timestamps in the exported log use the local time that is specified by the web browser.
- Exclude specific alerts from all pages on which alerts are displayed (see Excluding alerts).

- Narrow the list of alerts that are displayed on the current page:
  - Show or hide alerts of a specific severity by clicking the following icons:
    - **Critical alerts** icon ( )
    - **Warning alerts** icon ( )
    - **Informational alerts** icon ( )
  - Show only alerts from specific sources. You can choose one of the following options from the drop-down list:
    - All Alert Sources
    - Hardware Events
    - Management Events
    - Service Center Events
    - Customer Serviceable Events
    - Non-serviceable Events
  - Show only alerts with a specific date and time. You can choose one of the following options from the drop-down list:
    - All Dates
    - Previous two hours
    - Previous 24 hours
    - Past Week
    - Past Month
  - List only alerts that contain specific text by entering the text in the **Filter** field.
  - Sort the alerts by column by clicking a column heading.

Excluding alerts

If there are specific alerts that are of no interest to you, you can exclude the alerts from all pages on which alerts are displayed. Excluded alerts are still in the log but are hidden from all pages on which alerts are displayed, including log views and device status.

About this task

Excluded alerts are hidden for all users, not just the user that set the configuration.

You can place devices in maintenance mode, so that all events and alerts for those devices device are excluded (see Placing devices in maintenance mode).

Restriction: Only users with administrative authority can exclude or restore alerts.

Important: If you exclude status alerts, device status on the device summary and detailed pages does not change.

ProcedureComplete the following steps to exclude alerts from the alerts log.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts**. The Alerts page is displayed.

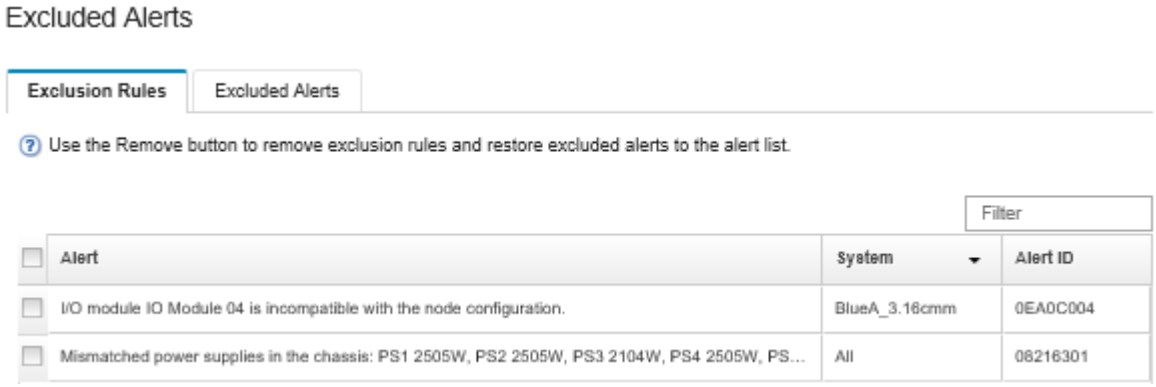
Step 2. Select the alerts to be excluded, and click the **Exclude alerts** icon ( ). The Exclude Alerts dialog is displayed.

Step 3. Select one of the following options:
- **Exclude selected alerts from all systems**. Excludes the selected alerts from all managed devices.
- **Exclude alerts only from systems in the scope of the instance selected**. Excludes the selected alerts from managed devices to which the selected alerts apply.

Step 4. Click **Save**.

After you finish

When you exclude alerts, Lenovo XClarity Administrator creates exclusion rules based on information that you provide. You can view a list of exclusion rules and excluded alerts from the Alerts page by clicking the **Show Excluded/Acknowledged Alerts** icon ( ). In the Excluded/Acknowledged Alerts dialog, click the **Exclusion Rules** tab to view the list of exclusion rules or click the **Excluded Alerts** tab to view the list of excluded alerts.



By default, excluded alerts do not influence the health status of managed devices. You can allow excluded alerts to influence the health status of managed devices from the Alerts page by clicking the toggle to enable **Show Excluded/Acknowledged Alerts**.

You can restore alerts that have been excluded in the alerts log by removing the appropriate exclusion rule.

To remove an exclusion rule, click the **Show Excluded Alerts** icon ( ) to display the Excluded Alerts dialog, select the exclusion rules or excluded alert to restore, and click **Remove**.

Resolving an alert

Lenovo XClarity Administrator provides information about the appropriate actions to perform to resolve an alert.

ProcedureComplete the following steps to resolve an alert.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts** to display the Alerts page.

Step 2. Locate the alert in the alerts log.

Step 3. Click the link in the **Alert** column to view information about the alert (including an explanation and recovery actions) and properties for the device that is the source of the alert (such as the Universally Unique Identifier).

Step 4. Complete the recovery actions that are listed under the **Details** tab to resolve the alert. The following example illustrates recovery actions for an event.

Change the security policy setting on the referenced managed chassis to match the current security policy on the management server.

To change the security policy on the chassis, open a command-line interface session on the Chassis Management Module (CMM) and run one of the following commands:

- To change the security policy level to `Secure`:

```
security -p secure -T mm[p]
```

- To change the security policy level to `Legacy`:
  ```
  security -p legacy -T mm[p]
  ```

Note: If the explanation and recovery actions for an alert are not displayed under the **Details** tab, go to Lenovo Flex System online documentation, and search for the alert ID (for example, `FQXHMSE0004G`). The website always provides the most up-to-date information.

If you follow the recommended actions and the problem persists, contact Lenovo Support.

Acknowledging alerts

When an active alert is acknowledged, the alert is listed on pages on which alerts are displayed but does not affect the severity status for the applicable device.

Procedure

Complete the following steps to acknowledge an alert.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Alerts**. The Alerts page is displayed.

Step 2. Select the alerts to be acknowledged.

Step 3. Click the **Acknowledge alerts** icon ( ).

After you finish

- You can view a list of acknowledged alerts from the Alerts page by clicking the **Show Excluded/ Acknowledged Alerts** icon ( ) to display the Excluded/Acknowledged Alerts dialog, and then clicking the **Acknowledged alerts** tab.
- You can remove the acknowledge for an active alert by clicking the **Show Excluded/Acknowledged Alerts** icon ( ) to display the Excluded/Acknowledged Alerts dialog, clicking the **Acknowledged alerts** tab, select the alerts, and then click the **Remove acknowledgement** icon ( ).

Working with events

From Lenovo XClarity Administrator, you have access to an event log and an audit log.

Learn more: XClarity Administrator: Monitoring

About this task

The *event log* provides a historical list of all hardware and management events.

The *audit log* provides a historical record of user actions, such as logging in to Lenovo XClarity Administrator, creating a new user, and changing a user password. You can use the audit log to track and document authentication and controls in IT systems.

Monitoring events in the event log

The *event log* provides a historical list of all hardware and management events.

About this task

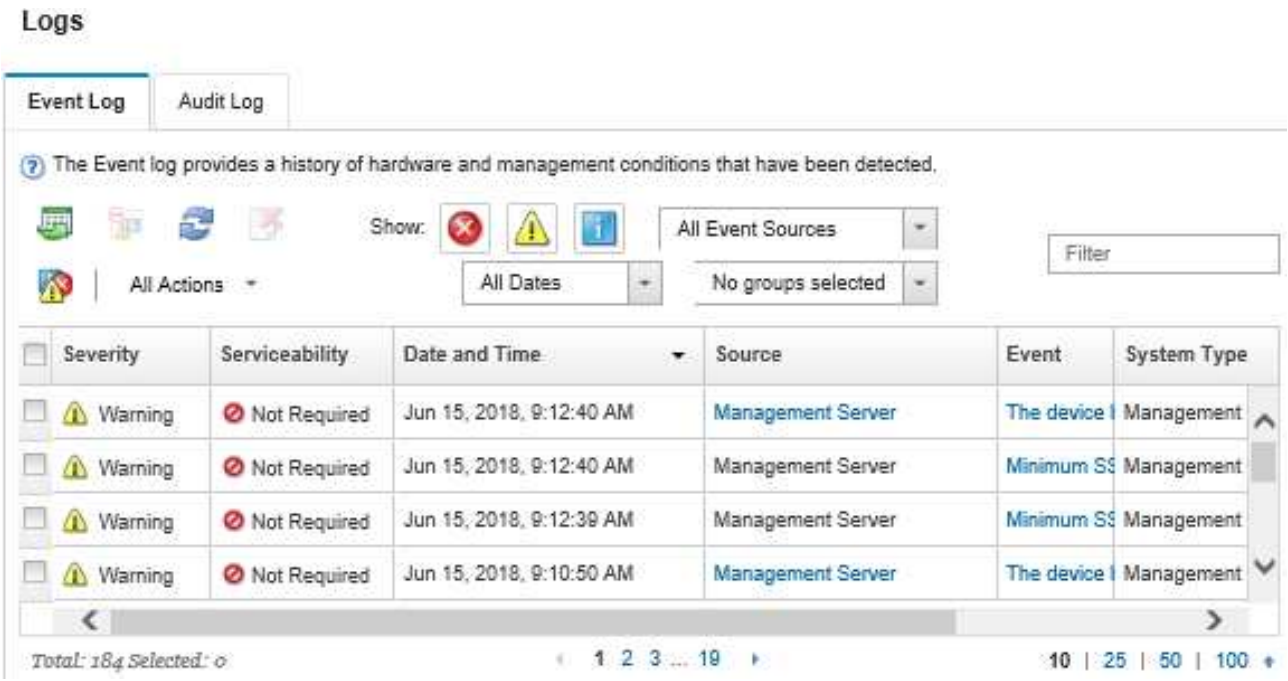
The event log contains informational and non-informational events. The number of each of these events varies until the maximum of 50,000 events is reached in the event log. At that point, there is a maximum of 25,000 informational and 25,000 non-information events. For example, there are 0 events in the event log initially. Assume events are received so that 20,000 informational events and 30,000 non-informational events are received. When the next event is received, the oldest informational event is discarded even if a non-informational event is older. Eventually, the log balances out so that there are 25,000 of each type of event.

Lenovo XClarity Administrator sends an event when the event log reaches 80% of the minimum size and another event when the sum of the event and audit logs reaches 100% of the maximum size.

Tip: You can export the event log to ensure that you have a complete record of all hardware and management events. To export the event log, click the **Export as CSV** icon ( ).

Procedure

To view the event log, click **Monitoring → Event Logs** from the Lenovo XClarity Administrator menu bar, and click the **Event Log** tab. The Event Log page is displayed.



The **Serviceability** column identifies whether the device requires service. This column can contain one of the following values:

- **Not required**. The event is informational and does not require service.
- **User**. Take appropriate recovery action to resolve the issue.

  To view information about a specific event, click the link in the **Event** column. A dialog is displayed with information about the properties for the device that sent the event, details about the event, and recovery actions.
- **Support**. If Call Home is enabled on Lenovo XClarity Administrator, the event is typically submitted to Lenovo Support Center unless an open service ticket for the same event ID already exists for the device.

  If Call Home is not enabled, it is recommended that you manually open a service ticket to resolve the issue (see Opening a service ticket in the Lenovo XClarity Administrator online documentation).

Results

From the Event Log page, you can perform the following actions:

- View the source of the event by clicking the link in the **Source** column.
- Refresh the list of events by clicking the **Refresh** icon ( ).

  Tip: The event log refreshes automatically every 30 seconds if new events are detected.
- Clear all events in the event log by selecting **All Actions → Clear event log**.
- View details about a specific event by clicking the link in the **Event** column and clicking the **Details** tab.
- Export the event log by clicking the **Export as CSV** icon ( ).

  Note: The timestamps in the exported log use the local time that is specified by the web browser.
- Exclude specific events from all pages on which events are displayed (see Excluding events).
- Narrow the list of hardware and management events that are displayed on the current page:
  - Show or hide events of a specific severity by clicking the following icons from the drop-down list:
    - **Critical events** icon ( )
    - **Warning events** icon ( )
    - **Informational events** icon ( )
  - Show only events from specific sources. You can choose one of the following options from the drop-down list:
    - All Alert Sources
    - Hardware Events
    - Management Events
    - Serviceable Events
    - Customer Serviceable Events
    - Non-serviceable Events
  - Show only events with a specific date and time. You can choose one of the following options:
    - All Dates
    - Previous 2 hours
    - Previous 24 hours
    - Past Week
    - Past Month
    - Custom

    If you select **Custom**, you can filter hardware and management events that were raised between a custom start date and the current date.
  - List only events that contain specific text by entering the text in the **Filter** field.
  - Sort the events by column by clicking on a column heading.

Monitoring events in the audit log

The *audit log* provides a historical record of user actions, such as logging in to Lenovo XClarity Administrator, creating a new user, and changing a user password. You can use the audit log to track and document authentication and controls in IT systems.

About this task

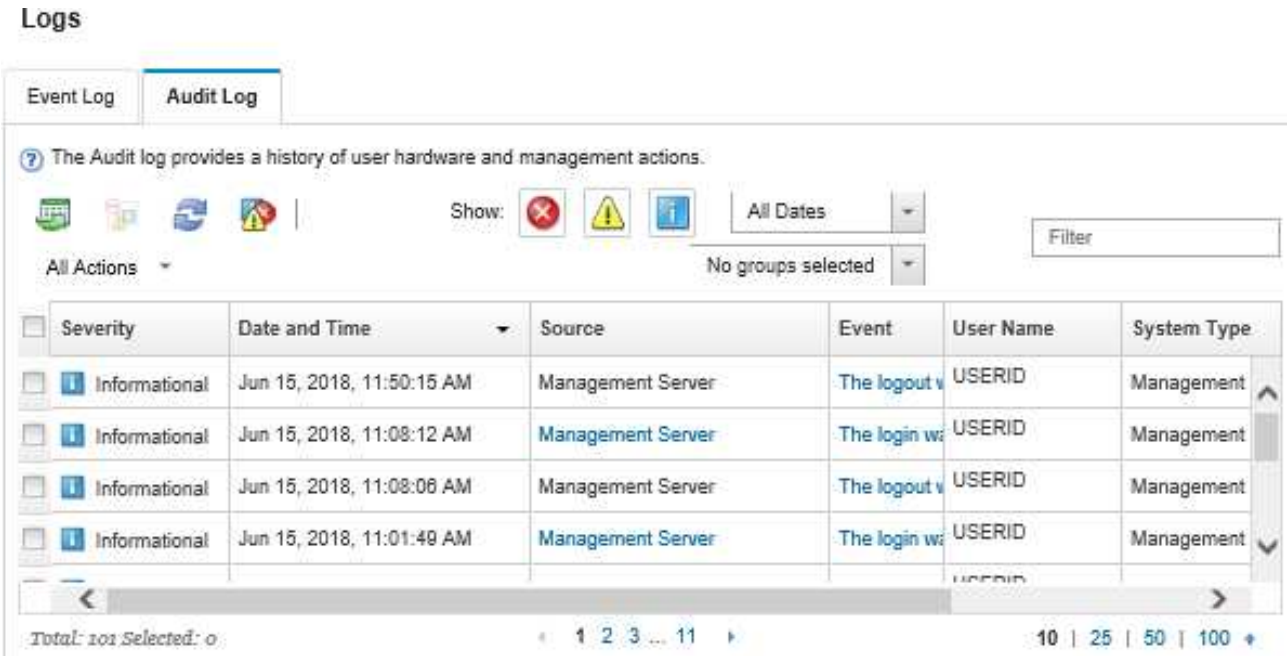
The audit log can contain a maximum of 50,000 events. When the maximum size is reached, the oldest event in the log is discarded and the new event is added to the log.

XClarity Administrator sends an event when the audit log reaches 80% of the maximum size and another event when the sum of the event and audit logs reaches 100% of the maximum size.

Tip: You can export the audit log to ensure that you have a complete record of all audit events. To export the audit log, click the **Export as CSV** icon ( ).

Procedure

To view the audit log, click **Monitoring → Event Logs** from the XClarity Administrator menu bar, and click the **Audit Log** tab. The Audit Log page is displayed.



To view information about a specific audit event, click the link in the **Event** column. A dialog is displayed with information about the properties for the device that sent the event, details about the event, and recovery actions.

Results

From this page, you can perform the following actions:

- View the source of the audit event by clicking the link in the **Source** column.
- Refresh the list of audit events by clicking the **Refresh** icon ( ).

  Tip: The event log refreshes automatically every 30 seconds if new events are detected.
- View details about a specific audit event by clicking the link in the **Event** column and then clicking the **Details** tab.
- Export the audit log by clicking the **Export as CSV** icon ( ).

  Note: The timestamps in the exported log use the local time that is specified by the web browser.
- Exclude specific audit events from all pages on which events are displayed (see Excluding events).
- Narrow the list of audit events that are displayed on the current page:
  - Show or hide events of a specific severity by clicking the following icons:

  - **Critical events** icon ( )
  - **Warning events** icon ( )
  - **Informational events** icon ( )
- Show only events with a specific date and time. You can choose one of the following options from the drop-down list:
  - All Dates
  - Previous 2 hours
  - Previous 24 hours
  - Past Week
  - Past Month
  - Custom

  If you select **Custom**, you can filter hardware and management events that were raised between a custom start date and the current date.
- List only events that contain specific text by entering the text in the **Filter** field.
- Sort the events by column by clicking on a column heading.

Resolving an event

Lenovo XClarity Administrator provides information about the appropriate actions to perform to resolve an event.

Procedure

Complete the following steps to resolve an event.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Event Logs** to display the Logs page.

Step 2. Click the **Event Log** tab.

Step 3. Locate the event in the events log.

Step 4. Click the link in the **Event** column to view information about that event (including an explanation and recovery actions) and about the device that is the source of the event.

Step 5. Click the **Details** tab.

Step 6. Complete the recovery actions under the **Details** tab to resolve the event.

Note: If the explanation and recovery action for an event are not displayed, go to Lenovo Flex System online documentation, and search for the event title. The website always provides the most up-to-date information.

If you follow the recommended actions and the problem persists, contact Lenovo Support.

Excluding events

If there are specific events that are of no interest to you, you can exclude the events from all pages on which events are displayed. Excluded events are still in the log but are hidden from all pages on which events are displayed.

About this task

Excluded events are hidden for all users, not just the user that set the configuration.

You can place devices in maintenance mode, so that all events and alerts for those devices are excluded (see Placing devices in maintenance mode).

Restriction: Only users with administrative authority can exclude or restore events.

Procedure

Complete the following steps to exclude events from the event logs.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Event Logs**, and click the **Event Log** tab. The Event Logs is displayed.

Step 2. Select the events to be excluded, and click the **Exclude events** icon ( ). The Exclude Events dialog is displayed.

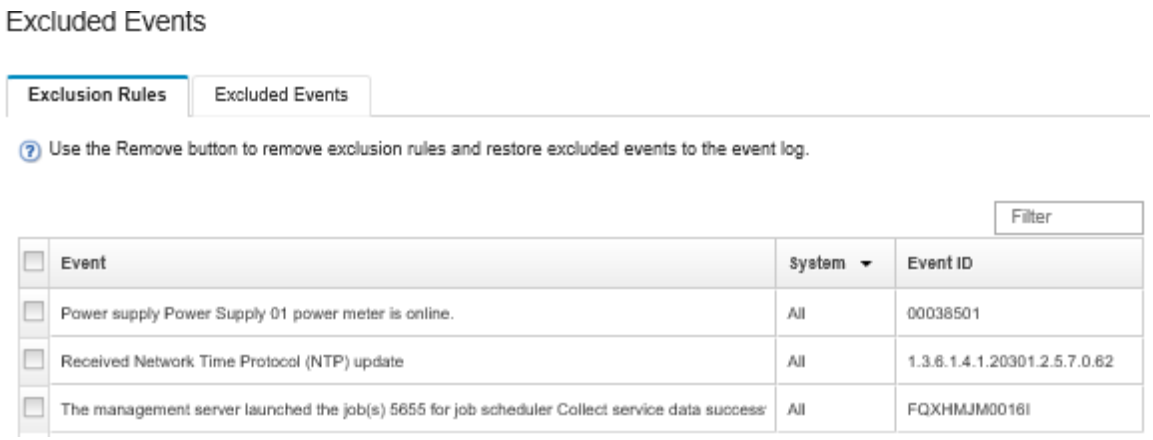
Step 3. Select one of the following options:
- **Exclude selected events from all systems**. Excludes the selected events from all managed devices.
- **Exclude events only from systems in the scope of the instance selected**. Excludes the selected events from managed devices to which the selected events apply.

Step 4. Click **Save**.

After you finish

When you exclude events, Lenovo XClarity Administrator creates exclusion rules based on information that you provide.

- View a list of exclusion rules and excluded events from the Logs page by clicking the **Show Excluded Events** icon ( ). In the Excluded Events dialog, click the **Exclusion Rules** tab to view the exclusion rules, or click the **Excluded Events** tab to view excluded events.



- Restore events that have been excluded in the event log by removing the appropriate exclusion rule. To remove an exclusion rule, click the **Show Excluded Events** icon ( ) to display the Excluded Events dialog, select the exclusion rules to restore, and click **Remove Exclusions**.
- Prevent serviceable events that are in the list of excluded events from automatically opening problem reports by clicking **Administration → Service and Support** from the Lenovo XClarity Administrator menu bar, clicking the **Service Forwarders** tab, and then selecting **No** next to the question **Do you want excluded events to open problem reports?**.

Forwarding events

You can configure Lenovo XClarity Administrator to forward events to mobile devices and to connected applications that you have in your environment for aggregating and monitoring hardware status and runtime issues for your hardware environment.

Learn more: XClarity Administrator: Monitoring

Forwarding events to syslog, remote SNMP manager, email, and other event services

You can configure Lenovo XClarity Administrator to forward events to connected applications that you have in your environment for aggregating and monitoring hardware status and runtime issues for your hardware environment. You can define the scope of events to be forwarded based on device, event class, event severity, and component.

About this task

Lenovo XClarity Administrator can forward events for one or more devices. For audit events, you can choose to forward all audit events or none. You cannot forward specific audit events. For hardware and management events, you can choose to forward events for one or more severities (critical, warning, and informational) and for one or more components (such as disk drives, processors, and adapters).

Lenovo XClarity Administrator uses event forwarders to forward events. An *event forwarder* includes information about the protocol to use, the recipient, the devices to monitor, and the events to forward. After you create and enable an event forwarder, Lenovo XClarity Administrator starts monitoring for incoming events based on the filter criteria. When a match is found, the associated protocol is used to forward the event.

The following protocols are supported:

- **Azure Log Analytics**. Lenovo XClarity Administrator forwards the monitored events to over the network to Microsoft Azure Log Analytics.
- **Email**. Lenovo XClarity Administrator forwards the monitored events to one or more email addresses using SMTP. The email contains information about the event, the host name of the source device, and links to the Lenovo XClarity Administrator web interface and Lenovo XClarity Mobile app.
- **FTP**. Forwards monitored events over the network to an FTP server.
- **REST**. Lenovo XClarity Administrator forwards the monitored events over the network to a REST Web Service.
- **SNMP**. Lenovo XClarity Administrator forwards the monitored events over the network to a remote SNMP manager. SNMPv1 and SNMPv3 traps are supported.

  For information about the management information base (MIB) file that describes the SNMP traps Lenovo XClarity Administrator generates, see lenovoMgrAlert.mib filelenovoMgrAlert.mib file in the Lenovo XClarity Administrator online documentation.
- **Syslog**. Lenovo XClarity Administrator forwards the monitored events over the network to a central log server where native tools can be used to monitor the syslog.

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Note: Events are not delivered if, for example, connectivity between Lenovo XClarity Administrator and the event forwarder is down or if the port is blocked.

Setting up event forwarding to Azure Log Analytics

You can configure Lenovo XClarity Administrator to forward specific events to Azure Log Analytics.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for Azure Log Analytics.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forwarder** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **Azure Log Analytics** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name and optional description for the event forwarder.
- Enter the primary key for the Azure Log Analytics interface.
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional**: If authentication is required, select one of the following authentication types:
  - **Basic**. Authenticates to the specified server using the specified user ID and password.
  - **None**. No authentication is used.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for Azure Log Analytics recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for Azure Log Analytics recipients are listed in the Output Format dialog.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
```

```
\"LXCA\":\"[[LXCA_IP]]\"}
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events**. Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events**. Send notifications about warranties.
- **Include Status Change events**. Sends notifications about changes in status.
- **Include Status Update events**. Sent notifications about new alerts.
- **Include Bulletin events**. Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

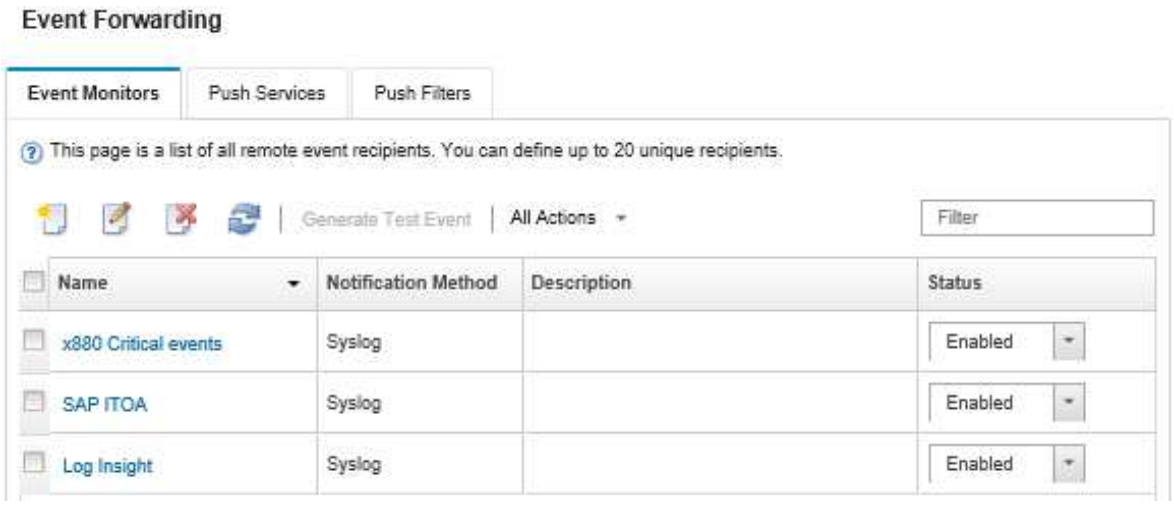
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate Azure Log Analytics server.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).

Setting up event forwarding to an email service using SMTP

You can configure Lenovo XClarity Administrator to forward specific events to an email service using SMTP.

Before you begin

To forward email to a web-based email service (such as Gmail, Hotmail, or Yahoo), your SMTP server must support forwarding web mail.

Before setting up an event forwarder to a Gmail web service, review information in Setting up event forwarding to a Gmail SMTP serviceSetting up event forwarding to syslog, remote SNMP manager, or email in the Lenovo XClarity Administrator online documentation.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for email using SMTP.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forwarder** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **Email** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name, destination host, and optional description for the event forwarder.
- Enter the port to use for forwarding events. The default is `25`.
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- Enter the email address for each recipient. Separate multiple email addresses by using a comma.

  To send the email to the support contact that is assigned for the device, select **Use Support Contact Email(s)** (see Defining the support contacts for a device in the XClarity Administrator online documentation).
- **Optional:** Enter the email address for the sender of the email (for example, `john@company.com`).

If you do not specify an email address, the sender address is LXCA.<*source_identifier*>@<*smtp_host*> by default.

If you specify only the sender domain, the format of the sender address is <*LXCA_host_name*>@<*sender_domain*> (for example, XClarity1@company.com).

Notes:

- If you set up your SMTP server to require a hostname to forward emails, and you do not set up a hostname for XClarity Administrator, it is possible that the SMTP server might reject forwarded events. If XClarity Administrator does not have a hostname, the event is forwarded with the IP address. If the IP address cannot be obtained, "localhost" is sent instead, which might cause the SMTP server to reject the event.
- If you specify the sender domain, the source does not identify in the sender address. Instead, information about the source of the event is included in the body of the email, including system name, IP address, type/model, and serial number.
- If the SMTP server accepts only emails that were sent by a registered user, the default sender address (LXCA.<*source_identifier*>@<*smtp_host*>) is rejected. In this case, you must specify at least a domain name in the **From address** field.

- **Optional:** To establish a secure connection to the SMTP server, select the following connection types:
  - **SSL**. Use the SSL protocol while communicating.
  - **STARTTLS**. Uses TLS to form a secure communication over an unsecure channel.

  If one of these connection types is selected, LXCA attempts to download and import the SMTP server's certificate to its truststore. You are asked to accept adding this certificate to the truststore.
- **Optional:** If authentication is required, select one of the following authentication types:
  - **Regular**. Authenticates to the specified SMTP server using the specified user ID and password.
  - **NTLM**. Uses the NT LAN Manager (NTLM) protocol to authentication to the specified SMTP server using the specified user ID, password, and domain name.
  - **OAUTH2**. Uses the Simple Authentication and Security Layer (SASL) protocol to authenticate to the specified SMTP server using the specified user name and security token. Typically, the user name is your email address.

    Attention: The security token expires after a short time. It is your responsibility to refresh the security token.
  - **None**. No authentication is used.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded in the email body and the format of the email subject. The information varies for each type of event forwarder.

The following example output format is the default format for email recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for the email recipients are listed in the Output Format dialog.

Email subject

```
[[DeviceName]]-[[EventMessage]]
```

Email body

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name         : [[DeviceName]]\n
Product name        : [[DeviceProductName]]\n
```

```
Host name           : [[DeviceHostName]]\n
Machine Type        : [[DeviceMachineType]]\n
Machine Model       : [[DeviceMachineModel]]\n
Serial Number       : [[DeviceSerialNumber]]\n
DeviceHealthStatus  : [[DeviceHealthStatus]]\n
IPv4 addresses      : [[DeviceIPV4Addresses]]\n
IPv6 addresses      : [[DeviceIPV6Addresses]]\n
Chassis             : [[DeviceChassisName]]\n
DeviceBays          : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID        : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity   : [[EventSeverity]]\n
  Event Class     : [[EventClass]]\n
  Sequence ID     : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID    : [[EventComponentUUID]]\n
  Serial Num      : [[EventSerialNumber]]\n
  MTM             : [[EventMachineTypeModel]]\n
  EventService    : [[EventService]]\n
  Console link    : [[ConsoleLink]]\n
  iOS link        : [[iOSLink]]\n
  Android link    : [[AndroidLink]]\n
  System Name     : [[DeviceFullPathName]]\n
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I,FQXHMEM0214I`).

- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events**. Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events**. Send notifications about warranties.
- **Include Status Change events**. Sends notifications about changes in status.
- **Include Status Update events**. Sent notifications about new alerts.
- **Include Bulletin events**. Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

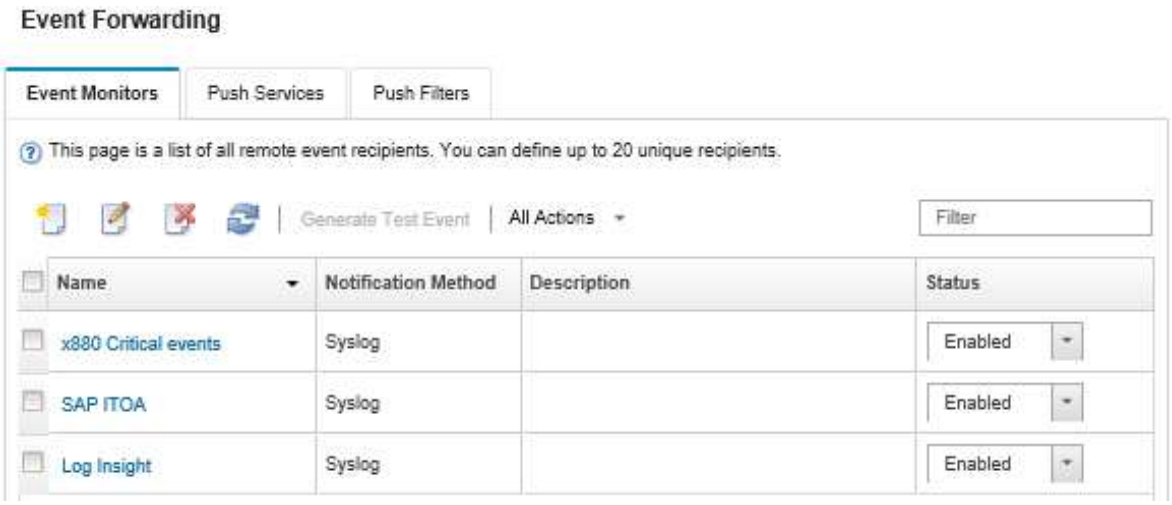
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate email service.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).

Setting up event forwarding to a Gmail SMTP service

You can setup Lenovo XClarity Administrator to forward monitored events to a web-based email service, such as Gmail.

Use the following configuration examples to help you set up your event forwarder to use the Gmail SMTP service.

Note: Gmail recommends using the OAUTH2 authentication method for the most secure communication. If you choose to use regular authentication, you will receive an email indicating that an application tried to use your account without using the latest security standards. The email includes instructions for configuring your email account to accept these types of applications.

For information about configuring a Gmail SMTP server, see https://support.google.com/a/answer/176600?hl=en.

Regular authentication using SSL on port 465

This example communicates with the Gmail SMTP server using the SSL protocol over port 465, and authenticates using a valid Gmail user account and password.

Parameter	Value
Host	smtp.gmail.com
Port	465
SSL	Select
STARTTLS	Clear
Authentication	Regular
User	Valid Gmail email address
Password	Gmail authentication password
From Address	(optional)

Regular authentication using TLS on port 587

This example communicates with the Gmail SMTP server using the TLS protocol over port 587, and authenticates using a valid Gmail user account and password.

Parameter	Value
Host	smtp.gmail.com
Port	587
SSL	Clear
STARTTLS	Select
Authentication	Regular
User	Valid Gmail email address
Password	Gmail authentication password
From Address	(optional)

OAUTH2 authentication using TLS on port 587

This example communicates with the Gmail SMTP server using the TLS protocol over port 587, and authenticates using a valid Gmail user account and security token.

Use the following example procedure to obtain the security token.

1. Create a project in the Google Developers Console, and retrieve the client ID and client secret. For more information, see the Google Sign-In for Websites webpage website.
   a. From a web browser, open the Google APIs webpage.
   b. Click **Select a project → Create a project** from the menu on that webpage. The New Project dialog is displayed.
   c. Type a name, select **Yes** to agree to the license agreement, and click **Create**.
   d. On the **Overview** tab, use the search field to search for “gmail.”
   e. Click **GMAIL API** in the search results.
   f. Click on **Enable**.
   g. Click the **Credentials** tab
   h. Click **OAuth consent screen**.
   i. Type a name in the **Product name shown to users** field, and click **Save**.
   j. Click **Create credentials → OAuth client ID**.

k. Select **Other**, and enter a name.

l. Click **Create**. The OAuth client dialog is displayed with your client ID and client secret.

m. Record the client ID and client secret for later use.

n. Click **OK** to close the dialog.

2. Use the oauth2.py Python script to generate and authorize a security token by entering the client ID and client secret that was generated when you created the project.

   Note: Python 2.7 is required to complete this step. You can download and install Python 2.7 from the Python website).

   a. From a web browser, open the gmail-oauth2-tools webpage.

   b. Click **Raw**, and then save the content as a file name `oauth2.py` on your local system.

   c. Run the following command a terminal (Linux) or a command line (Windows):

   ```
   py oauth2.py --user=<your_email> --client_id=<client_id>
      --client_secret=<client_secret> --generate_oauth2_token
   ```

   For example

   ```
   py oauth2.py --user=jon@gmail.com
      --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
   ```

   This command returns a URL that you must use to authorize the token and retrieve a verification code from the Google website, for example:

   ```
   To authorize token, visit this url and follow the directions:

   https://accounts.google.com/o/oauth2/auth?client_id=884243132302
   -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&redirect_uri=
   urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&response_type=code&scope=https%3A%2F%2Fmail.
   google.com%2F

   Enter verification code:
   ```

   d. From a web browser, open the URL that was returned in the previous step.

   e. Click **Allow** to agree to this service. A verification code to returned.

   f. Enter the verification code in the **oauth2.py** command.

   The command returns the security token and refreshes token, for example:

   ```
   Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
   Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
   Access Token Expiration Seconds: 3600
   ```

   Important: The security token expires after a period of time. You can use the oauth2.py Python script and the refresh token to generate a new security token. It is your responsibility to generate the new security token and update the event forwarder in Lenovo XClarity Administrator with the new token.

3. From the Lenovo XClarity Administrator web interface, set up event forwarder for email using the following attributes:

Parameter	Value
Host	smtp.gmail.com
Port	587
SSL	Clear
STARTTLS	Select

Parameter	Value
Authentication	OAUTH2
User	Valid Gmail email address
Token	Security token
From Address	(optional)

Setting up event forwarding to an FTP server

You can configure Lenovo XClarity Administrator to forward specific events to an FTP server.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for an FTP server.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forwarder** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **FTP** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name, destination host, and optional description for the event forwarders.
- Enter the port to use for forwarding events. The default is 21.
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional:** Specify the sequence of characters to be removed from the file content.
- Enter the file-name format to use for the file that contains the forwarded event. The default format is `event_[[EventSequenceID]].txt`.

  Note: Each file contains information for a single event.
- Enter the path on the remote FTP server where the file is to be uploaded.
- Choose the character encoding, either **UTF-8** or **Big5** . This is UTF-8 by default.
- Select the authentication type. This can be one of the following values.
  - **Anonymous**. (default) No authentication is used
  - **Basic**. Authenticates to the FTP server using the specified user ID and password.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarders.

The following example output format is the default format for FTP recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for FTP recipients are listed in the Output Format dialog.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n"
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.

5. Select the event classes and serviceability level that you want to forward.
6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, FQXHMEM0214I,FQXHMEM0214I).

- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events**. Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events**. Send notifications about warranties.
- **Include Status Change events**. Sends notifications about changes in status.
- **Include Status Update events**. Sent notifications about new alerts.
- **Include Bulletin events**. Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:
- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.

- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.

Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate FTP server.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).

Setting up event forwarding to a REST Web Service

You can configure Lenovo XClarity Administrator to forward specific events to a REST Web Service.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for a REST Web Service.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forwarder** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **REST** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the resource path on which the forwarder is to post the events (for example, /rest/test).
- Select the protocol to use for forwarding events. This can be one of the following values.
  - **HTTP**
  - **HTTPS**
- Select the REST method. This can be one of the following values.
  - **PUT**
  - **POST**
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional:** If authentication is required, select one of the following authentication types:
  - **Basic**. Authenticates to the specified server using the specified user ID and password.
  - **None**. No authentication is used.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for REST Web Service recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for REST Web Service recipients are listed in the Output Format dialog.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you

select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.
  6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.
- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events**. Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events**. Send notifications about warranties.
- **Include Status Change events**. Sends notifications about changes in status.
- **Include Status Update events**. Sent notifications about new alerts.
- **Include Bulletin events**. Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

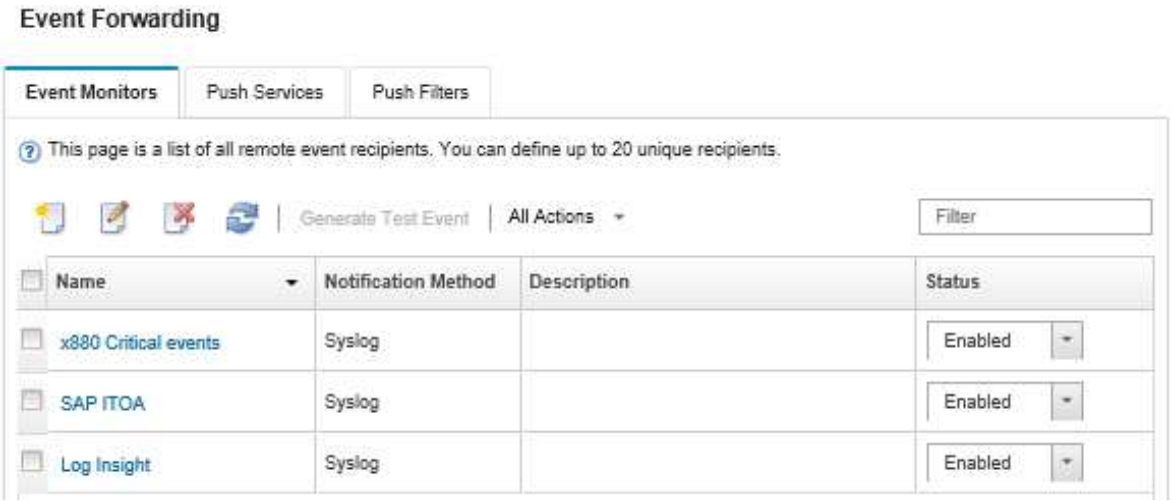
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.

4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:
- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate REST Web Service.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).

Setting up event forwarding to a remote SNMPv1 or SNMPv3 manager

You can configure Lenovo XClarity Administrator to forward specific events to a remote SNMPv1 or SNMPv3 manager.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

For information about the XClarity Administrator MIB, see lenovoMgrAlert.mib file.

Procedure

Complete the following steps to create an event forwarder for a remote SNMPv1 or SNMPv3 manager.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forwarder** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **SNMPv1** or **SNMPv3** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name and destination host for the event forwarder.
- Enter the port to use for forwarding events. The default is `162`.
- **Optional:** Enter additional information, including the description, contact name, and location.
- Select the SNMP version. This can be one of the following values.
  - **SNMPv1**. If this version is selected, specify the community password that is sent with every SNMP request to the device.
  - **SNMPv3**. This is the default version and is recommended for enhanced security. If SNMPv3 is selected, optionally specify the user ID, authentication type and password, and privacy type and password.

    If the SNMPv3 trap receiver requires the engine ID for the XClarity Administrator instance, you can find the engine ID by performing the following steps:

    1. Ensure that the connection parameters (username, authProtocol, authPassword, privProtocol, privPassword) match the ones set in XClarity Administrator.
    2. Using your preferred software (such as snmpwalk), perform an SNMP GET request on the XClarity Administrator server using one of the following OIDs:
       - EngineID: 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots : 1.3.6.1.6.3.10.2.1.2.0

       Use the following syntax for the **snmpget** command. Note that the -a forwarder authentication type can be SHA or blank (no authentication).
       ```
       snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDER_A
       ```

       For example, if the XClarity Administrator IP address is 192.0.1.0, the authentication type is SHA, and the privacy type is AES, the following command shows the engineID.
       ```
       snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_1 1
       ```

       The following example response is returned. In this example, the engineID is 0x80001370017F00000134C27E12.

```
iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
```

- Enter the time-out period (in seconds) for the request. Default is 30 seconds.
- **Optional**: If trap authentication is needed, enter the user ID and authentication password. The same user ID and password must be entered in the remote SNMP manager to which the traps are forwarded.
- Select the authentication protocol that is used by the remote SNMP manager to verify the trap sender. This can be one of the following values
  - **SHA**. Uses the SHA protocol to authentication to the specified SNMP server using the specified user ID, password, and domain name.
  - **None**. No authentication is used
- If trap encryption is needed, enter the privacy type (encryption protocol) and password. This can be one of the following values. The same protocol and password must be entered in the remote SNMP manager to which the traps are forwarded.
  - **AES**
  - **DES**
  - **None**

Step 5. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 6. Select **Enable this forwarder** to activate event forwarding for this event forwarder.

Step 7. Click **Next** to display the **Devices** tab.

Step 8. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 9. Click **Next** to display the **Events** tab.

Step 10. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I,FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.
  5. Select the event classes and serviceability level that you want to exclude.

6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.

- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 11. Choose whether to include certain types of events.

- **Include All Audit events**. Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events**. Send notifications about warranties.
- **Include Status Change events**. Sends notifications about changes in status.
- **Include Status Update events**. Sent notifications about new alerts.
- **Include Bulletin events**. Sends notification about new bulletins.

Step 12. Select the types of events and severities for which you want to be notified.

Step 13. Select whether to filter events by serviceability.

Step 14. Click **Next** to display the **Scheduler** tab.

Step 15. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

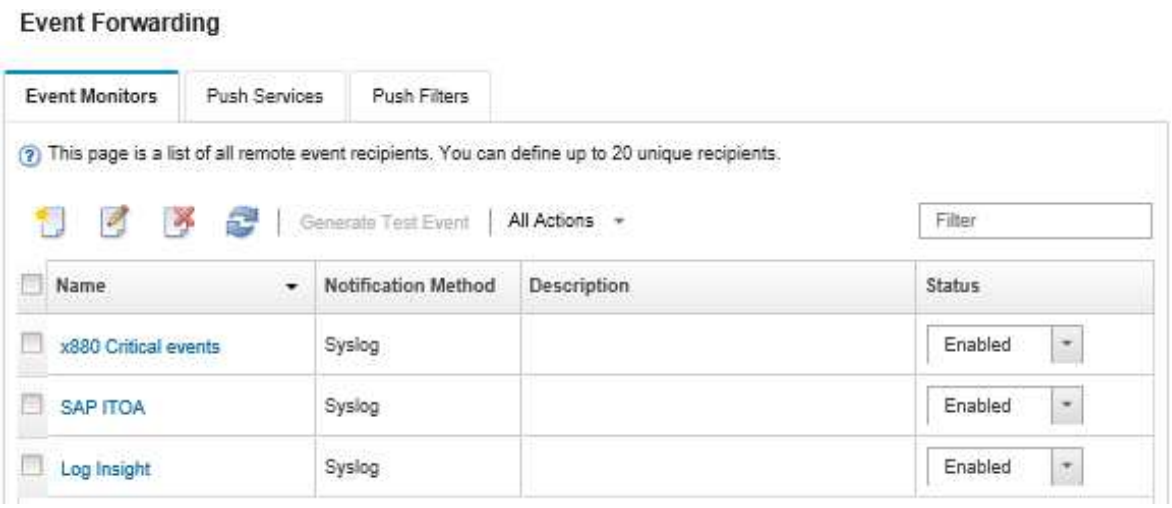
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 16. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 17. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate remote SNMP manager.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).
- Download the MIB file that contains information about SNMP traps by clicking the **Create** icon ( ), and then clicking **Download MIB File** on the General tab of New Event Forwarding dialog

lenovoMgrAlert.mib file

This management information base (MIB) file describes the SNMP traps that Lenovo XClarity Administrator generates, including alerts that were raised by XClarity Administrator and managed devices. You can compile this MIB file in any SNMP trap manager so that the SNMP traps that are sent from XClarity Administrator can be rendered meaningfully.

You can download the MIB file from the web interface by clicking **Monitoring → Event Forwarding** from the menu bar, clicking the **Create** icon ( ), selecting **SNMP** for the event-forwarder type, and then clicking **Download MIB File** at the bottom of the dialog.

The following objects are included in all outgoing SNMP traps. Additional objects might be included in some SNMP traps. All objects are described in the MIB file. Note that recovery information is not included in the trap.

Note: This list might differ from one release of XClarity Administrator to another.

- **mgrTrapAppId**. This is “Lenovo Event Manager.”
- **mgrTrapCommonEvtID**. Common event ID
- **mgrTrapDateTime**. Local date and time when the event was raised
- **mgrTrapEventClass**. The source of the event. This can Audit, Cooling, Power, Disks, Memory, Processors, System, Test, Adaptor, Expansion, IOModule, or Blade.

- **mgrTrapEvtID**. The unique identifier for the event
- **mgrTrapFailFRUs**. A comma separated list of the failing FRU UUIDs, if applicable
- **mgrTrapFailSNs**. A comma separated list of the serial numbers for failing FRUs, if applicable.
- **mgrTrapFullyQualifiedDomainName**. The fully qualified domain name: the hostname and the domain name
- **mgrTrapID**. Trap ID
- **mgrTrapMsgText**. Message text (English only)
- **mgrTrapMsgID**. Message identifier
- **mgrTrapMtm**. Model type model of the device that raised the event
- **mgrTrapService**. Serviceability indicator. This can be 000 (Unknown), 100 (None), 200 (Service Center), or 300 (Customer)
- **mgrTrapSeverity**. Severity indicator. This can be Informational, Warning, Minor, Major, or Critical
- **mgrTrapSN**. Serial number of the device that raised the event
- **mgrTrapSrcIP**. IP address of the device from which the raised event was received
- **mgrTrapSrcLoc**. Location of the device that raised the event, in English only (for example, Slot#xx)
- **mgrTrapSrcName**. Hostname or display name of the device that raised the event
- **mgrTrapSysContact**. User-configured contact ID
- **mgrTrapSysLocation**. User-configured device-location information
- **mgrTrapSystemName**. Device name, component name, and slot location
- **mgrTrapTxtId**. Host name or IP address of Lenovo Event Manager server that raised the trap
- **mgrTrapUserid**. User ID that is associated with the event (if the event is internal and event class is Audit)
- **mgrTrapUuid**. UUID of the device that raised the event

Setting up event forwarding to a syslog

You can configure Lenovo XClarity Administrator to forward specific events to a syslog.

About this task

You can create and enable up to 20 event forwarders to send events to specific recipients.

If XClarity Administrator is rebooted after event forwarders are configured, you must wait for the management server to regenerate internal data before events are forwarded correctly.

Note: For XClarity Administrator v1.2.0 and later, **Switches** is included on the **Events** tab in the New Event Forwarder and Change Event Forwarder dialogs. If you upgraded to 1.2.0 or later from an earlier release, remember to update your event forwarders to include or exclude RackSwitch events as appropriate. This is necessary even if you selected the **All Systems** checkbox to select all devices.

Procedure

Complete the following steps to create an event forwarder for a syslog.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Event Forwarder** tab.

Step 3. Click the **Create** icon ( ). The **General** tab of New Event Forwarder dialog is displayed.

Step 4. Select **Syslog** as the event-forwarder type, and fill in the protocol-specific information:

- Enter the name, destination host, and optional description for the event forwarder.
- Enter the port to use for forwarding events. The default is `514`.
- Select the protocol to use for forwarding events. This can be one of the following values.
  - **UDP**
  - **TCP**
- Enter the time-out period (in seconds) for the request. Default is 30 seconds.

- Optionally select the format for the timestamp in the syslog. This can be one of the following values.
  - **Local time**. The default format, for example `Fri Mar 31 05:57:18 EDT 2017`.
  - **GMT time**. International standard (ISO8601) for dates and times, for example `2017-03-31T05:58:20-04:00`.

Step 5. Click **Output Format** to choose the output format of the event data to be forwarded. The information varies for each type of event forwarder.

The following example output format is the default format for sylog recipients. All words between double square brackets are the variables that are replaced with actual values when an event is forwarded. The available variables for sylog recipients are listed in the Output Format dialog.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

You can click **Reset to defaults** to change the output format back to the default fields.

Step 6. Click the **Allow Excluded Events** toggle to either allow or prevent excluded event from being forwarded.

Step 7. Select **Enable this forwarder** to activate event forwarding for this event forwarder.

Step 8. Click **Next** to display the **Devices** tab.

Step 9. Select the devices and groups that you want to monitor for this event forwarder.

Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

Step 10. Click **Next** to display the **Events** tab.

Step 11. Select the filters to use for this event forwarder.

- **Match by event category**.
  1. To forward all audit events regardless of the status level, select **Include All Audit events**.
  2. To forward all warranty events, select **Include Warranty events**.
  3. To forward all health-status-change events, select **Include Status Change events**.
  4. To forward all health-status-update events, select **Include Status Update events**.
  5. Select the event classes and serviceability level that you want to forward.
  6. Enter IDs for one or more events that you want to exclude from forwarding. Separate IDs by using a comma (for example, `FQXHMEM0214I,FQXHMEM0214I`).
- **Match by event code**. Enter IDs for one or more events that you want to forward. Separate multiple IDs by using a comma.
- **Exclude by event category**.
  1. To exclude all audit events regardless of the status level, select **Exclude All Audit events**.
  2. To exclude all warranty events, select **Exclude Warranty events**.
  3. To exclude all health-status-change events, select **Exclude Status Change events**.
  4. To exclude all health-status-update events, select **Exclude Status Update events**.

5. Select the event classes and serviceability level that you want to exclude.
6. Enter IDs for one or more events that you want to forward. Separate IDs by using a comma.

- **Exclude by event code**. Enter IDs for one or more events that you want to exclude. Separate multiple IDs by using a comma.

Step 12. Choose whether to include certain types of events.

- **Include All Audit events**. Sends notifications about audit events, based on the selected event classes and severities.
- **Include Warranty events**. Send notifications about warranties.
- **Include Status Change events**. Sends notifications about changes in status.
- **Include Status Update events**. Sent notifications about new alerts.
- **Include Bulletin events**. Sends notification about new bulletins.

Step 13. Select the types of events and severities for which you want to be notified.

Step 14. Select whether to filter events by serviceability.

Step 15. Click **Next** to display the **Scheduler** tab.

Step 16. Optional: **Optional:** Define the times and days when you want the specified events to be forwarded to this event forwarder. Only events that occur during the specified time slot are forwarded.

If you do not create a schedule for the event forwarder, events are forwarded 24x7.

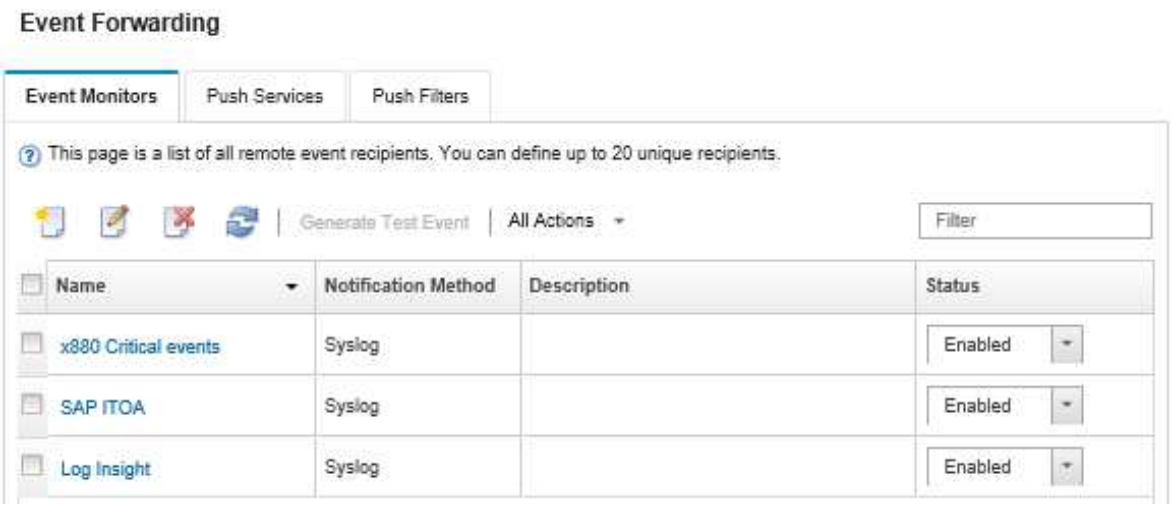
1. Use the **Scroll left** icon (◀) and **Scroll right** icon (▶), and **Day**, **Week**, and **Month** buttons to find the day and time that you want to start the schedule.
2. Double-click the time slot to open the New Time Period dialog.
3. Fill in the required information, including the date, start and end times, and whether the schedule is to be reoccurring.
4. Click **Create** to save the schedule and close the dialog. The new schedule is added to the calendar.

Tip:

- You can change the time slot by dragging the schedule entry to another time slot in the calendar.
- You can change the duration by selecting the top or bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change the end time by selecting the bottom of the schedule entry and dragging it to the new time in the calendar.
- You can change a schedule by double-clicking the schedule entry in the calendar and clicking **Edit Entry**.
- You can view a summary of all schedule entries by selecting **Show Scheduler Summary**. The summary includes the time slot for each entry and which entries are repeatable.
- You can delete a schedule entry from the calendar or scheduler summary by selecting the entry and clicking **Delete Entry**.

Step 17. Click **Create**.

The event forwarder is listed in the Event Forwarding table.



Step 18. Select the new event forwarder, click **Generate Test Event**, and then verify that the events are forwarded correctly to the appropriate syslog.

After you finish

From the Event Forwarding page, you can perform the following actions on a selected event forwarder.

- Refresh the list of event forwarders by clicking the **Refresh** icon ( ).
- View details about a specific event forwarder by clicking the link in the **Name** column.
- Change the event-forwarder properties and filter criteria by clicking the event-forwarder name in the **Name** column.
- Delete the event forwarder by clicking the **Delete** icon ( ).
- Suspend event forwarding (see Suspending event forwarding).

Suspending event forwarding

You can suspend event forwarding by disabling the event forwarder. Suspending event forwarding stops the monitoring of incoming events. Events that are received while monitoring is suspended are not forwarded.

About this task

The disabled state is not persistent. If the management node is restarted, all event forwarders become enabled.

Procedure

Complete the following steps to disable the forwarding of events.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Forwarding Events**. The Event Forwarding page is displayed.

Step 2. Select **Disable** in the **Status** column for each event forwarder that you want to suspend.

Forwarding events to mobile devices

You can configure Lenovo XClarity Administrator to push event notifications to mobile devices

Before you begin

The following requirements must be met to forward events to mobile devices:

- Ensure that a valid DNS server is configured to allow Lenovo XClarity Administrator to connect to the Apple or Google push servers. This can be configured by clicking the **Administration → Network Access → Edit Network Access** and then clicking the **Internet Settings** tab (see Configuring network access).
- Ensure that all required ports for event management are open on the network and firewalls. For information about port requirements, see Port availability in the Lenovo XClarity Administrator online documentation.

About this task

When the Lenovo XClarity Mobile app is installed on a mobile device, you can enable each connected Lenovo XClarity Administrator instance to push event notifications to that mobile device. When push notifications are enabled for a specific instance, a subscription is created in Lenovo XClarity Administrator for that mobile device.

You can define the events that are pushed to the mobile device by assigning predefined or customized global event filters for each Lenovo XClarity Administrator instance. The predefined global event filters are enabled by default. Lenovo XClarity Administrator starts monitoring for incoming events based on the filter criteria. When a match is found, the event is forwarded to the mobile device.

For more information about Lenovo XClarity Mobile and supported mobile devices, see Using the Lenovo XClarity Mobile app.

Procedure

To set up push notifications to that mobile device, complete the following steps from the Lenovo XClarity Mobile app on your mobile device.

Step 1. Enable push notifications:

- You can enable push notifications when you create a connection to a Lenovo XClarity Administrator instance. Push notifications are enabled by default.
- You can enable push notifications on existing connections by enabling one or more event filters

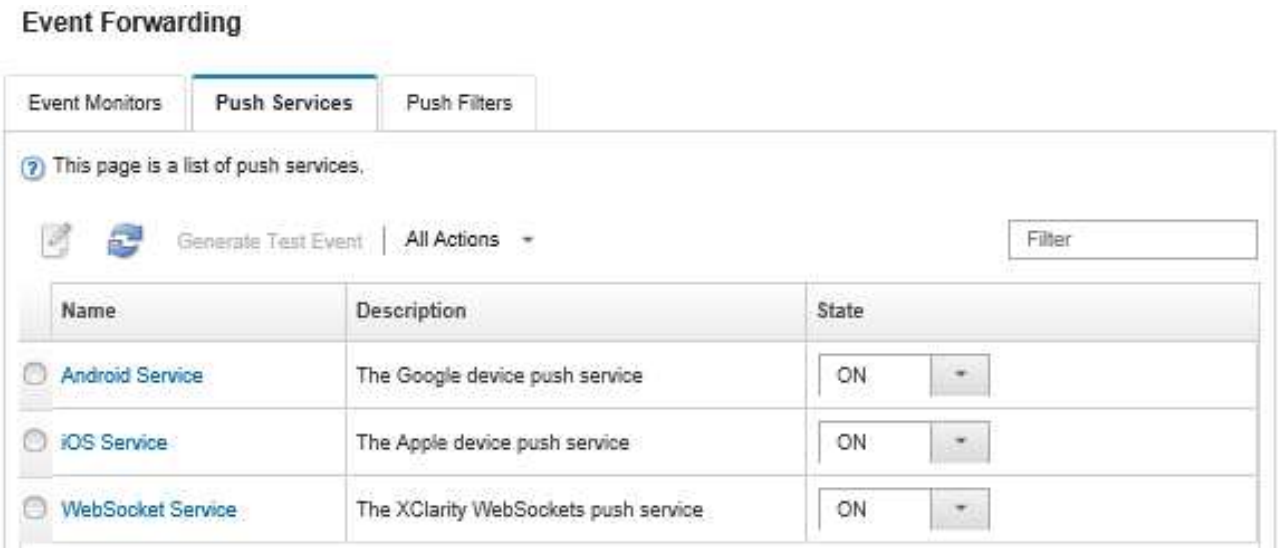
Step 2. Assign global event filters to specify which events are to be forwarded to the mobile device:

Note: You can add or remove global filters from the subscription only from the Lenovo XClarity Mobile app. You can create global filters only from the Lenovo XClarity Administrator web interface. For information about creating customized global event filters, see Creating event filters for mobile devices and WebSockets.

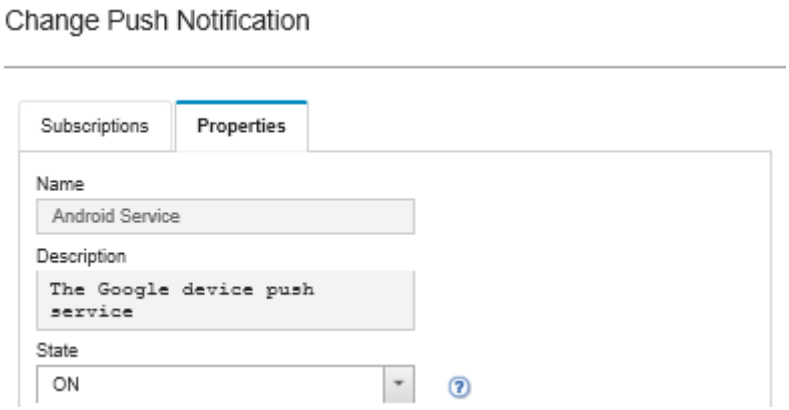
1. Tap **Settings → Push notifications**. A list of Lenovo XClarity Administrator connections is displayed.
2. Tap the Lenovo XClarity Administrator instance to display a list of push filters.
3. Enable the event filters for the events that you want pushed to the mobile device for the Lenovo XClarity Administrator instance.
4. Tap **Touch to generate test push notification** to verify that the event notifications are pushed correctly.

Results

You can manage subscriptions from the Event Forwarding page in the Lenovo XClarity Administrator web interface. Click **Monitoring → Event Forwarding** to display the Event Forwarding page.



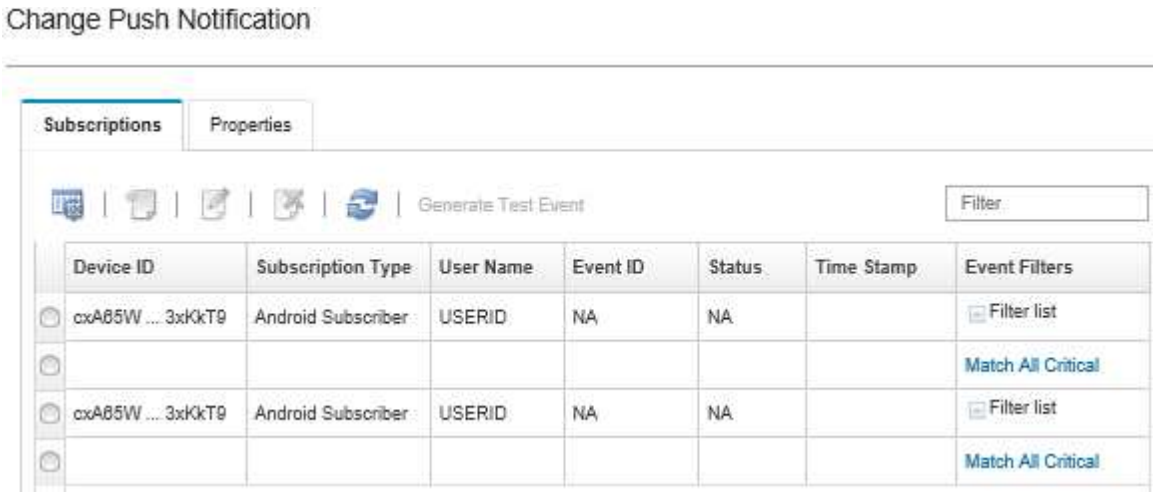
- You can change the device notification service properties from the **Push Service** tab on the Event Forwarding page by clicking the link for the push notification service (Google or Apple) in the **Name** column to display the Change Push Notification dialog, and then click the **Properties** tab.



- You can enable and disable subscriptions:
  - Enable or disable all subscriptions for a specific device notification service from the **Push Service** tab on the Event Forwarding page by selecting the **ON** or **OFF** state in the table for the device notification service.
  - Enable or disable all subscriptions for a specific device from the Lenovo XClarity Mobile app by tapping **Settings → Push notification**, and then enabling or disabling Enabled push notification.
  - Enable or disable a specific subscription from the Lenovo XClarity Mobile app by tapping **Settings → Push notification**, tapping a Lenovo XClarity Administrator connection, and enabling at least one event filter or disabling all event filters.
- You can generate a test event for all subscriptions for a specific mobile service from the **Push Service** tab on the Event Forwarding page by selecting the mobile service and clicking **Generate Test Event**.
- You can view a list of current subscriptions. From the **Push Service** tab on the Event Forwarding page, click the link for the applicable device notification service (Android or iOS) in the **Name** column to display the Change Push Notification dialog, and then click the **Subscriptions** tab. The device ID identifies each subscription.

  Tips:

  - The device ID is the first and last 6 digits of the push registration ID. You can find the push registration ID from the Lenovo XClarity Mobile app by tapping **Settings → About → Push registration ID**.
  - If you are logged in as a user with one of the following roles, all subscriptions are displayed; otherwise, subscriptions for only the logged-in user are displayed.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- You can view the list of event filters that are assigned to the subscription from the **Subscriptions** tab on the Change Push Notification dialog by expanding the **Filter list** in the **Event Filters** column for the subscription.



- You can create event filters for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription, and click the **Create** icon ( ).

  Note: These event filters apply to only a specific subscription and cannot be used by other subscriptions.

  You can also edit or remove an event filter by selecting the event filter and clicking the **Edit** icon ( ) or **Remove** icon ( ), respectively.
- You can determine the status of the last attempted push for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog. The **Time Stamp** column indicates the date and time of the last push. The **Status** indicates whether the push notification was successfully delivered to the push service. No status is available regarding whether the push notification was successfully delivered to the device from the service. If the delivery to the push service failed, the Status column provides additional information about the failure.
- You can generate a test event for a specific subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription and clicking **Generate Test Event**.
- You can remove a subscription from the **Subscriptions** tab on the Change Push Notification dialog by selecting the subscription, and clicking the **Remove** icon ( ).

Forwarding events to WebSocket services

You can configure Lenovo XClarity Administrator to push event notifications to WebSocket services.

About this task

The WebSocket subscriptions are not stored persistently in Lenovo XClarity Administrator. When Lenovo XClarity Administrator is rebooted, the WebSocket subscribers must subscribe again.

Procedure

To push event notification to a WebSocket service, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.

Step 2. Click the **Push Services** tab.

Step 3. Click the link for the **WebSocket Service** in the **Name** column. The Change Push Notification dialog is displayed.

Step 4. Click the **Subscriptions** tab.

Step 5. Click the **Create** icon ( ).

Step 6. Enter the IP address of the destination host.

Step 7. Click **Create**.

Step 8. Select the new subscription, click **Generate Test Event**, and then verify that the events are forwarded correctly to the WebSocket service.

Results

From the **Subscriptions** tab on the Change Push Notification dialog, you can perform the following actions on a selected WebSocket subscription:

- Refresh the list of WebSocket services by clicking the **Refresh** icon ( ).
- Delete subscriptions by selecting the subscriptions and clicking the **Delete** icon ( ).
- Determine the status of the last attempted push for a specific subscription by viewing the content of the **Status** column. If the attempt failed, this column contains a message that describes the error.

From the **Properties** tab on the Change Push Notification dialog, you can perform the following actions:

- Change the WebSocket service properties, including the connection idle time, maximum buffer size, maximum number of subscribers, and the register time-out period.
- You can reset the WebSocket service to the default settings by clicking **Restore Defaults**.
- Suspend pushing event notifications to all subscriptions for the WebSocket service by setting the **State** to Off.

From the **Push Service** tab on the Event Forwarding page, you can generate a test event for all WebSocket subscriptions by selecting the WebSocket service and clicking **Generate Test Event**.

Creating event filters for mobile devices and WebSockets

You can create global events filters that can be used in one or more subscriptions for mobile devices and WebSockets. You can also create event filters that are unique to a subscription.

Before you begin

You must have supervisor authority to create event filters.

You can create up to 20 global event filters.

About this task

The following global event filters are predefined:

- **Match All Critical**. This filter matches all critical events that are generated by any managed device or by XClarity Administrator.
- **Match All Warning**. This filter matches all warning events that are generated by any managed device or by XClarity Administrator.

Procedure

To create a global event filter, complete the following steps.

- Create a global event filter that can be used by any subscription.
  1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The Event Forwarding page is displayed.
  2. Click the **Push Filters** tab.
  3. Click the **Create** icon ( ). The **General** tab of New Push Filter dialog is displayed.
  4. Specify the name and option description for this event filter.
  5. Click **Next** to display the **Systems** tab.
  6. Select the devices that you want monitor.

     Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.
  7. Click **Next** to display the **Events** tab.
  8. Select the components and severities for which you want events to be forward.

     Tip:
     – To forward all hardware events, select **Match all events**.
     – To forward audit events, select **Include All Audit events**.
     – To forward warranty events, select **Include Warranty events**.
  9. Click **Create**.
- Create an event filter for a specific subscription:
  1. From the XClarity Administrator menu bar, click **Monitoring → Event Forwarding**. The New Event Forwarding page is displayed.
  2. Click the **Push Filters** tab.
  3. Select the link for the type of mobile device (Android or iOS) in the Name column of the table. The Change Push Notification dialog is displayed.
  4. Click the **Subscriptions** tab to display a list of active subscriptions.
  5. Select the subscription, and click the **Create** icon ( ). The **General** tab of New Event Filter dialog is displayed.
  6. Specify the name and option description for this event filter.
  7. Click **Next** to display the **Systems** tab.
  8. Select the devices that you want monitor.

     Tip To forward events for all managed devices (current and future), select the **Match all systems** checkbox.If you do not select the **Match all systems** checkbox, ensure that the selected devices do not have a DUMMY-UUID in the UUID column. A Dummy-UUID is assigned to devices that have not

yet recovered after a restart or are not discovered completely by the management server. If you select a device with a Dummy-UUID, event forwarding works for this device until the moment when the device is fully discovered or recovered and the Dummy-UUID changes to its real UUID.

9. Click **Next** to display the **Events** tab.
10. Select the components and severities for which you want events to be forward.

    Tip:
    - To forward all hardware events, select **Match all events**.
    - To forward audit events, select **Include All Audit events**.
    - To forward warranty events, select **Include Warranty events**.
11. Click **Create**.

After you finish

From the Push Filters tab on the Event Forwarding page, you can perform the following actions on a selected event filter:

- Refresh the list of event filters by clicking the **Refresh** icon ( ).
- View details about a specific event filter by clicking the link in the **Name** column.
- Change the event filter properties and filter criteria by clicking the **Edit** icon ( ).

Delete the event filter by clicking the **Delete** icon ( ).

Working with jobs

Jobs are longer running tasks that are performed against one or more devices. You can schedule certain jobs to run only one time (immediately or at later time), on a reoccurring basis, or when a specific event occurs.

Jobs run in the background. You can see the status of each job from the jobs log.

Monitoring jobs

You can view a log of all jobs that are started by Lenovo XClarity Administrator. The jobs log includes jobs that are running, completed, or have errors.

About this task

Jobs are longer running tasks that are performed against one or more devices. For example, if you deploy an operating system to multiple servers, each server deployment is listed as a separate job.

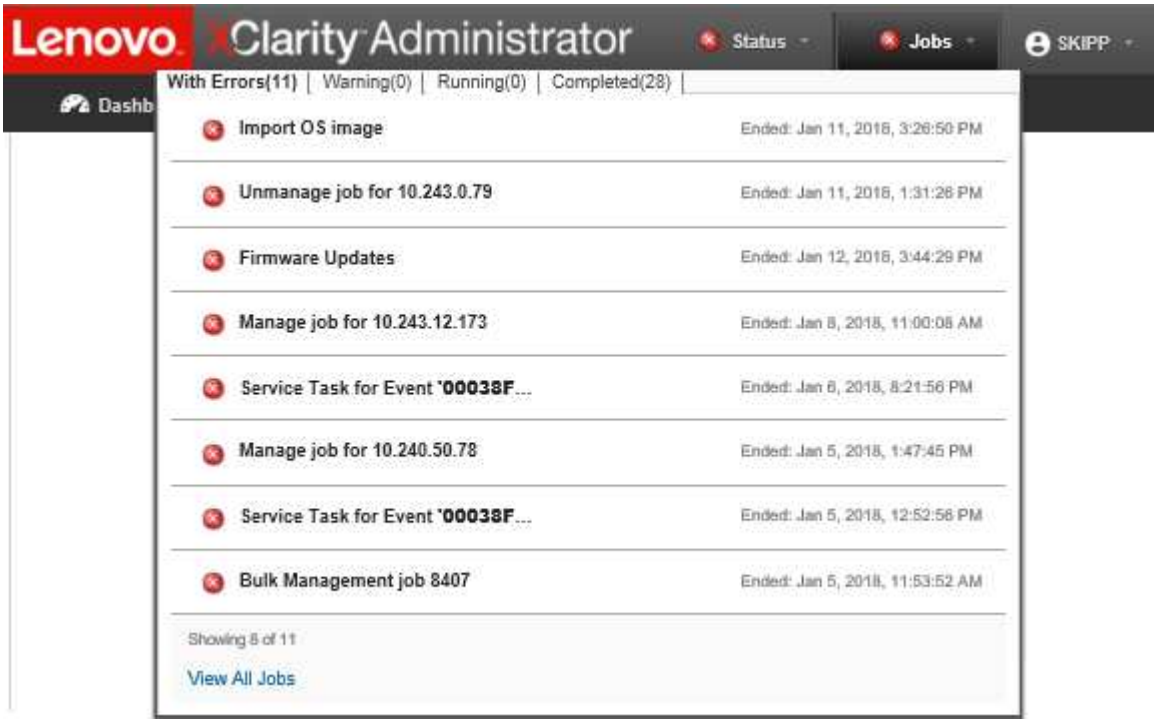
Jobs run in the background. You can see the status of each job from the jobs log.

The jobs log contains information about each job. The log can contain a maximum of 1000 jobs or 1 GB. When the maximum size is reached, the oldest jobs that completed successfully are deleted. If there are no jobs that completed successfully in the log, the oldest jobs that completed with warnings are deleted. If there are no jobs that completed successfully or with warnings in the log, the oldest jobs that completed with errors are deleted.

Procedure

Complete one of the following steps to display the jobs log.

- From the XClarity Administrator title bar, click **Jobs** to display a summary of jobs that are running, completed, and have errors.

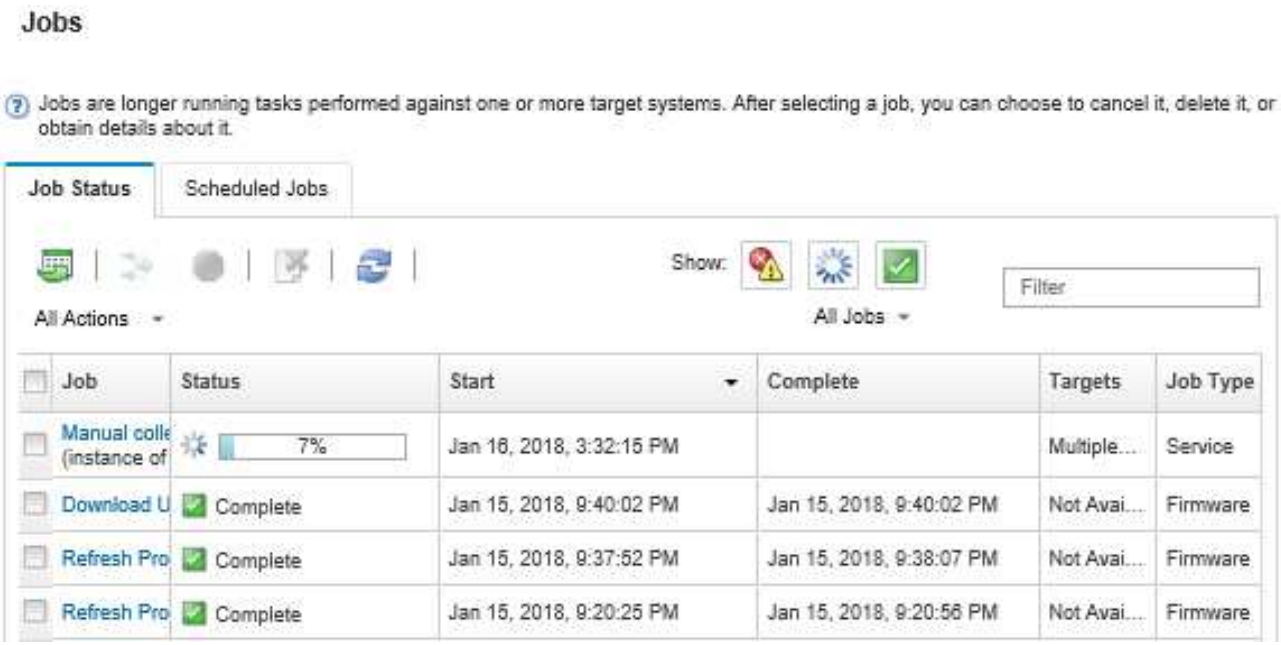


  From this pull down, you can click the following tabs:
  - **Errors**. Displays a list of all jobs that have errors associated with them.
  - **Warnings**. Displays a list of all jobs that have warnings associated with them.
  - **Running**. Displays a list of all jobs that are currently in progress.
  - **Completed**. Displays a list of all jobs that are completed.

  Hover over a job entry in the pull down to get more information about the job, including the status, progress, and user that created the job.
- From the XClarity Administrator title bar, click **Jobs**, and click the **View All Jobs** link to display the Jobs Status page.
- From the XClarity Administrator menu bar, click **Monitor → Jobs** and click the **Job Status** tab to display the Jobs Status page.

After you finish

The Jobs page is displayed with a list of all jobs for XClarity Administrator.



From this page, you can perform the following actions:

- Create job schedules by clicking the **Scheduled Jobs** tab (see Scheduling jobs).
- View more information about a specific job by clicking the job description in the **Jobs** column. A dialog is displayed with a list of subtasks (subjobs) and their targets, a summary of the subtasks including any necessary actions, and log details including the severity and timestamp for each message. You can choose to hide or show logs for child tasks.
- For scheduled jobs, view information about the job schedule by clicking the “this” link under the job description in the **Jobs** column.
- Change the number of jobs that are displayed per page. The default is 10 jobs. You can display 25, 50, or all jobs.
- Narrow the list of jobs that are displayed:
  - List only jobs from a specific source by clicking **Job Types** and choosing from the following options.
    - **All Job Types**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**
    - **Power**
    - **Remote Access**
    - **System ID**
    - **OS Images**
    - **OS Deployment**
    - **OS Profile Export**
    - **Custom**
    - **Inventory**
    - **Unknown**
  - List only scheduled jobs that are associated with a specific schedule type by clicking **Schedule Types** and choosing from the following options.
    - **All Schedule Types**

  - **One Time**
  - **Recurring**
  - **Triggered**
- Hide or show jobs that have errors or warnings by clicking the **Hide error/warning jobs** icon ( ).
- Hide or show jobs that are currently running by clicking the **Hide running jobs** icon ( ).
- Hide or show jobs that are completed by clicking the **Hide completed jobs** icon ( ).
- List only jobs that contain specific text by entering the text in the **Filter** field.
- If filtering is applied to the page, remove the filter by clicking the **Show All Jobs** icon ( ).
- Sort the jobs by column by clicking a column heading.

- Export the jobs list as a CSV file by clicking the **Export as CSV** icon ( ).

  Note: The timestamps in the exported log use the local time that is specified by the web browser.
- Cancel running jobs or subtasks by selecting one or more running jobs or subtasks and clicking the **Stop** icon ( ).

  Note: It might take several minutes to cancel the job.
- Delete completed jobs or subtasks from the jobs log by selecting one or more completed jobs or subtasks and clicking the **Delete** icon ( ).
- Export information about specific jobs by selecting the jobs and clicking the **Export as CSV** icon ( ).
- Refresh the jobs log by clicking the **Refresh** icon ().

Scheduling jobs

You can create schedules in Lenovo XClarity Administrator to run certain tasks at specific times.

About this task

You can schedule the following types of jobs:
- Simple tasks, such as powering off and rebooting
- Collecting service data for specific devices
- Refreshing the firmware-update and OS device-driver catalogs from the Lenovo website
- Refreshing the XClarity Administrator updates catalog from the Lenovo website
- Downloading firmware from the Lenovo website
- Updating firmware and OS device drivers on managed devices
- Backing up XClarity Administrator data and settings
- Backing up and restoring switch configuration data

You can schedule jobs to run:
- Only one time (immediately or at a later time)
- On a recurring basis
- When a specific event occurs

Procedure

To create and schedule a job, complete the following steps.

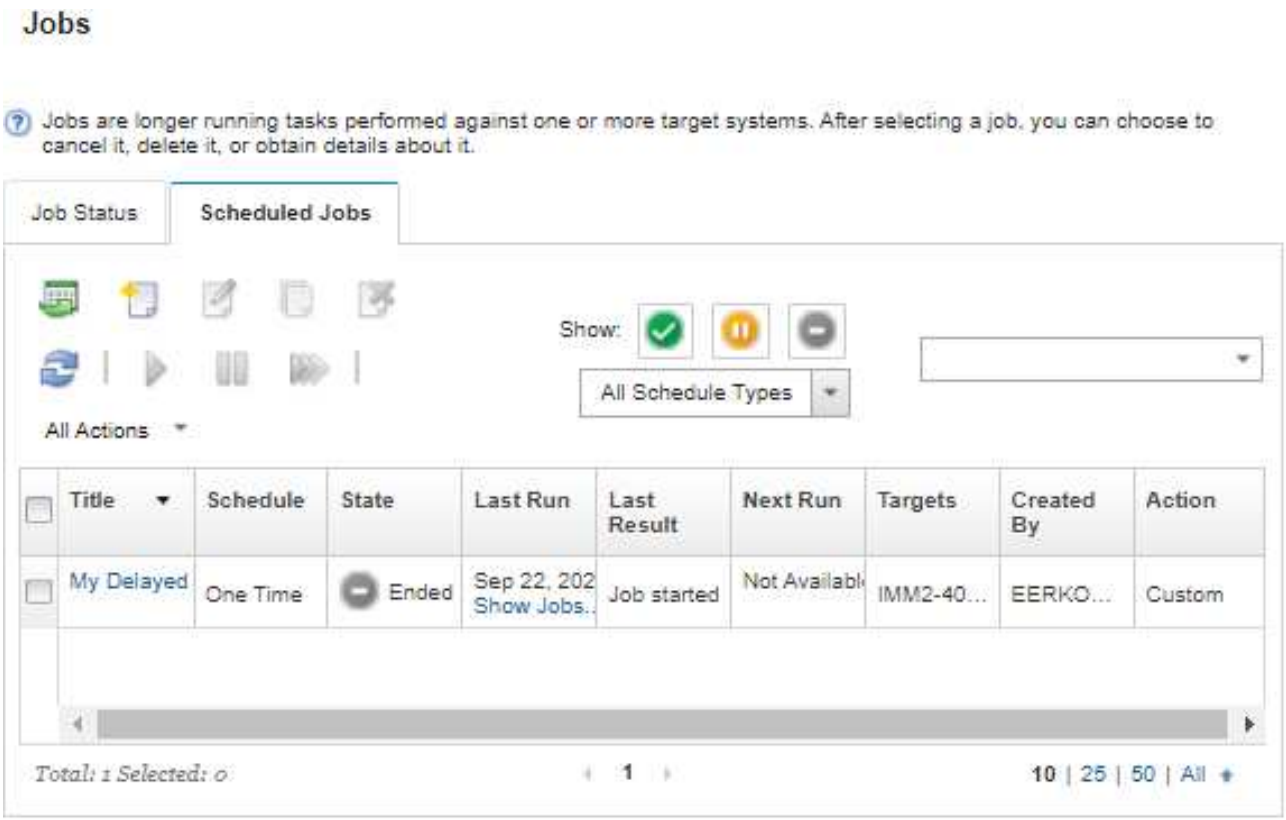
- For complex tasks, such as updating firmware and collecting service data, create the job from the current the task page or dialog.

1. Click **Schedule** to create a schedule for running this task. The Schedule New Job dialog is displayed.
2. Enter a name for the job.
3. Specify when the job is to be run. The available options depend on the type of job. Some jobs cannot be recurring or triggered by an event
   - **One Time**. These jobs run only one time. Specify the date and time when you want this job to run.
   - **Recurring**. These jobs run more than one time. Specify the when and how often you want this job to run.
   - **Triggered by Event**. These jobs run when a specific event occurs.
     a. Specify the date and time when you want this job to run, and click **Next**.
     b. Select the event to trigger the job.
4. Click **Create Job**.

- For simple tasks, such as powering on and rebooting, create the job schedule from the Jobs page.
  1. From the XClarity Administrator menu bar, click **Monitor → Jobs**, and click the **Scheduled Job** tab to display the Scheduled Jobs page.
  2. Click the **Create** icon ( ) to display the Schedule New Jobs dialog.
  3. Enter a name for the job.
  4. Specify when the job is to be run.
     - **One Time**. These jobs run only one time.
       a. Specify the date and time when you want this job to run, and click **Next**.
       b. Select managed devices on which the job is to run.
     - **Recurring**. These jobs run more than one time.
       a. Specify the when and how often you want this job to run.
       b. Select managed devices on which the job is to run**.**
     - **Triggered by Event**. These jobs run when a specific event occurs.
       a. Specify the date and time when you want this job to run, and click **Next**.
       b. Select managed devices on which the job is to run, and click **Next**.
       c. Select the event to trigger the job.
  5. Click **Create**.

After you finish

The Scheduled Jobs tab is displayed with a list of all job schedules in XClarity Administrator.



From this page, you can perform the following actions:

- View information about all active and completed jobs for a specific job schedule by clicking the link in the **Job** column.
  - Narrow the list of job schedules that are displayed by a specific schedule type by clicking **Schedule Types** and choosing from the following options:
    - **All Schedule Types**
    - **One Time**
    - **Recurring**
    - **Triggered**
  - Hide or show only job schedules that are in a specific state by clicking one of the following icons:
    - All scheduled jobs that are active by clicking the **Active** icon ( ).
    - All scheduled jobs that are not active by clicking the **Paused** icon ( ).
    - All scheduled jobs that already ran and are not scheduled to run again by clicking the **Ended** icon ( ).
  - List only scheduled jobs that contain specific text by entering the text in the **Filter** field.
  - Sort the scheduled jobs by column by clicking a column heading.
- View when the job ran last by looking at the **Last Run** column. View the status of the last run job by clicking the “Job Status” link in that column.
- View when the job is scheduled to run next by looking at the **Next Run** column. View a list of all future dates and times by clicking the “More” link in that column.
- Immediately run the job that is associated with the schedule by clicking the **Run** icon ( ).
- Disable or enable a job schedule by clicking the **Pause** icon ( ) or **Activate** icon ( ) respectively.

- Copy and then modify a job schedule by clicking the **Copy** icon ( ).
- Edit a job schedule by clicking the **Edit** icon ( ).
- Delete one or more selected job schedules by clicking the **Delete** icon ( ).
- Export information about specific job schedules by selecting the schedules and clicking the **Export as CSV** icon ( ).
- Refresh the list of job schedule by clicking the **All Actions → Refresh**.

Adding a resolution and comments to a job

You can add a resolution and comments to a completed job, regardless of the success or error state. You can do this for a parent job and for subtasks in the job.

Procedure

Complete one of the following steps to add a resolution and comments to a job.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Monitor → Jobs**, and click the **Job Status** tab to display the Jobs Status page.

Step 2. Click the link for the job in the **Job** column to display the job details.

Step 3. Click the **Notes** icon ( ) to display the Notes dialog.

From this dialog, you can see a history of all notes and resolutions that were added to the job. You can clear the history by clicking **Clear All Records**.

Step 4. Choose one of the following resolutions.
- **No Changes**
- **Investigating**
- **Resolved**
- **Aborted**

Step 5. Add a remark in the **Note** field.

Step 6. Click **Apply**.

On the Job Status page, the resolution is displayed in the **Status** column for that job.

Viewing relationships between jobs and events

A *flow diagram* is a graphical view that shows relationships between activities (including jobs and events) that are manually initiated by a user or automatically initiated by Lenovo XClarity Administrator. The flow diagram helps to identify problems by illustrating the sequence of actions that were initiated and events that were generated, when they generated, and what caused them to be generated.

Before you begin

Activity flows are disabled by default. You must enable activity flows before flows can be generated for an activity. You can view flows only for activities that occur when Activity Flow is enabled.

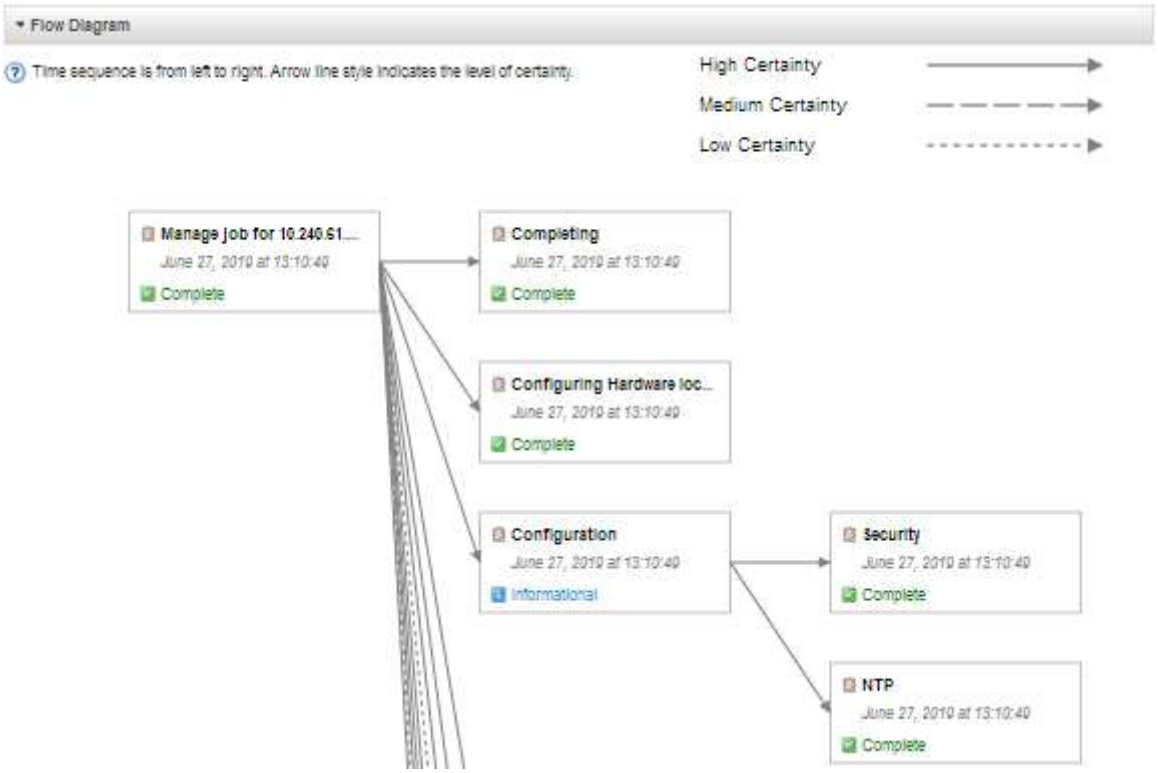
Attention: Activity flows increase memory usage by XClarity Administrator. It is recommended that you do not enable activity flows if memory usage by XClarity Administrator is already high.

About this task

The following example illustrates a flow diagram. The sequence of events flow from left to right. Each node in the flow represents a single activity and includes the activity description, date, and status. You can hover the cursor over the node title to view additional information about the activity.

The style of the lines between the nodes indicates the certainty of relationship between nodes.

- Solid lines represent a high certainty.
- Long-dashed lines represent a medium certainty.
- Short-dashed lines represent a low certainty.



Procedure

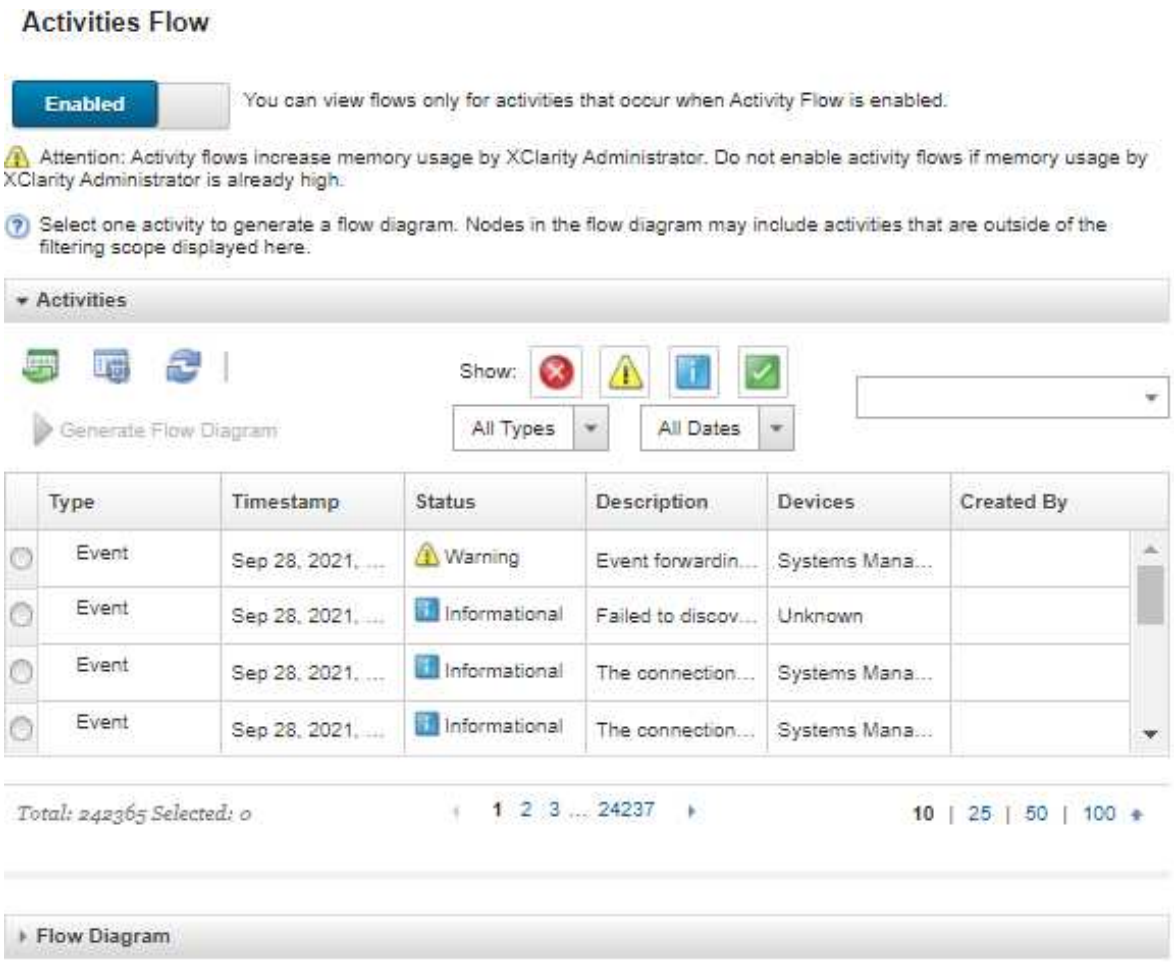
Complete the following steps to view the flow diagram for a specific activity.

Step 1. From the XClarity Administrator menu bar, click **Monitoring → Activities flow** to display the Activities flow page

Step 2. Enable activity flows by selecting **Enable Activities Flow**.

Step 3. In the **Activities** section, select the job or event.

You can sort the table columns to make it easier to find specific activities. In addition, you can select a status type, activities type, date, enter a custom filter, or enter text (such as a name or IP address) in the **Filter** field, and to list only those activities that meet the selected criteria



Step 4. Click **Generate Flow Diagram** to display the flow diagram in the **Flow Diagram** section

After you finish

From this page you can perform the following actions:

- View additional information about each activity in the flow diagram by hovering the cursor over the activity.
- Export related flow for the selected activities to a CSV file clicking the **Actions → Export to CSV**.

Chapter 4. Management considerations

There are several alternatives to choose from when managing devices. Depending on the devices being managed, you might need multiple management solutions running at the same time.

A device can be managed by only one instance of Lenovo XClarity Administrator. However, you can use other management software (such as VMware vRealize Operations Manager) in tandem with Lenovo XClarity Administrator to *monitor* devices that XClarity Administrator manages.

Attention: Extra care must be taken when using multiple management tools to manage your devices to prevent unforeseen conflicts. For example, submitting power-state changes using another tool might conflict with configuration or update jobs that are running in XClarity Administrator.

ThinkSystem, ThinkServer and System x devices

If you intend to use another management software to monitor your managed devices, create a new local user with the correct SNMP or IPMI settings from the IMM interface. Ensure that you grant SNMP or IPMI privileges, depending on the your needs.

Flex System devices

If you intend to use another management software to monitor your managed devices, and if that management software uses SNMPv3 or IPMI communication, you must prepare your environment by performing the following steps for each managed CMM:

1. Log in to the management controller web interface for the chassis using the `RECOVERY_ID` user name and password.
2. If the security policy is set to **Secure**, change the user authentication method.
   a. Click **Mgt Module Management → User Accounts**.
   b. Click the **Accounts** tab.
   c. Click **Global login settings**.
   d. Click the **General** tab.
   e. Select **External first, then local authentication** for the user authentication method.
   f. Click **OK**.
3. Create a new local user with the correct SNMP or IPMI settings from the management controller web interface.
4. If the security policy is set to **Secure**, log out and then log in to the management controller web interface using the new user name and password. When prompted, change the password for the new user.

You can now use the new user as an active SNMP or IPMI user.

Note: If you unmanage and then manage the chassis again, this new user account becomes locked and disabled. In this case, repeat these steps to create a new user account.

© Copyright Lenovo 2015, 2022

Chapter 5. Managing resource groups

You can use resource group in Lenovo XClarity Administrator to create logical set of managed devices that you can view collectively and act on.

Learn more: XClarity Administrator: Resource groups

About this task

There are three types of resource groups:

- **Static**. Customized group of specific devices.
- **Dynamic**. Rule-based group of devices (for example, all servers of a specific type). This group contains a dynamic list of devices based on a set of inventory properties.

Actions cannot be performed on a resource group; however, you can select all devices in the group, and perform actions collectively on all selected devices.

Viewing the status of devices in a resource group

You can view the status of all managed devices in a resource group.

About this task

The following status icons are used to indicate the overall health of all devices the resource group. The overall health of the group indicates the device with the highest severity in the group.

- **Critical** icon ( )
- **Warning** icon ( )
- **Normal** icon ( )

Procedure

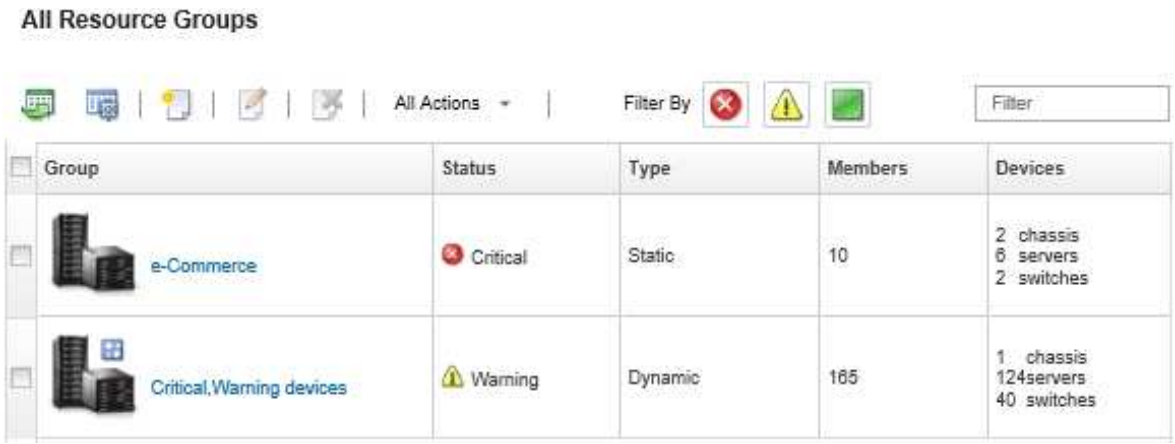
Complete the following steps to view the status of devices in a resource group.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of all managed devices and other resources, including resource groups.

© Copyright Lenovo 2015, 2022

Step 2. From the XClarity Administrator menu bar, click **Hardware → Resource Groups**. The All Resource Groups page is displayed.

The All Resource Groups page lists each resource group, including the name of the group, the number of managed devices that are in the group, and the status of the device with the highest severity in the group.



From this page, you can perform the following actions:

- Create a new resource group (see Creating a dynamic resource group and Creating a static resource group)
- Edit group membership by selecting a group and clicking the **Edit** icon ( ).
- Edit group properties by selecting the group and clicking **All Actions → Edit properties**.
- Remove a resource group by selecting a group and clicking the **Delete** icon ( ).

Note: Removing a group only removes the group definition. It does not affect the devices in the group.

- Export detailed information about all devices in one or more resource groups to a CSV file clicking the **Export** icon ( ).

Step 3. From the All Resource Groups page, click the name in the **Groups** column to display the list of devices in that group.

From this page, you can perform the following actions:

- Add or remove devices in a static resource group by clicking the **Edit** icon ( ).
- Display detailed information about a specific device in the resource group by clicking the device name in the **Device Name** column.
- Export detailed information about all devices in one or more resource groups to a CSV file clicking the **Export** icon ( ).

Viewing the members of a resource group

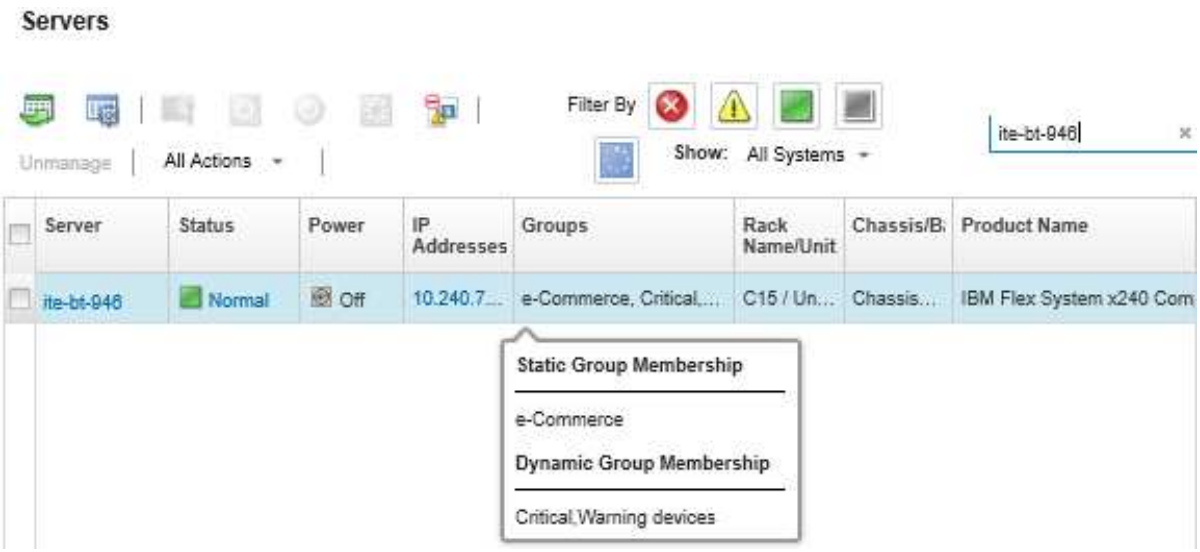
You can view detailed information about the resource groups including group members.

Procedure

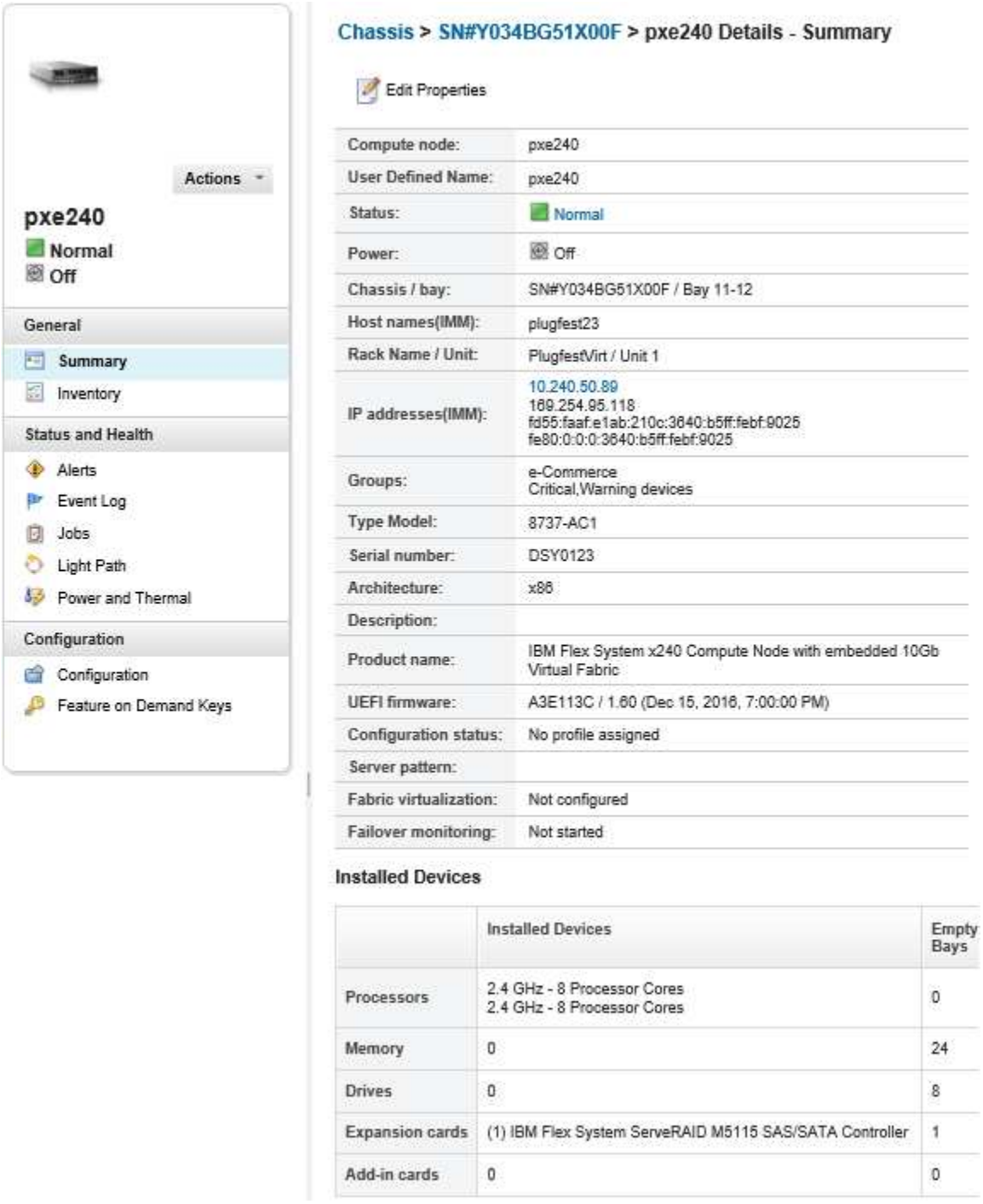
Complete the following steps to view group membership.

- To view all groups of which a device is a member.
  1. From the Lenovo XClarity Administrator menu bar, click **Hardware** and then click the device type to the display the all-devices page.

     Hover over the group lists in the **Groups** column to list the groups of which the device is a member.

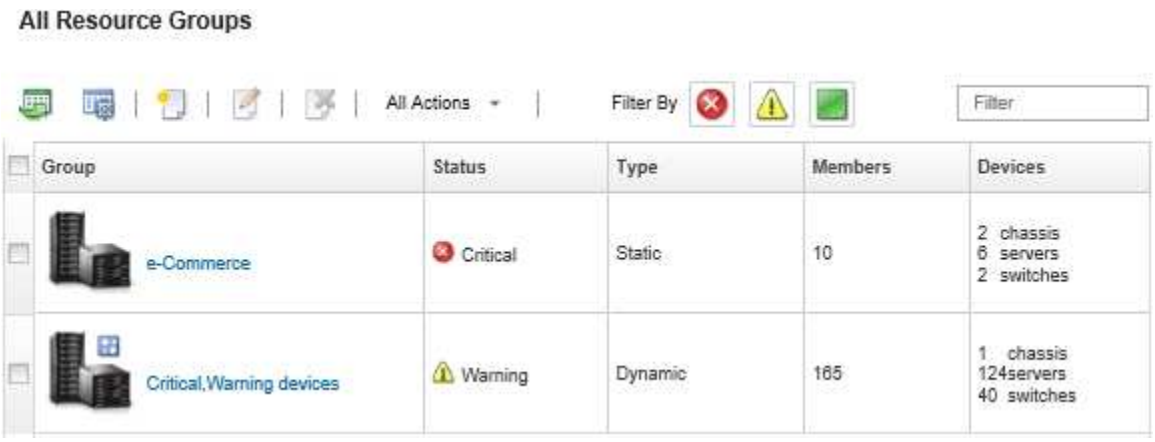


2. Click the link for the device name in the first column. The summary page for that device is displayed, including a list of resource groups of which the device is a member.



- To view the members of a group.
  1. From the XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of the all managed devices and other resources, including racks.
  2. From the XClarity Administrator menu bar, click **Hardware → Groups**. The Resource Groups page is displayed.

     This page lists the total number of members and the number of member of each device type in the group.



3. From the All Resource Groups page, click the name in the **Groups** column to display the resource group details.

   This page lists each device that is a member of the resource group.

Creating a dynamic resource group

You can create a resource group for a dynamic set of managed devices based on a set of criteria.

About this task

You can create a dynamic resource group using one or more of the following criteria for each device type.

Criteria	Chassis	Dense chassis	Servers	Flex System switch	RackS-witch switch	Storage device
Add-in card name			✓ (except ThinkServ-er)			
Contact	✓		✓		✓	✓
Description	✓	✓	✓		✓	✓
Fully-qualified domain name	✓		✓			
Hostname	✓		✓	✓	✓	

Criteria	Chassis	Dense chassis	Servers	Flex System switch	RackS-witch switch	Storage device
IPv4 address*	✓		✓	✓	✓	✓
IPv6 address	✓		✓	✓	✓	
Location	✓	✓	✓		✓	✓
Machine type	✓		✓	✓	✓	✓
Model	✓		✓	✓	✓	✓
Overall health state	✓		✓	✓	✓	✓
Processor cores			✓			
Product name	✓		✓	✓	✓	✓
Rack	✓	✓	✓		✓	✓
Room	✓	✓	✓		✓	✓
User-defined name	✓	✓ (v2.1.0 and later)	✓	✓	✓	✓

Note: For IPv4 addresses, you can specify a single address or a range of addresses, separated by dash or using an asterisk as wildcard (for example, `1.1.1.*` or `1.1.1.1-1.1.1.255` without spaces).

Procedure

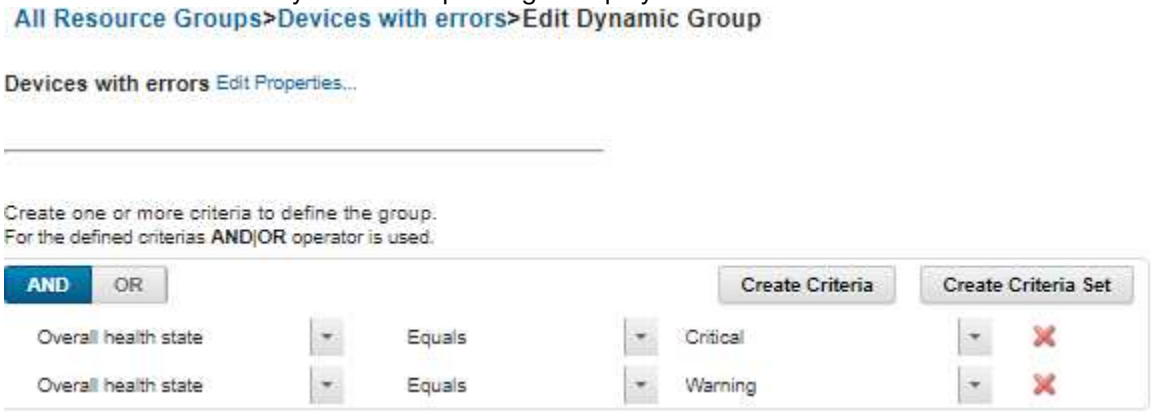
To create and populate a dynamic resource group, complete the following steps

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Resource Groups**. The All Resource Groups page is displayed.

Step 2. Click the **Create** icon ( ) to create an empty group. The Create Empty Group dialog is displayed.

Step 3. Select **Dynamic Group** to group of devices based on a set of criteria.

Step 4. Click **Create**. The Edit Dynamic Group dialog is displayed.



Step 5. Add criteria for this dynamic group.

- Select the operator to use for the group set. This can be one of the following values:
  - **AND**. Members must satisfy all specified values.
  - **OR**. Members must satisfy one or more of the specified values.
- Click **Create Criteria** to add and a new criteria rule to the set.

- Click **Create Criteria Set** to add a subset of criteria rules.

Note: New criteria and criteria sets are always added to the bottom of the list.

Step 6. Click **Apply** to save the group criteria and create the group, or click **Preview** to see what devices are included in the group using the current criteria without creating the group.

After you finish

- You can see which resource groups a device belongs from the **Groups** column on the all-devices pages and the device summary pages.
- You can modify the criteria for the dynamic group by selecting the resource group and clicking the **Edit** icon ( ).
- You can modify resource-group properties by clicking **All Actions → Edit properties**.

Creating a static resource group

You can create a resource group that contains a customized set of managed devices.

Procedure

To create and populate a static resource group, complete the following steps.

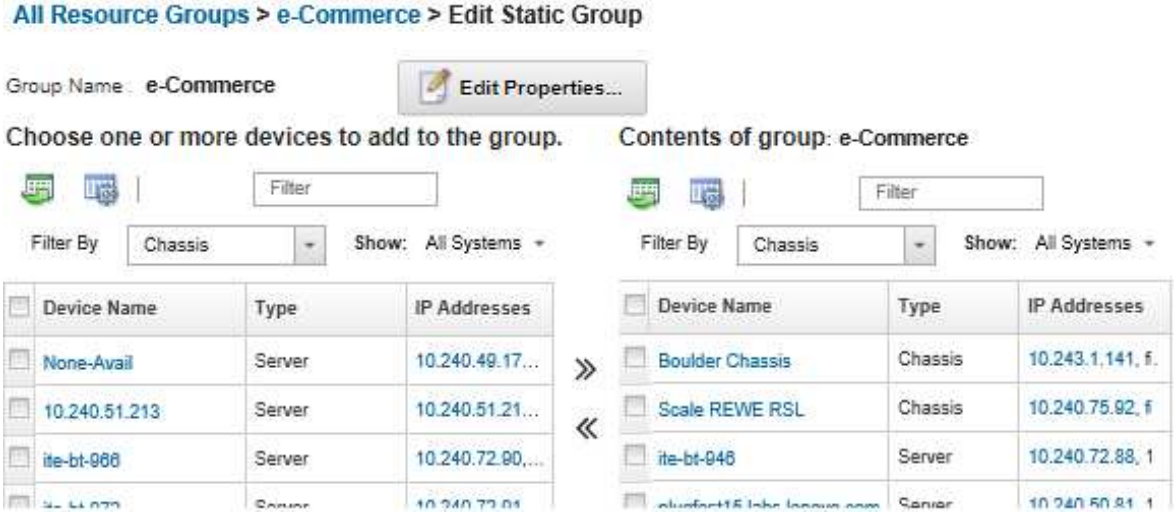
Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Resource Groups**. The Resource Groups page is displayed.

Step 2. Click the **Create** icon ( ) to create an empty group. The Create Empty Group dialog is displayed.

Step 3. Specify the group name and optional description.

Step 4. Select **Static Group** to create a group of explicitly defined devices.

Step 5. Click **Create**. The Edit Static Group page is displayed.



Step 6. Select the devices that you want to add to the group from the **All available devices not in group** list, and click the **Add** icon (») to move the selected devices to the **Contents of group** list.

Notes:

- You can sort the lists to make it easier to find specific devices by clicking on the column headers. In addition, you can select a device type from the **Filter By** drop-down list, select a chassis from the drop-down list, or enter text (such as a name or IP address) in the **Filter** field to list only those devices that meet the selected criteria

- If you choose to move a chassis to the group, the devices in the chassis are not automatically added to the group. To add all chassis components to the group, select **Chassis → <*chassis_name*>** in the **Show** drop-down menu to list all components in the specified chassis, select the checkbox next to the Device Name column heading to select all devices, and then click the **Add** icon (») to move the selected devices to the **Contents of group** list.

After you finish

- You can see which resource groups a device belongs from the **Groups** column on the all-devices pages and the device summary pages.
- You can add or remove a device from a static resource group from the all-devices pages and the device details pages by clicking **All Actions → Groups → Add to Group** or **All Actions → Groups → Remove from Group**.

  Note: You can add and remove devices only from static resource groups. You cannot remove them from dynamic groups.
- You can modify resource-group properties by clicking **All Actions → Edit properties**.

Removing a resource group

You can remove a resource group from Lenovo XClarity Administrator.

About this task

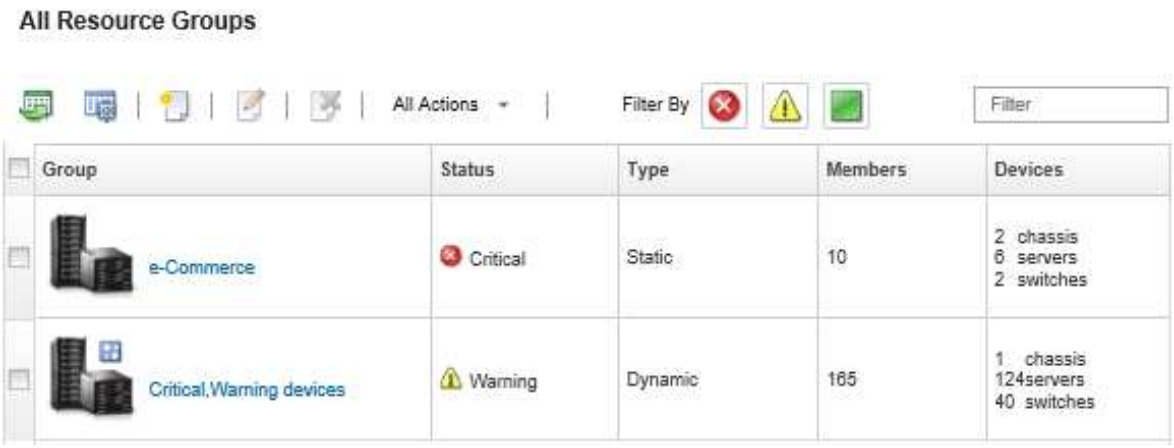
Deleting a group only deletes the group definition. It does not affect the devices in that group.

Procedure

Complete the following steps to remove a resource group.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Resource Groups**. The All Resource Groups page is displayed.

The All Resource Groups page lists each resource group, including the name of the group, the number of managed devices that are in the group, and the status of the device with the highest severity in the group.



Step 2. Select the resource group to be removed.

Step 3. Click the **Delete** icon (✖).

Step 4. Click **Delete**.

Modifying resource-group properties

You can modify the properties for a specific resource group.

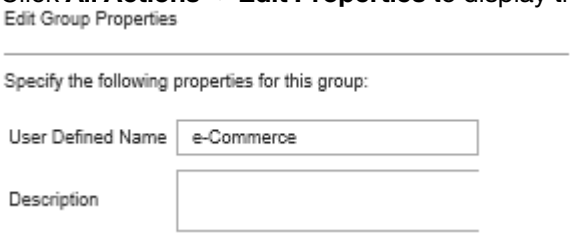
Procedure

Complete the following steps to modify the resource-group properties

Step 1. From the XClarity Administrator menu bar, click **Hardware → Resource Groups** to display the All Resource Groups page

Step 2. Select the resource group to be updated.

Step 3. Click **All Actions → Edit Properties** to display the Edit Group Properties dialog.



Step 4. Change the following information, as needed.
- Group name
- Description

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface

Chapter 6. Managing racks

You can use racks in Lenovo XClarity Administrator to group your managed devices to reflect the physical rack setup in your datacenter.

Before you begin

After moving a node from one chassis to another, wait 5 to 10 minutes before attempting to edit the racks in XClarity Administrator that contains the chassis.

When you move a device out of a rack, the rack name and lowest rack unit values are cleared in device inventory. The room and location values are not cleared.

About this task

This procedure describes how to create and populate a single rack with managed devices and fillers interactively.

If you must add many devices to racks, or edit many racks, consider using a spreadsheet to perform a bulk import or implementing a PowerShell script to automate the task. For more information about using the bulk-import, see Managing chassis and Managing servers. For information about PowerShell scripts, see PowerShell (LXCAPSTool) toolkit in the XClarity Administrator online documentation.

XClarity Administrator recognizes rack properties that are defined in a manageable device. When you manage that device, XClarity Administrator sets the system properties for that device and updates the rack view. If the rack does not exist in XClarity Administrator, a new rack is created and the device is added to the new rack.

Notes:

- System x3500 M5 servers, NeXtScale nx360 M5 servers, ThinkServer SD350 servers, and tower servers are not supported in rack view.
- System x3850 X5 scalable-complex systems, you must add each node (server) to the rack individually.
- Demo hardware is not persistent in rack views when XClarity Administrator is restarted.

Procedure

To create and populate racks, complete the following steps.

- Create and populate a single rack with managed devices.
  1. From the XClarity Administrator menu bar, click **Hardware → Racks**. The All Racks page is displayed.

     The All Racks page shows each rack as a thumbnail image with the name of the rack, the number of managed devices that are in the rack, and the status of the device with the highest severity.

     Notes: You can filter the racks by severity by clicking the following icons in the toolbar. You can also enter a rack name in the **Filter** field to further filter the racks that are displayed.
     - **Critical alerts** icon ( )
     - **Warning alerts** icon ( )
     - **Normal alerts** icon ( )

© Copyright Lenovo 2015, 2022

2. Click the **Create** icon ( ) to create an empty rack. The Create Empty Rack dialog is displayed.
3. Fill in the dialog with the rack name, height, location, and room.

   Notes:

   – Rack names do not need to be unique. You can create racks with the same name as long as the location or room or both are different.

   – The rack name can include only the upper and lower case letters, numbers, and the following special characters: period (.), dash (-), and underscore (_).

   – The location can be a maximum of 23 characters.
4. Click **Create**. A thumbnail image for the new rack is added to the All Racks page.
5. Double-click the thumbnail image for the rack. The rack-view page is displayed with an empty rack image and properties for that rack.

6. Click **Edit Rack** to display the Edit Rack page.

7. Add all appropriate managed devices and fillers to the graphical view:

   Note: Only managed devices that are in an Online state can be added to the rack.

   - Click the **Chassis** tab to view a list of managed chassis that have not been added to a rack. Drag and drop a managed chassis to the desired location in the rack to add the chassis to the rack.
   - Click the **Server Enclosures** tab to view a list of managed rack-servers and multi-node server enclosures that have not been added to a rack. Drag and drop a rack server or server enclosures into the rack at the desired location to add the rack server to the rack.
   - Click the **RackSwitch** tab to view a list of managed RackSwitch switches that have not been added to a rack. Drag and drop a RackSwitch switch into the rack at the desired location to add the switch to the rack.
   - Click the **Storage** tab to view a list of various storage devices. Drag and drop the appropriate storage device into the rack at the desired location to add the storage device to the rack.
   - Click the **Fillers** tab to view a list of various fillers. Drag and drop the appropriate filler into the rack at the desired location to add the filler to the rack.

     A *filler* is any device that is in the rack that is not managed by XClarity Administrator. The following fillers are available:
     - Generic fillers
     - Generic rack switches
     - Storage controllers and enclosures
     - Partner storage controllers and enclosures (such as IBM, NetApp, and EMC)

   - The location, room, rack, and lowest rack unit properties are updated for the device when you add or remove devices from a rack.
   - You can sort the list of devices on each tab by using the **View by** drop-down list. In addition, you can enter text (such as a name or IP address) in the **Filter** field to further filter the devices that are displayed.
   - You can remove managed devices and fillers from the rack by dragging and dropping the objects outside the rack.

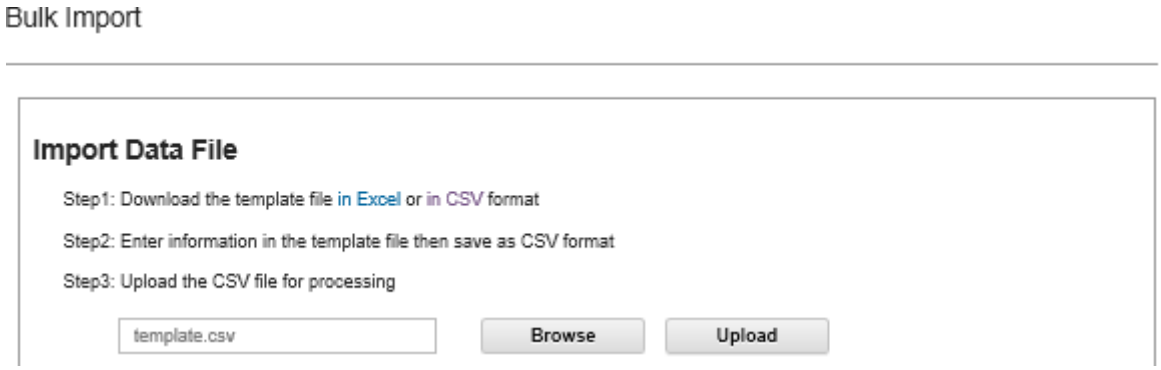
8. Click **Save** to save the rack configuration.

   The configuration process might take several minutes to complete. During configuration, the rack and location information is pushed to the CMM or baseboard management controller for the managed devices.

9. Customize the fillers that you added to the rack by clicking the filler and then clicking **Edit Properties**. In the Edit Properties dialog, you can specify a name, lowest rack unit (LRU), and a URL to use to launch the management user interface for that device.

   Tip: After the rack configuration is saved, you can launch the management user interface for a filler by clicking the filler in the rack and then clicking the **Launch URL** link.

- Create and populate racks using a bulk-import file.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Click **Bulk Import**. The Bulk Import wizard is displayed.

  3. Click the **in Excel** or **in CSV** link on the Import Data File page to download the template bulk-import file in Excel or CSV format.

     Important: The template file might change from one release to the next. Ensure that you always use the latest template.

  4. Fill in the data worksheet in the template file, and save the file in CSV format.

     Tip: The Excel template includes a **Data** worksheet and a **Readme** worksheet. Use the **Data** worksheet to fill in your device data. The **Readme** worksheet provides information about how to fill in each field on the **Data** worksheet (including which fields are required) and sample data.

     Important:

     – Devices are managed in the order that is listed in the bulk-import file.
     – XClarity Administrator uses rack-assignment information that is defined in the device configuration when the device is managed. If you change the rack assignment in XClarity Administrator, XClarity Administrator updates the device configuration. If you update the device configuration after the device is managed, the changes are reflected in XClarity Administrator.
     – It is recommended but not required to explicitly create a rack in the spreadsheet before assigning the rack to a device. If a rack is not explicitly defined and the rack does not already exist in XClarity Administrator, the rack-assignment information that is specified for a device is used to create the rack with a default height of 52U.

       If you want to use another height for the rack, you must explicitly define the rack in the spreadsheet before assigning it to a device.

     To define your racks in the bulk-import file, complete the following required columns.
     – (Columns A) Specify “rack” for the device type.
     – (Columns V) Specify the rack name.
     – (Column X) Specify rack height. The following rack heights are supported: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U, and 52U.

The following figure shows an example bulk-import file with racks defined.

A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

Note: You can use the same bulk-import file to manage devices and add those devices to a rack (see Managing systems in the Lenovo XClarity Administrator online documentation).

5. From the Bulk Import wizard, enter the name of the CSV file to upload file for processing. You can click **Browse** to help you find the file.
6. Click **Upload** to upload and validate the file.
7. Click **Next** to display the Input Summary page with a list of rack and other devices to be managed, and review the summary of racks and other devices that you want to manage.
8. Click **Next** to display the Device Credentials page. Click on each tab, and optionally specify global settings and credentials to use for all devices of a specific type. The devices that will use the global settings and credentials are listed on right side of each tab.
9. Click **Manage**. The Monitoring Results page is displayed with information about the management status of each device in the bulk-import file.

   A job is created for the management process. If you close the Bulk-Import wizard, the management process continues running in the background. You can monitor the status of the management process from the jobs log. For information about the jobs log, see “Monitoring jobs” on page 161.

After you finish

You can change the rack numbering order preference (see Setting inventory preferences).

Viewing the status of devices in a rack

For each rack, you can view the status of all managed devices in the rack.

Procedure

Complete the one or more of the following action to view the status of all devices in a rack.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of the all managed devices and other resources, including racks.

Step 2. From the XClarity Administrator menu bar, click **Hardware → Racks**. The Racks page is displayed.

The Racks page shows each rack as a thumbnail image with the name of the rack, the number of managed devices that are in the rack, and the status of the device with the highest severity.

Notes: You can sort the list by rack name, number of devices in the rack, or by severity to make it easier to find specific racks. Sorting is ordered from left to right, top to bottom. In addition, you can filter the racks by severity by clicking on the following icons in the toolbar or enter a rack name in the **Filter** field to further filter the racks that are displayed.

- **Critical alerts** icon ( )
- **Warning alerts** icon ( )
- **Normal alerts** icon ( )

Step 3. From the All Racks page, click the rack name or double-click a rack thumbnail to display the graphical view and properties for that rack.

The *rack view* is a graphical view of the front rack that shows each device in the rack, including chassis, rack servers, top-of-rack switches, and fillers. A status icon on each device indicates the current status of that device.

From this page, you can perform the following actions:

- Add or remove devices in the rack by clicking **Edit Rack**.

  Note: When you change the components in the rack, there might be a short delay before the information appears in the XClarity Administrator interface.
- Modify device and filter properties (including the name, location, and URL to launch the management web interface) by clicking the device or filler, and then clicking the **Edit Properties** in the device summary pane.
- View the management controller web interface for a device or filler by clicking the device or filler, and then clicking the **Launch URL** link in the device summary pane.

Step 4. Display a summary or detailed status for a device or component:

a. Click a device or component in the rack to display the status summary and properties and status for the device or component.

b. Double-click a device to display the device details page.

Procedure

You can change the rack numbering order preference (see Setting inventory preferences).

Removing a rack

You can remove a rack from Lenovo XClarity Administrator.

Procedure

Complete the following steps to remove a rack.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Racks**. The All Racks page is displayed.

The All Racks page shows each rack as a thumbnail image with the name of the rack, the number of managed devices that are in the rack, and the status of the device with the highest severity.

Notes: You can sort the list by rack name, number of devices in the rack, or by severity to make it easier to find specific racks. Sorting is ordered from left to right, top to bottom. In addition, you can filter the racks by severity by clicking on the following icons in the toolbar or enter a rack name in the **Filter** field to further filter the racks that are displayed.

- **Critical alerts** icon ( )
- **Warning alerts** icon ( )
- **Normal alerts** icon ( )

Step 2. Select the thumbnail for the rack to be removed.

Step 3. Click the **Remove** icon ( ).

Step 4. Click **Remove**.

Results

The thumbnail for the rack is removed from the All Racks page, and all devices that were in the rack are now available for inclusion in other rack on the Edit Racks page.

Chapter 7. Managing chassis

Lenovo XClarity Administrator can manage several types of systems, including the Flex System chassis.

Learn more: XClarity Administrator: Discovery

Before you begin

Note: Chassis components (such as CMMs, Flex compute nodes, and Flex switches) are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed chassis components separate from the chassis.

Before managing chassis, ensure that the following conditions are met:

- Review the management considerations before managing a device. For information, see Management considerations in the XClarity Administrator online documentation.
- Certain ports must be available to communicate with the CMM for the chassis being managed. Ensure that these ports are available before you attempt to manage a chassis. For more information about ports, see Port availability in the XClarity Administrator online documentation.
- Ensure that the minimum required firmware is installed on each chassis that you want to manage using XClarity Administrator. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.
- Ensure that the **Number of simultaneous active sessions for LDAP users** setting in the CMM is set to 0 (zero) for the chassis. You can verify this setting from the CMM web interface by clicking **Mgmt Module Management → User Accounts**, click **Global Login Settings**, and then click the **General** tab.
- Ensure that there are at least three TCP command-mode sessions set for out-of-band communication with the CMM. For information about setting the number of sessions, see tcpcmdmode command in the CMM online documentation.
- To discover a chassis that is on a *different* subnet from XClarity Administrator, ensure that one of the following conditions are met:
  - Ensure that you enable multicast SLP forwarding on the top-of-rack switches, as well as the routers in your environment. See the documentation that was provided with your specific switch or router to determine whether multicast SLP forwarding is enabled and to find procedures to enable it if it is disabled.
  - If SLP is disabled on the endpoint or on the network, you can use DNS discovery method instead by manually adding a service record (SRV record) to your domain name server (DNS), for XClarity Administrator for example.

    ```
    _lxca._tcp.labs.lenovo.com      service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```

    Then, enable DNS discovery on the CMM from the management web interface, by clicking **Mgt Module Management → Network Protocol**, clicking the **DNS** tab, and selecting **Use DNS to discover Lenovo XClarity Administrator**.

    Notes:

    - The CMM must be running a firmware level dated May 2017 to support automatic discovery using DNS.
    - If there are multiple XClarity Administrator instances in your environment, the chassis is discovered only by the instance that is the first to respond to the discovery request. The chassis is not discovered by all instances.

© Copyright Lenovo 2015, 2022

Consider implementing either IPv4 *or* IPv6 addresses for all CMMs and Flex switches that are managed by XClarity Administrator. If you implement IPv4 for some CMMs and Flex switches and IPv6 for others, some events might not be received in the audit log (or as audit traps).

Attention: If you intend to manage CMMs that are running a firmware level of Flex stack release 1.3.2.1 2PET12K through 2PET12Q, that have been running more than three weeks, and that are in a dual-CMM configuration, you must virtually reseat the CMMs before updating firmware using XClarity Administrator.

Important: If you intend to use other management software in addition to Lenovo XClarity Administrator to monitor your chassis, and if that management software uses SNMPv3 communication, you must first create a local CMM user ID that is configured with the appropriate SNMPv3 information and then log in to the CMM using that user ID and change the password. For more information, see Management considerations in the XClarity Administrator online documentation.

About this task

XClarity Administrator can automatically discover chassis in your environment by probing for manageable systems that are on the same IP subnet as XClarity Administrator. To discover chassis that are in other subnets, specify an IP address or range of IP addresses, or import information from a spreadsheet.

After the chassis are managed by XClarity Administrator, XClarity Administrator polls each managed chassis periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed chassis and perform management action (such as configuring system information, network setting, and failover). For chassis that are in protected mode, management actions are disabled.

Chassis are managed using *XClarity Administrator managed authentication*.

By default, devices are managed using XClarity Administrator managed authentication to log in to the devices. When managing rack servers and Lenovo chassis, you can choose to use local authentication or managed authentication to log in to the devices.

- When *local authentication* is used for rack servers, Lenovo chassis, and Lenovo rack switches, XClarity Administrator uses a stored credential to authenticate to the device. The *stored credential* can be an active user account on the device or a user account in an Active Directory server.

  You must create a stored credential in XClarity Administrator that matches an active user account on the device or a user account in an Active Directory server before managing the device using local authentication (see Managing stored credentials in the XClarity Administrator online documentation).

  Notes:

  – RackSwitch devices support only stored credentials for authentication. XClarity Administrator user credentials are not supported.
- Using *managed authentication* allows you to manage and monitor multiple devices using credentials in the XClarity Administrator authentication server instead of local credentials. When managed authentication is used for a device (other than ThinkServer servers, System x M4 servers, and switches), XClarity Administrator configures the device and its installed components to use the XClarity Administrator authentication server for centralized management.

  – When managed authentication is enabled, you can manage devices using either manually-entered or stored credentials (see Managing user accounts and in the XClarity Administrator online documentation).

    The stored credential is used only until XClarity Administrator configures the LDAP settings on the device. After that, any change to the stored credential has no impact the management or monitoring of that device.

Note: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.

- If a local or external LDAP server is used as the XClarity Administrator authentication server, user accounts that are defined in the authentication server are used to log in to XClarity Administrator, CMMs and baseboard management controllers in the XClarity Administrator domain. Local CMM and management controller user accounts are disabled.
- If an SAML 2.0 identity provider is used as the XClarity Administrator authentication server, SAML accounts are not accessible to managed devices. However, when using an SAML identity provider and an LDAP server together, if the identity provider uses accounts that exist in the LDAP server, LDAP user accounts can be used to log into the managed devices while the more advanced authentication methods that are provided by SAML 2.0 (such as multifactor authentication and single sign-on) can be used to log into XClarity Administrator.
- Single sign-on allows a user that is already logged in to XClarity Administrator to automatically log in to the baseboard management control (XCC). Single sign-on is enabled by default when a ThinkSystem or ThinkAgile server is brought into management by XClarity Administrator (unless the server is managed with CyberArk passwords). You can configure the global setting to enable or disable single sign-on for all managed ThinkSystem and ThinkAgile servers. Enabling single sign-on for a specific ThinkSystem and ThinkAgile server overrides the global setting for all ThinkSystem and ThinkAgile servers (see Managing servers).

  Note: Single sign-on is disabled automatically when using the CyberArk identity-management system for authentication.
- When managed authentication is enabled for ThinkSystem SR635 and SR655 servers:
  - Baseboard management-controller firmware supports up to five LDAP user roles. XClarity Administrator adds these LDAP user roles to the servers during management: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin**, and **lxc-os-admin**.

    Users must be assigned to at least one of the specified LDAP user roles to communicate with ThinkSystem SR635 and SR655 servers.
  - Management-controller firmware does not support LDAP users with the same username as local user of the sever.
- For ThinkServer and System x M4 servers, the XClarity Administrator authentication server is not used. Instead, an IPMI account is created on the device with the prefix “LXCA_” followed by a random string. (The existing local IPMI user accounts are not disabled.) When you unmanage a ThinkServer server, the “LXCA_” user account is disabled, and the prefix “LXCA_” is replaced with the prefix “DISABLED_”. To determine whether a ThinkServer server is managed by another instance, XClarity Administrator checks for IPMI accounts with the prefix “LXCA_”. If you choose to force management of a managed ThinkServer server, all the IPMI accounts on the device with the “LXCA_” prefix are disabled and renamed. Consider manually clearing IPMI accounts that are no longer used.

  In XClarity Administrator v2.4 and later, if you use manually-entered credentials, XClarity Administrator automatically creates a stored credential and uses that stored credential to manage the device.

  Notes: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.
  - Each time you manage a device using manually-entered credentials, a new stored credential is created for that device, even if another stored credential was created for that device during a previous management process.
  - When you unmanage a device, XClarity Administrator does not delete stored credentials there were automatically created for that device during the management process.

A device can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device on the initial XClarity Administrator, and then manage it with the new XClarity Administrator. If an error occurs during the unmanagement process, you can select the **Force management** option during management on the new XClarity Administrator.

Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a device is already managed by another manager until after it attempts to manage the device.

During the management process, XClarity Administrator performs the following actions:

- Logs in to the chassis using the provided credentials.
- Collects inventory for all components in each chassis, such as the CMM, compute nodes, storage devices, and Flex switches.

  Note: Some inventory data is collected after the management process completes. The chassis is in the Pending status until all inventory data is collected. You cannot perform certain tasks on a managed device (such as deploying a server pattern) until all inventory data is collected for that device and the chassis is no longer in the Pending state.
- Configures the settings for the NTP server so that all managed devices use the NTP server from XClarity Administrator.
- Assigns the last-edited firmware-compliance policy to the chassis.
- For Lenovo Flex devices, optionally configures the devices firewall rules so that incoming requests are accepted from only XClarity Administrator.
- Exchanges security certificates with the CMM, copying the CMM security certificate into the XClarity Administrator trust store and sending the XClarity Administrator CA security certificate to the CMM. The CMM loads the certificate into the CMM trust store and distributes it to the compute-node service processors for inclusion in their trust stores.
- Configures managed authentication. The settings for the CMM LDAP client are changed to use XClarity Administrator as the authentication server, and the Global Login Settings in the CMM are changed to **External Authentication Server Only**. For more information about managed authentication, see Managing the authentication server.
- Creates the recovery user account (`RECOVERY_ID`). For more information about the `RECOVERY_ID` account, see Managing the authentication server.

Attention: When managing a chassis, the XClarity Administrator changes the maximum number of simultaneous Secure TCP Command Mode connections to 15 and sets the maximum number of simultaneous Legacy TCP Command Mode connections to 0. This overrides settings that you might have already set on the CMM.

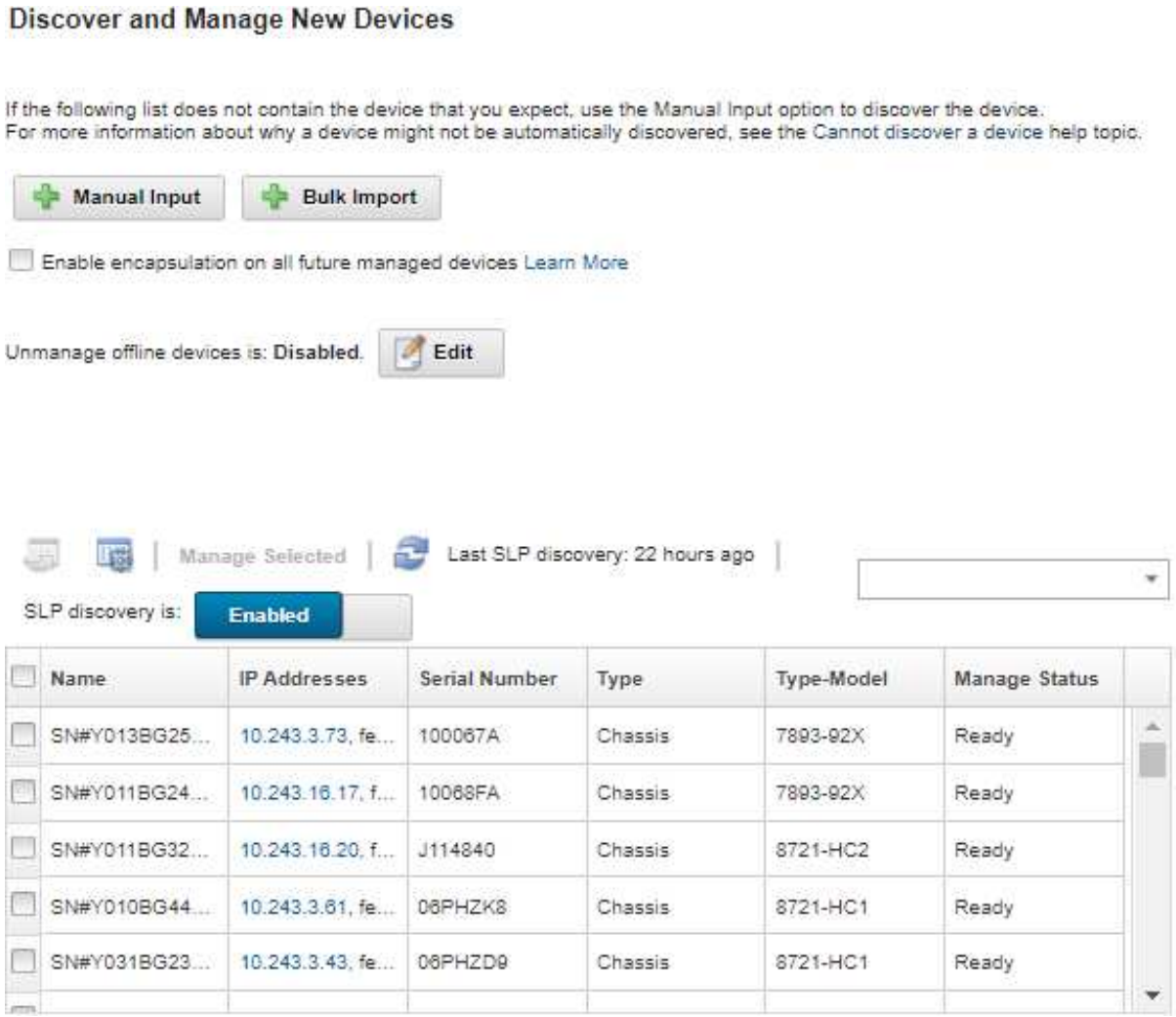
Note: XClarity Administrator does not modify the security settings or cryptographic settings (cryptographic mode and the mode used for secure communications) during the management process. You can modify the cryptographic settings after the chassis is managed (see Configuring cryptography settings).

Procedure

Complete one of the following procedures to discover and manage your chassis using XClarity Administrator.

- Discover and manage a large number of chassis and other devices using a bulk-import file (see Managing systems in the Lenovo XClarity Administrator online documentation).
- Discover and manage chassis that are on the same IP subnet as XClarity Administrator.

1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage New Devices page is displayed.



   You can sort the table columns to make it easier to find the chassis that you want to manage. In addition, you can enter text (such as a system name or IP address) in the **Filter** field to further filter the chassis that are displayed. You can change the columns that are displayed and the default sort order by clicking the **Customize Columns** icon ( ).

2. Click the **Refresh** icon ( ) to discover all manageable devices in the XClarity Administrator domain. Discovery might take several minutes.
3. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

   Encapsulation can be enabled or disabled on specific devices after they are managed.

   Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
4. Select one or more chassis that you want to manage.

5. Click **Manage Selected**.
6. Choose to use XClarity Administrator managed authentication or local authentication for this device. Managed authentication is selected by default. To use local authentication, clear **Managed Authentication**.

   Note: Managed and local authentication are not supported for ThinkServer and System x M4 servers.
7. Choose the type of credentials to use for the device and specify the appropriate credentials:
   - **Use manually entered credentials**
     - Specify the local user ID and password with **lxc-supervisor** authority for authenticating to the CMM.
     - (Optional) Specify a new password for the CMM user account if the password is currently expired on the device.
   - **Use stored credentials**

     Select the stored credential with **lxc-supervisor** authority to use for this managed device. You can add stored credentials by clicking **Manage Stored Credentials**.

     Note: If you choose to use local authentication, you must select a stored credential to manage the device.

   Tip: It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

   For more information about normal and stored credentials, see Managing user accounts and Managing stored credentials.
8. Specify the recovery password if managed authentication is selected.

   A recovery account (`RECOVERY_ID`) is created on the CMM, and all local user accounts are disabled. If there is a problem with XClarity Administrator, and it stops working for some reason, you *cannot* log in to the CMM using normal user accounts. However, you can log in using the `RECOVERY_ID` account.

   Note:
   - The recovery password is required if you choose to use managed authentication and is not allowed if you if you choose to use local authentication.
   - You can choose to use a local recovery account or stored recovery credentials. In either case, the user name is always `RECOVERY_ID`.
   - Ensure that the password follows the security and password policies for the device. Security and password policies might vary.
   - Ensure that you record the recovery password for future use.

   For more information about the recovery ID, see Managing the authentication server.
9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:
   - You can select from a list of role groups that are assigned to the current user.
   - If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.
10. Click **Manage**.

A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.

When the process is complete, the dialog displays the number of devices in the chassis and the chassis status.

Note: Some inventory data is collected after the management process completes. The chassis is in the Pending status until all inventory data is collected. You cannot perform certain tasks on a managed device (such as deploying a server pattern) until all inventory data is collected for that device and the chassis is no longer in the Pending state.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    – If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    – If the managing XClarity Administrator was taken down before the devices were unmanaged.

    – If the devices were not unmanaged successfully.

    Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

12. If this is a new chassis, click **Continue to Chassis Configuration** to validate and change management network settings for the entire chassis (including compute nodes and Flex switches) and to configure the compute node information, local storage, I/O adapters, boot targets, and firmware settings by creating and deploying server patterns. For more information, see Modifying the management-IP settings for a chassis and Configuring servers using configuration patterns.

- Discover and manage chassis that are not on the same IP subnet as XClarity Administrator by manually specifying IP addresses.

  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

     Encapsulation can be enabled or disabled on specific devices after they are managed.

     Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
  3. Select **Manual Input**.
  4. Specify the network addresses of the chassis that you want to manage:

     – Click **Single System**, and enter a single IP address domain name, or fully-qualified domain name (FQDN).

Note: To specify an FQDN, ensure that a valid domain name is specified on Network Access page (see Configuring network access).

- Click **Multiple Systems**, and enter a range of IP addresses. To add another range, click the **Add** icon (). To remove a range, click the **Remove** icon ().

5. Click **OK**.
6. Choose to use XClarity Administrator managed authentication or local authentication for this device. Managed authentication is selected by default. To use local authentication, clear **Managed Authentication**.

   Note: Managed and local authentication are not supported for ThinkServer and System x M4 servers.
7. Choose the type of credentials to use for the device and specify the appropriate credentials:
   - **Use manually entered credentials**
     - Specify the local user ID and password with **lxc-supervisor** authority for authenticating to the CMM.
     - (Optional) Specify a new password for the CMM user account if the password is currently expired on the device.
   - **Use stored credentials**

     Select the stored credential with **lxc-supervisor** authority to use for this managed device. You can add stored credentials by clicking **Manage Stored Credentials**.

     Note: If you choose to use local authentication, you must select a stored credential to manage the device.

   Tip: It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

   For more information about normal and stored credentials, see Managing user accounts and Managing stored credentials.
8. Specify the recovery password if managed authentication is selected.

   A recovery account (`RECOVERY_ID`) is created on the CMM, and all local user accounts are disabled. If there is a problem with XClarity Administrator, and it stops working for some reason, you *cannot* log in to the CMM using normal user accounts. However, you can log in using the `RECOVERY_ID` account.

   Note:
   - The recovery password is required if you choose to use managed authentication and is not allowed if you if you choose to use local authentication.
   - You can choose to use a local recovery account or stored recovery credentials. In either case, the user name is always `RECOVERY_ID`.
   - Ensure that the password follows the security and password policies for the device. Security and password policies might vary.
   - Ensure that you record the recovery password for future use.

   For more information about the recovery ID, see Managing the authentication server.
9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:
   - You can select from a list of role groups that are assigned to the current user.

– If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. Monitor the progress to ensure that the process completes successfully.

    When the process is complete, the dialog is displayed the number of devices in the chassis and the chassis status.

    Note: Some inventory data is collected after the management process completes. The chassis is in the Pending status until all inventory data is collected. You cannot perform certain tasks on a managed device (such as deploying a server pattern) until all inventory data is collected for that device and the chassis is no longer in the Pending state.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    – If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    – If the managing XClarity Administrator was taken down before the devices were unmanaged.

    – If the devices were not unmanaged successfully.

    Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

12. If this is a new chassis, click **Continue to Chassis Configuration** to validate and change management network settings for the entire chassis (including compute nodes and Flex switches) and to configure the compute node information, local storage, I/O adapters, boot targets, and firmware settings by creating and deploying server patterns. For more information, see Modifying the management-IP settings for a chassis and Configuring servers using configuration patterns.

After you finish

- Discover and manage additional devices.
- Deploy operating-system images to the servers that do not already have an operating system installed. For more information, see Installing operating systems on bare-metal servers.
- Update firmware on devices that are not in compliance with current policies (Updating firmware on managed devices).
- Add the newly managed devices to the appropriate rack to reflect the physical environment (see Managing racks).
- Monitor hardware status and details (see Viewing the status of a managed server).
- Monitor events and alerts (see Working with events and Working with alerts).

Viewing the status of a managed chassis

You can view a summary and detailed status for the managed chassis and their installed components from Lenovo XClarity Administrator.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

The following status icons are used to indicate the overall health of the device. If the certificates do not match, "(Untrusted)" is appended to the status of each applicable device, for example Warning (Untrusted). If there is a connectivity issue or a connection to the device is not trusted, "(Connectivity)" is appended to the status of each applicable device, for example Warning (Connectivity).

- ( ) Critical
- ( ) Warning
- ( ) Pending
- ( ) Informational
- ( ) Normal
- ( ) Offline
- ( ) Unknown

Procedure

Complete the following steps to view the status for a managed chassis.

- View detailed information about the chassis by clicking the **Details** link or by clicking **Actions → Views → Details**.
- Launch the CMM web interface for the chassis by clicking the **IP address** link (see Launching the CMM web interface for a chassis).
- Modify information (such as support contact, location, and description) by clicking **Actions → Inventory → Edit Properties**.
- Modify the management IP settings for the entire chassis, including compute nodes and Flex switches, by clicking **Actions → Inventory → Edit Management IP addresses**.
- Export detailed information about one or more chassis to a single CSV file by selecting the chassis and clicking **Actions → Inventory → Export Inventory**.

  Note: You can export inventory data for a maximum of 60 devices at one time.

  Tip: When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Resolve issues that might arise between the Lenovo XClarity Administrator security certificate and the security certificate of the CMM in the chassis by selecting a chassis and clicking **Actions → Security → Resolve Untrusted Certificates**.

Viewing the details of a managed chassis

You can view the detailed information about the managed chassis from Lenovo XClarity Administrator, including the firmware levels, IP addresses, and universally unique identifier (UUID).

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

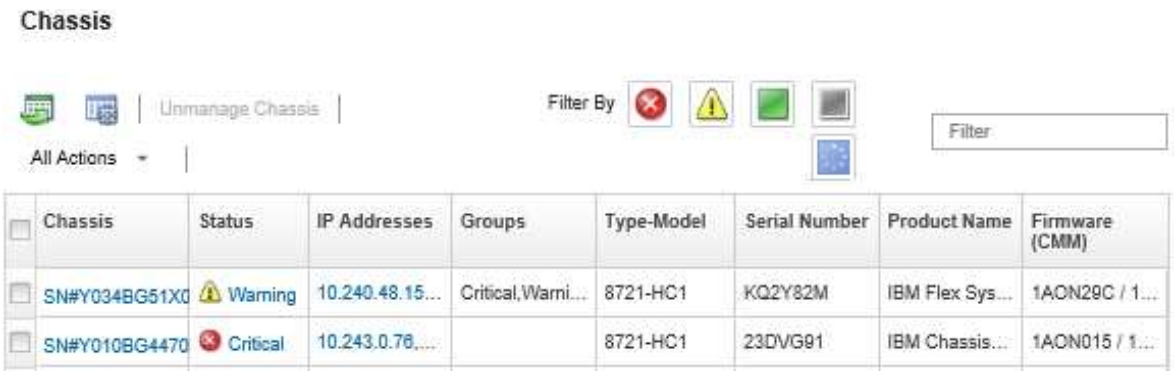
The system-level air temperature is measured by a physical sensor at the front of the server. This temperature represents inlet air temperature for the server. Note that the air temperature that is reported by XClarity Administrator and the CMM might differ if the temperature is captured at different points in time.

Procedure

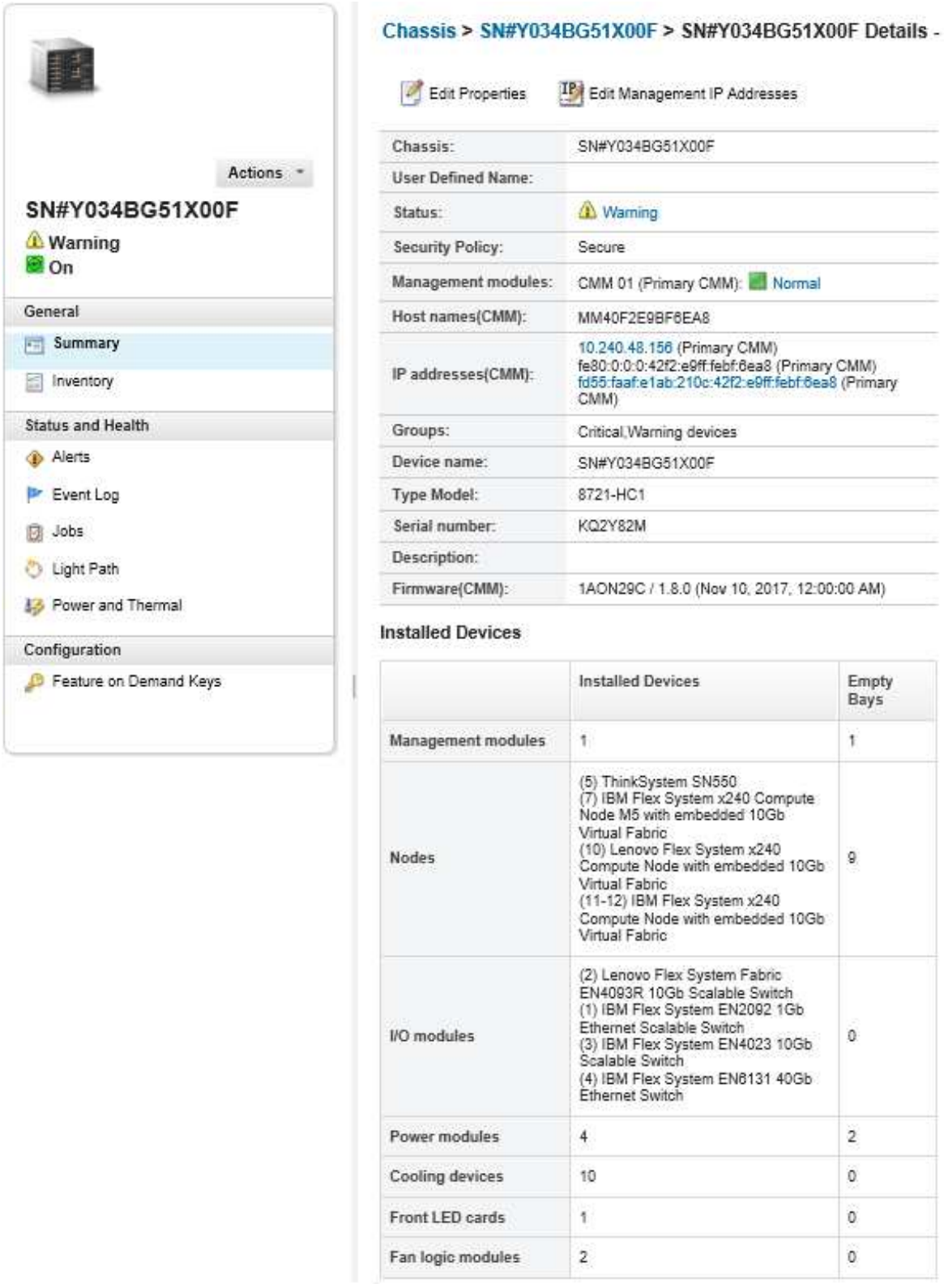
Complete the following steps to view the details for a managed chassis.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Chassis**. The Chassis page is displayed with a tabular view of all managed chassis.

You can sort the table columns to make it easier to find the chassis that you want to manage. In addition, you can enter text (such as a chassis name or IP address) in the **Filter** field to further filter the chassis that are displayed.



Step 2. Click the chassis name in the **Chassis** column. The status summary page for that chassis is displayed, showing the chassis properties and components that are installed in the chassis.



Step 3. Complete one or more of the following actions:

- Click **Summary** to view a summary of the chassis, including system information and installed components (see Viewing the status of a managed chassis).
- Click **Inventory Details** to view details about the chassis components, including:

  - Firmware levels for all components in the chassis.
  - Details of the CMM, such as the hostname, IPv4 address, IPv6 address, and MAC addresses.
  - Asset details of the chassis and CMM installed in the chassis, including name, universally unique identifier (UUID), and location.
- Click **Alerts** to display the list of current alerts for this chassis (see Working with alerts).
- Click **Event Log** to display the list of events for this chassis (see Monitoring events in the event log).
- Click **Jobs** to display a list of jobs associated with the chassis (see Monitoring jobs).
- Click **Light Path** to display the current status of the chassis LEDs, including Location, Fault, and Information. This is the equivalent of looking at the front panel of the chassis.
- Click **Power and Thermal** to display details about power and air flow.

  Tip: Use the refresh button on your web browser to collect the latest power and thermal data. Collecting data might take several minutes.
- Click **Feature on Demand Keys** to access information that is needed to order a Feature on Demand key and other agentless information (see Viewing Features on Demand keys).

After you finish

In addition to displaying summary and detailed information about a chassis, you can perform the following actions:

- View a chassis in graphical rack or chassis view by clicking **Actions → Views → Show in Rack View** or **Actions → Views → Show in Chassis View**.
- Launch the CMM web interface by clicking the **IP address** link (see Launching the CMM web interface for a chassis).
- Modify information (such as support contact, location and description) by clicking **Edit Properties** (see Modifying the system properties for a chassis).
- Modify the management IP settings for the entire chassis, including compute nodes and Flex switches, by clicking **All Actions → Inventory → Edit Management IP addresses** (see Modifying the management-IP settings for a chassis).
- Export detailed information about the chassis to a CSV file clicking the **Actions → Inventory → Export Inventory**.

  Notes:

  - For more information about inventory data in the CSV file, see the GET /chassis/*<UUID_list>* in the XClarity Administrator online documentation.
  - When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Unmanage a chassis (see Unmanaging a chassis).
- Enable or disable firewall rule changes on a chassis that limit incoming requests only from XClarity Administrator by selecting the chassis and clicking **Actions → Security → Enable Encapsulation** or **Actions → Security → Disable Encapsulation**.

  The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

  The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.

- Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the CMM in the chassis by selecting a chassis and clicking **Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).

Backing up and restoring CMM-configuration data

Lenovo XClarity Administrator does not include built-in backup functions for CMM-configuration data. Instead, use the backup functions that are available for your managed CMM.

Use the management web interface or the command-line interface (CLI) to back up and restore the CMM.

- Back up CMM configuration data
  - From the management web interface, click **Mgt Module Management → Configuration → Backup Configuration**. For more information, see Saving a CMM configuration through the web interface in the Flex Systems online documentation.
  - From the CLI, use the **write** command. For more information, see CMM write command in the Flex Systems online documentation
- Restore CMM configuration data
  - From the management web interface, click **Mgt Module Management → Configuration → Restore Configuration from File**. For more information, see Restoring a CMM configuration through the web interface in the Flex Systems online documentation.
  - From the CLI, use the **read** command. For more information, see CMM read command in the Flex Systems online documentation.

Note: Tip: You can find additional information about backing up and restoring chassis components in the PureFlex and Flex System Backup and Restore Best Practices Guide.

Launching the CMM web interface for a chassis

You can launch the CMM web interface for a specific chassis from Lenovo XClarity Administrator.

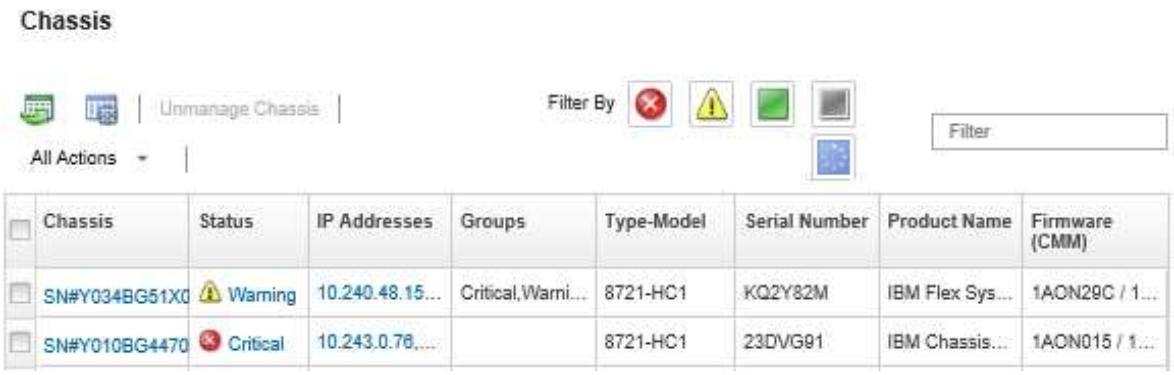
Procedure

Complete the following steps to launch a CMM web interface.

Note: Launching this CMM web interface from XClarity Administrator using the Safari web browser is not supported.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Chassis** to display the Chassis page.

You can sort the table columns to make it easier to find the chassis that you want to manage. In addition, you can enter text (such as a chassis name or IP address) in the **Filter** field to further filter the chassis that are displayed.



Step 2. Click the link for the chassis in the **Chassis** column. The status summary page for that chassis is displayed.

Step 3. Click **All Actions → Launch → Management Web Interface**. The CMM web interface is started.

Tip: You can also click the IP address to launch the CMM.

Step 4. Log on to the CMM web interface using your XClarity Administrator user credentials.

Modifying the system properties for a chassis

You can modify the system properties for a specific chassis.

Procedure

Complete the following steps to modify the system properties.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Chassis** to display the Chassis page.

Step 2. Select the chassis to be updated.

Step 3. Click **All Actions → Inventory → Edit Properties** to display the Edit dialog.

Step 4. Change the following information, as needed.
- Server name
- Support contact
- Description

Note: The location, room, rack, and lowest rack unit properties are updated by XClarity Administrator when you add or remove devices from a rack in the web interface (see Managing racks).

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface.

Modifying the management-IP settings for a chassis

You can modify the management-IP settings for the entire chassis, including compute nodes, storage devices, and Flex switches.

Procedure

Complete the following steps to modify the management-IP settings.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Chassis** to display the Chassis page.

Step 2. Select the chassis.

Step 3. Click **All Actions → Inventory → Edit Management IP Addresses** to display the Chassis and Components IP Settings page.

Step 4. Change the following global settings, as needed.

- Choose to enable or disable IPv4 addresses.

  If you enable IPv4 addresses, specify the following settings. IPv4 global settings are applied to a component when its IPv4 address is updated.
  – (Optional) Choose to obtain IP addresses using statically assigned IP addresses.
  – Specify the subnet mask and gateway address.
- Specify the following settings for IPv6 addresses. IPv6 global settings are applied to a component when its IPv6 address is updated.
  – (Optional) Choose to obtain IP addresses using statically assigned IP addresses.

    If static IP addresses are used, you can also choose to use stateless IP address auto configuration and stateful IP address configuration.
  – Specify the prefix length and gateway address.
- Choose to enable or disable DNS servers.

  If you enable DNS servers:
  – Choose the DNS server search preference.
  – Enter the IP addresses to use for the DNS search order.
  – Enter the domain name.

Step 5. Change the following CMM IP settings.

- Enter the hostname and IP address for the CMM.
- Click **Auto-Generate IP addresses** to create IP addresses for the compute nodes, storage devices, and Flex switches using the CMM IP address as the starting point.

Step 6. Enter the hostname and IP addresses for each compute node in the chassis

Step 7. Enter the hostname and IP addresses for each storage device in the chassis.

Step 8. Enter the IP addresses for each Flex switch in the chassis.

Step 9. Click **Save**. A dialog box displays with a summary of the network settings.

Step 10. Click **Apply**.

All existing components in the chassis are updated to the specified global settings. When the update is complete, the dialog displays the settings that were changed.

Note: When you change this information, there might be a short delay before the information appears in the Lenovo XClarity Administrator interface.

Step 11. Click **Close**.

Configuring CMM failover

When you install a second CMM in a chassis, the second CMM is automatically configured as a standby CMM by default. If the primary CMM fails, the IP address for the standby CMM changes to the same IP address that was used for the primary CMM, and standby CMM takes over the management of the chassis. However, you can perform more advanced failover configuration from the management controller web interface for the chassis.

About this task

For example, you can choose to:

- Disable the network interface for the standby CMM to prevent failover.
- Enable the network interface for the standby CMM, and allow IP addresses to swap between the two CMMs during failover.
- Enable the network interface for the standby CMM, and prevent the IP addresses from swapping between the two CMMs during failover.

For more information about CMM advanced failover capabilities, see the advfailover command in the CMM online documentation.

Procedure

To enable swappable IP address for the primary and standby CMMs, complete the following steps.

Step 1. From the management controller web interface for the chassis, click **Mgt Module Management** → **Network** → **Ethernet** to display the Ethernet Configuration page.

Step 2. Select either **IPv4** and **IPv6** for your system.

Step 3. Under **Configure IP address**, select the option to use a static IP address. Repeat for the other protocol.

Step 4. Click **Mgt Module Management** → **Properties** → **Advanced Failover**, and enable the advance failover option.

Step 5. Select **Swap Management Module IP address**.

Step 6. Perform test scenarios to verify that the failover works correctly and that Lenovo XClarity Administrator can connect to primary and backup CMMs.

Restarting a CMM

You can restart a Chassis Management Module (CMM) from Lenovo XClarity Administrator.

Procedure

Complete the following procedure to restart a chassis.

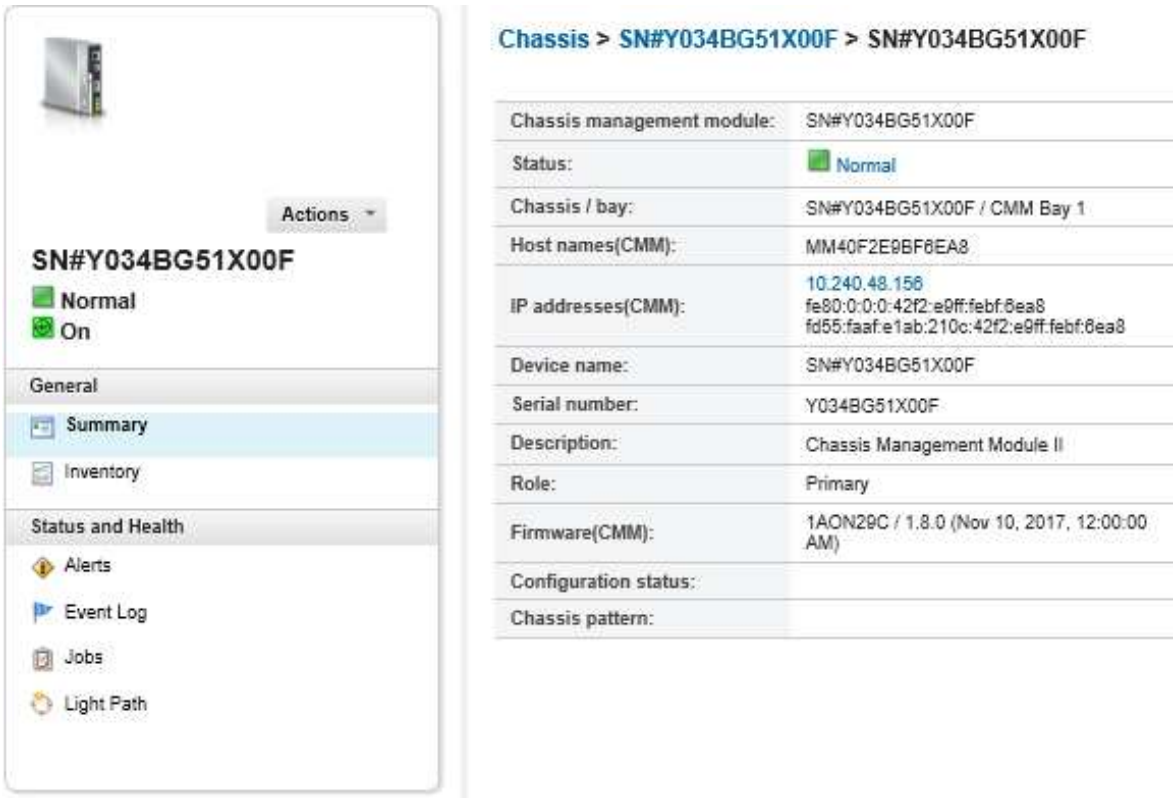
Note: When the CMM is restarted, all existing network connections to the CMM are lost temporarily.

Step 1. From the XClarity Administrator menu, click **Hardware** → **Chassis**. The Chassis page is displayed with a tabular view of all managed chassis.

Step 2. Click the chassis name in the **Chassis** column to display the graphical chassis view.

Step 3. Click the CMM graphic to display the in the CMM Summary page.

Tip: You can also click **Table View**, and then click the CMM name in the **Name** column to display the CMM Summary page.



Step 4. Click **Actions → Power Actions → Restart**.

Step 5. Click **Restart Immediately**.

This operation might take a few minutes to complete, and you might need to refresh the page to see the results.

Virtually reseating a CMM

You can simulate removing and reinserting a Chassis Management Module (CMM) in a chassis,

About this task

During the virtual reseat, all existing network connections to the CMM are lost, and the power state of the CMM changes.

Attention: Before performing a virtual reseat, ensure that you have saved all user data on the CMM.

Procedure

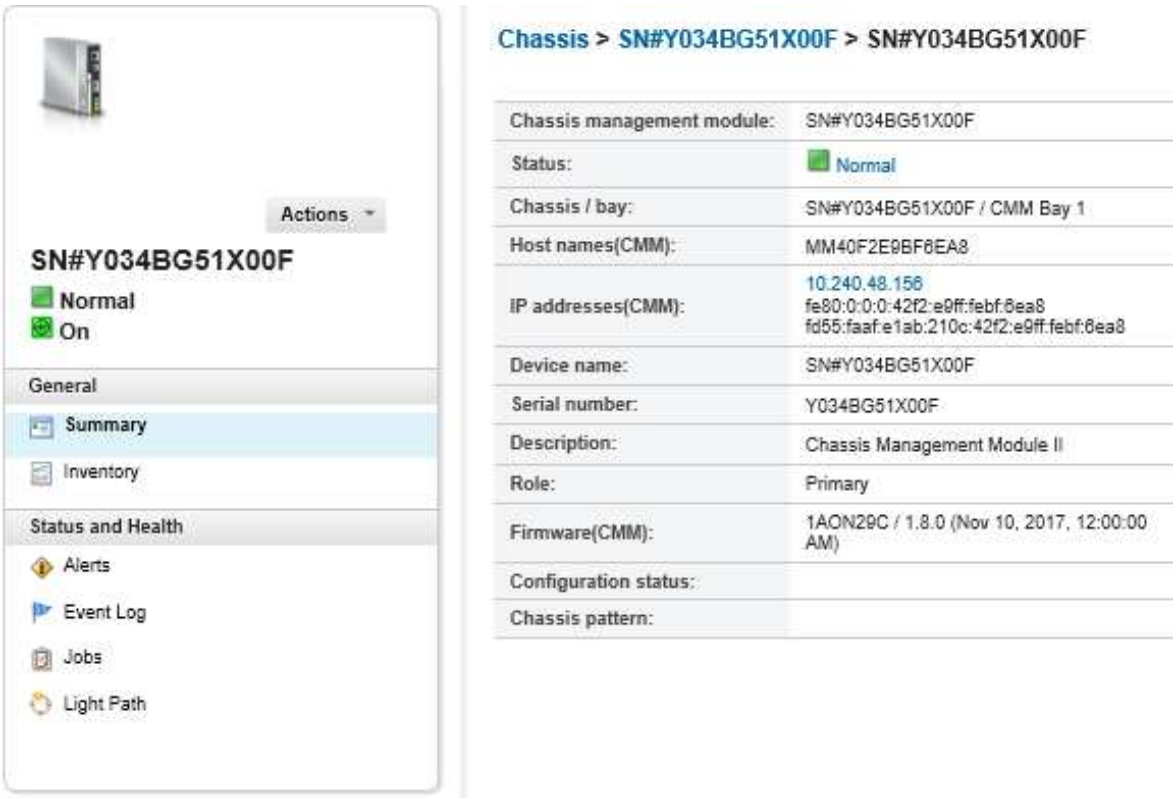
Perform the following steps to virtually reseat a CMM.

Step 1. From the Lenovo XClarity Administrator menu, click **Hardware → Chassis**. The Chassis page is displayed with a tabular view of all managed chassis.

Step 2. Click the chassis name in the **Chassis** column to display the graphical chassis view.

Step 3. Click the CMM graphic to display the in the CMM Summary page.

Tip: You can also click **Table View**, and then click the CMM name in the **Name** column to display the CMM Summary page.



Step 4. Click **Actions → Service → Virtual Reseat**.

Step 5. Click **Virtual Reseat**.

Resolving expired or invalid stored credentials for a chassis

When a stored credential becomes expired or inoperable on a device, the status for that device is shown as “Offline.”

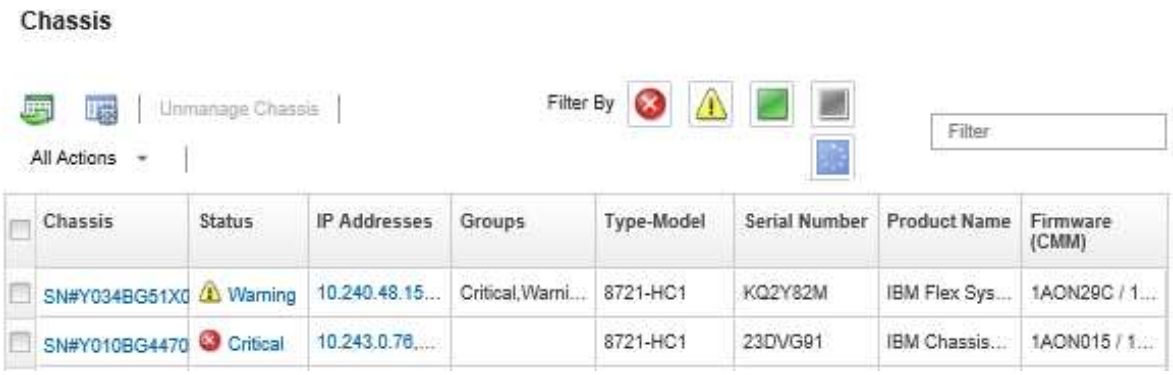
Procedure

To resolve an expired or invalid stored credential for a chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Chassis**. The Chassis page is displayed with a tabular view of all managed chassis.

Step 2. Click the **Power** column header to group all offline chassis at the top of the table.

You can sort the table columns to make it easier to find the chassis that you want to manage. In addition, you can enter text (such as a chassis name or IP address) in the **Filter** field to further filter the chassis that are displayed.



Step 3. Select the chassis to be resolved.

Step 4. Click **All Actions → Security → Edit Stored Credentials**.

Step 5. Change the password for the stored credential or select another stored credential to use for the managed device.

Note: If you managed more than one device using the same stored credentials and you change the password for the stored credentials, that password change affects all devices that are currently using the stored credentials.

Recovering management with a CMM after a management server failure

If a chassis is being managed by Lenovo XClarity Administrator, and XClarity Administrator fails, you can restore the management functions and the local user accounts for a CMM until the management node is restored or replaced.

Procedure

Complete one of the following procedures to restore management on a CMM.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, manage the device again using the RECOVERY_ID account and password and the **Force management** option (see Managing chassis).
- Reset the CMM to factory defaults by pressing the pinhole button on the CMM using a paperclip for at least 10 seconds. For more information about resetting the CMM, including important notices, see CMM Reset in the Flex Systems online documentation.
- Reset the CMM configuration using the following steps:
  1. Through an SSH session, open a management command-line interface for the chassis, and log in with the `RECOVERY_ID` account.

     Note: The password for the `RECOVERY_ID` account was set when you selected the chassis for management on the Management Domain page. For more information about central account management, see Managing chassis.

     If this is the first time that you have used the `RECOVERY_ID` account to log in to the CMM, you must change the password.
  2. If you are prompted, type the new password for the `RECOVERY_ID` account.
  3. Restore the CMM configuration by performing one of the following steps:
     - If you are running CMM firmware release June 2015 or later, run the following command:
       `read -f unmanage -T mm[p]`
       For more information, see the read command in the CMM online documentation.

– If you are running CMM firmware release earlier than June 2015, run the following commands in the order shown:
  a. **env -T mm[p]**
  b. **sslcfg -client disabled -tc1 remove**
  c. **accseccfg -am local**
  d. **ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""**
  e. **ntp -en disabled -i 0.0.0.0 -v3en disabled**
  f. **cimsub -clear all**
  g. **fsmcm -off**

     The **fsmcm** command disables XClarity Administrator user-account management and allows you to use local CMM user accounts to authenticate to the CMM and any management processor that is installed in the chassis.

     After you run the **fsmcm -off** command, the `RECOVERY_ID` account is removed from the CMM user registry. When you run the **fsmcm -off** command, the CMM CLI session terminates. You can now authenticate to the CMM and other chassis components by using local CMM credentials, and use local CMM credentials to access the CMM web interface or CLI for the chassis until user management by XClarity Administrator is restored.

     For more information, see the fsmcm command in the CMM online documentation.

After XClarity Administrator is restored or replaced, you can manage the chassis again (see Managing chassis). All information about the chassis (such as network settings) is retained.

Unmanaging a chassis

You can remove a chassis from management by Lenovo XClarity Administrator. This process is called *unmanaging*. After the chassis is unmanaged, you can log in to the CMM for the chassis by using the local CMM user accounts.

Before you begin

You can enable XClarity Administrator to automatically unmanage devices that are offline for a specific amount of time. This is disabled by default. To enable the automatic unmanagment of offline devices, click **Hardware ➞ Discover and Manage New Devices** from the XClarity Administrator menu, and then click **Edit** next to **Unmanage offline devices is Disabled**. Then, select **Enable unmanage offline devices** and set the time interval. By default, devices are unmanaged after being offline for 24 hours.

Before you unmanage a chassis, ensure that there are no active jobs running against any devices that are installed in the chassis.

When Call Home is enabled in XClarity Administrator, Call Home is disabled on all managed chassis and servers to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time (see Re-enabling call home on all managed devices in the XClarity Administrator online documentation).

About this task

When you unmanage a chassis, XClarity Administrator performs the following actions:

- Clears the configuration used for centralized user management.
- Removes the CMM security certificate from the XClarity Administrator trust store.

- If Encapsulation is enabled on the device, configures the devices firewall rules to the settings before the device was managed.
- Removes access to the NTP server from the CMM.
- Removes the CIM subscriptions to the CMM from the XClarity Administrator configuration so that XClarity Administrator no longer receives events from that chassis.

When you unmanaged a chassis, XClarity Administrator retains certain information about the chassis. That information is reapplied when you manage the same chassis again.

When you unmanage a chassis, events that were sent from the chassis components are discarded. You can retain these events by forwarding the events to an external repository, such as a syslog (see Forwarding events).

Tip: All demo devices that are optionally added during initial setup are nodes in a chassis. To unmanage the demo devices, unmanage the chassis using the **Force unmanage even if the device is not reachable** option.

Procedure

To unmanage a chassis, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Chassis** to display the Chassis page.

Step 2. Select one or more chassis from the lists of managed chassis.

Step 3. Click **Unmanage Chassis**. The Unmanage dialog is displayed.

Step 4. Optional: **Optional:** Select **Force unmanage even if the device is not reachable**.

Important: When unmanaging demo hardware, ensure that you select this option.

Step 5. Click **Unmanage**.The Unmanage dialog shows the progress of each step in the unmanagement process.

Step 6. When the unmanagement process is complete, click **OK**.

After you finish

After the unmanage process is completed, you can log in to the CMM using the local CMM user accounts. If you do not remember the user names or passwords for any local CMM user accounts, reset the CMM to factory defaults to log in to the CMM. For information about resetting the CMM to factory defaults, see CMM Reset in the Flex Systems online documentation in the CMM product documentation.

Recovering a chassis that was not unmanaged correctly

If a chassis was not unmanaged correctly, you must recover the chassis before you can remanage it.

Procedure

Complete one of the following procedures to restore management on a CMM.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, manage the device again using the RECOVERY_ID account and password and the **Force management** option (see Managing chassis).
- Reset the CMM to factory defaults by pressing the pinhole button on the CMM using a paperclip for at least 10 seconds. For more information about resetting the CMM, including important notices, see CMM Reset in the Flex Systems online documentation.
- Reset the CMM configuration using the following steps:

1. Through an SSH session, open a management command-line interface for the chassis, and log in with the `RECOVERY_ID` account.

   Note: The password for the `RECOVERY_ID` account was set when you selected the chassis for management on the Management Domain page. For more information about central account management, see Managing chassis.

   If this is the first time that you have used the `RECOVERY_ID` account to log in to the CMM, you must change the password.
2. If you are prompted, type the new password for the `RECOVERY_ID` account.
3. Restore the CMM configuration by performing one of the following steps:
   - If you are running CMM firmware release June 2015 or later, run the following command:
     `read -f unmanage -T mm[p]`
     For more information, see the read command in the CMM online documentation.
   - If you are running CMM firmware release earlier than June 2015, run the following commands in the order shown:
     a. **env -T mm[p]**
     b. **sslcfg -client disabled -tc1 remove**
     c. **accseccfg -am local**
     d. **ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""**
     e. **ntp -en disabled -i 0.0.0.0 -v3en disabled**
     f. **cimsub -clear all**
     g. **fsmcm -off**

        The **fsmcm** command disables XClarity Administrator user-account management and allows you to use local CMM user accounts to authenticate to the CMM and any management processor that is installed in the chassis.

        After you run the **fsmcm -off** command, the `RECOVERY_ID` account is removed from the CMM user registry. When you run the **fsmcm -off** command, the CMM CLI session terminates. You can now authenticate to the CMM and other chassis components by using local CMM credentials, and use local CMM credentials to access the CMM web interface or CLI for the chassis until user management by XClarity Administrator is restored.

        For more information, see the fsmcm command in the CMM online documentation.

After XClarity Administrator is restored or replaced, you can manage the chassis again (see Managing chassis). All information about the chassis (such as network settings) is retained.

Chapter 8. Managing servers

Lenovo XClarity Administrator can manage several types of systems, including ThinkAgile, ThinkSystem, Converged, Flex System, NeXtScale, System x®, and ThinkServer® servers.

Learn more: XClarity Administrator: Discovery

Before you begin

Note: Flex compute nodes are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed Flex compute nodes independent of the chassis.

You can discover and manage Flex Power Systems compute nodes; however, you can use XClarity Administrator only to view properties and status for those servers. You must use other management alternative (such as Flex System Manager or Flex Power Systems Hardware Management Console) to take any management-related actions on the devices, such as updating firmware or configuring the device. You cannot use the Flex System Manager management node and the XClarity Administrator to manage compute nodes in the same chassis.

Note: If you have a managed chassis that contains both Flex System and Flex Power System compute nodes, and you cannot log in to the Flex Power System compute nodes directly, see Cannot log in to managed Flex Power System compute nodes in the XClarity Administrator online documentation.

Before managing servers, ensure that the following conditions are met:

- Review the management considerations before managing a device. For information, see Management considerations in the XClarity Administrator online documentation.
- Certain ports must be available to communicate with devices. Ensure that all required ports are available before you attempt to manage servers. For information about ports, see Port availability in the XClarity Administrator online documentation.
- Ensure that the minimum required firmware is installed on each server that you want to manage using XClarity Administrator. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.
- Ensure that CIM over HTTPS is enabled on the device.
  1. Log in to the management web interface for the server using the `RECOVERY_ID` user account,
  2. Click **IMM Management → Security**.
  3. Click the **CIM Over HTTPS** tab, and ensure that **Enable CIM Over HTTPS** is selected.
- For ThinkSystem SR635 and SR655 servers:
  - Ensure that an operating system is installed, and that the server was booted to the OS, mounted bootable media, or efishell at least once so that XClarity Administrator can collect inventory for those servers.
  - Ensure that IPMI over LAN is enabled. IPMI over LAN is disabled by default on these servers and must be manually enabled before the servers can be managed. To enable IPMI over LAN using TSM, click **Settings → IPMI Configuration**. You might need to restart the server to activate the change.
- If the device's server certificate is signed by an external certificate authority, ensure that the certificate authority certificate and any intermediate certificates are imported into the XClarity Administrator trust store (see Deploying customized server certificates to managed devices).
- To discover a server that is on a *different* subnet from XClarity Administrator, ensure that one of the following conditions are met:

© Copyright Lenovo 2015, 2022

  - Ensure that you enable multicast SLP forwarding on the top-of-rack switches, as well as the routers in your environment. See the documentation that was provided with your specific switch or router to determine whether multicast SLP forwarding is enabled and to find procedures to enable it if it is disabled.
  - If SLP is disabled on the endpoint or on the network, you can use DNS discovery method instead by manually adding a service record (SRV record) to your domain name server (DNS), for XClarity Administrator for example
    `_lxca._tcp.labs.lenovo.com  service = 0 0 443 fvt-xhmc3.labs.lenovo.com.`

    Then, enable DNS discovery on the baseboard management console from the management web interface, by clicking **IMM Management → Network Protocol**, clicking the **DNS** tab, and selecting **Use DNS to discover Lenovo XClarity Administrator**.

    Notes:

    - The management controller must be running a firmware level dated May 2017 or later to support automatic discovery using DNS.
    - If there are multiple XClarity Administrator instances in your environment, the server is discovered only by the instance that is the first to respond to the discovery request. The server is not discovered by all instances.
- To discover and manage ThinkServer servers, ensure that the following requirements are met. For more information, see Cannot discover a device and Cannot manage a device in the XClarity Administrator online documentation.
  - The hostname of the server must be configured using a valid hostname or IP address if you want XClarity Administrator to discover the servers automatically.
  - The network configuration must allow SLP traffic between XClarity Administrator and the server.
  - Unicast SLP is required.
  - If you want XClarity Administrator to automatically discover ThinkServer servers, multicast SLP is required. In addition, SLP must be enabled on the ThinkServer System Manager (TSM).
  - If ThinkServer servers are on a different network than XClarity Administrator, ensure that the network is configured to allow inbound UDP through port 162 so that XClarity Administrator can receive events for those devices.
- For ThinkAgile, ThinkSystem, Converged, Flex System. NeXtScale, and System x servers, if you remove, replace, or configure any adapters in the server, restart the server at least once to update the new adapter information in the baseboard management controller and XClarity Administrator reports (Powering on and off a server).
- When performing management actions on a server, ensure that the server is either powered off or powered on to the BIOS/UEFI Setup or to a running operating system. (You can boot to BIOS/UEFI Setup from the Servers page in XClarity Administrator by clicking **All Actions → Power Actions → Restart to BIOS/UEFI Setup**.) If server is powered on without an operating system, the management controller continuously resets the server in an attempt to find an operating system.
- Ensure that all `UEFI_Ethernet_*` and `UEFI_Slot_*` settings are enabled in the server UEFI Settings. To verify the settings, restart the server and when the prompt `<F1> Setup` is displayed, press `F1` to start the Setup utility. Navigate to **System Settings → Devices and I/O Ports → Enable / Disable Adapter Option ROM Support**, and then locate the **Enable / Disable UEFI Option ROM(s)** section to verify that the settings are enabled.

  Note: If supported, you can also use the Remote Console feature in the baseboard management interface to review and modify the settings remotely.
- System x3950 X6 servers must be managed as two 4U enclosures, each with its own baseboard management controller.

About this task

XClarity Administrator can automatically discover rack and tower servers in your environment by probing for manageable devices that are on the same IP subnet as XClarity Administrator. To discover rack and tower servers that are in other subnets, specify an IP address or range of IP addresses, or import information from a spreadsheet.

Important: For System x3850 and x3950 X6 servers, you must manage each server in the scalable rack environment.

After the servers are managed by XClarity Administrator, Lenovo XClarity Administrator polls each managed server periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed server and perform management actions (such as configuring system settings, deploying operating-system images, and powering on and off).

By default, devices are managed using XClarity Administrator managed authentication to log in to the devices. When managing rack servers and Lenovo chassis, you can choose to use local authentication or managed authentication to log in to the devices.

- When *local authentication* is used for rack servers, Lenovo chassis, and Lenovo rack switches, XClarity Administrator uses a stored credential to authenticate to the device. The *stored credential* can be an active user account on the device or a user account in an Active Directory server.

  You must create a stored credential in XClarity Administrator that matches an active user account on the device or a user account in an Active Directory server before managing the device using local authentication (see Managing stored credentials in the XClarity Administrator online documentation).

  Notes:

  – RackSwitch devices support only stored credentials for authentication. XClarity Administrator user credentials are not supported.
- Using *managed authentication* allows you to manage and monitor multiple devices using credentials in the XClarity Administrator authentication server instead of local credentials. When managed authentication is used for a device (other than ThinkServer servers, System x M4 servers, and switches), XClarity Administrator configures the device and its installed components to use the XClarity Administrator authentication server for centralized management.

  – When managed authentication is enabled, you can manage devices using either manually-entered or stored credentials (see Managing user accounts and in the XClarity Administrator online documentation).

    The stored credential is used only until XClarity Administrator configures the LDAP settings on the device. After that, any change to the stored credential has no impact the management or monitoring of that device.

    Note: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.

  – If a local or external LDAP server is used as the XClarity Administrator authentication server, user accounts that are defined in the authentication server are used to log in to XClarity Administrator, CMMs and baseboard management controllers in the XClarity Administrator domain. Local CMM and management controller user accounts are disabled.

  – If an SAML 2.0 identity provider is used as the XClarity Administrator authentication server, SAML accounts are not accessible to managed devices. However, when using an SAML identity provider and an LDAP server together, if the identity provider uses accounts that exist in the LDAP server, LDAP user accounts can be used to log into the managed devices while the more advanced authentication methods that are provided by SAML 2.0 (such as multifactor authentication and single sign-on) can be used to log into XClarity Administrator.

- Single sign-on allows a user that is already logged in to XClarity Administrator to automatically log in to the baseboard management control (XCC). Single sign-on is enabled by default when a ThinkSystem or ThinkAgile server is brought into management by XClarity Administrator (unless the server is managed with CyberArk passwords). You can configure the global setting to enable or disable single sign-on for all managed ThinkSystem and ThinkAgile servers. Enabling single sign-on for a specific ThinkSystem and ThinkAgile server overrides the global setting for all ThinkSystem and ThinkAgile servers (see Managing servers).

  Note: Single sign-on is disabled automatically when using the CyberArk identity-management system for authentication.
- When managed authentication is enabled for ThinkSystem SR635 and SR655 servers:
  - Baseboard management-controller firmware supports up to five LDAP user roles. XClarity Administrator adds these LDAP user roles to the servers during management: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin**, and **lxc-os-admin**.

    Users must be assigned to at least one of the specified LDAP user roles to communicate with ThinkSystem SR635 and SR655 servers.
  - Management-controller firmware does not support LDAP users with the same username as local user of the sever.
- For ThinkServer and System x M4 servers, the XClarity Administrator authentication server is not used. Instead, an IPMI account is created on the device with the prefix “LXCA_” followed by a random string. (The existing local IPMI user accounts are not disabled.) When you unmanage a ThinkServer server, the “LXCA_” user account is disabled, and the prefix “LXCA_” is replaced with the prefix “DISABLED_”. To determine whether a ThinkServer server is managed by another instance, XClarity Administrator checks for IPMI accounts with the prefix “LXCA_”. If you choose to force management of a managed ThinkServer server, all the IPMI accounts on the device with the “LXCA_” prefix are disabled and renamed. Consider manually clearing IPMI accounts that are no longer used.

  In XClarity Administrator v2.4 and later, if you use manually-entered credentials, XClarity Administrator automatically creates a stored credential and uses that stored credential to manage the device.

  Notes: When managed authentication is enabled for a device, you cannot edit stored credentials for that device using XClarity Administrator.
  - Each time you manage a device using manually-entered credentials, a new stored credential is created for that device, even if another stored credential was created for that device during a previous management process.
  - When you unmanage a device, XClarity Administrator does not delete stored credentials there were automatically created for that device during the management process.

A device can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device on the initial XClarity Administrator, and then manage it with the new XClarity Administrator. If an error occurs during the unmanagement process, you can select the **Force management** option during management on the new XClarity Administrator.

Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a device is already managed by another manager until after it attempts to manage the device.

Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a ThinkServer device is already managed; therefore, managed ThinkServer devices might appear in the list of manageable devices.

During the management process, XClarity Administrator performs the following actions:

- Logs in to the server using the provided credentials.
- Collects inventory for each server.

  Note: Some inventory data is collected after the management process completes. You cannot perform certain tasks on a managed server (such as deploying a server pattern) until all inventory data is collected for that server and the server is no longer in the Pending state.
- Configures settings for the NTP server so all managed devices use the same NTP server configuration that is configured on XClarity Administrator.
- (System x and NeXtScale severs only) Assigns the last-edited firmware-compliance policy to the server.
- (Lenovo System x and NeXtScale severs only) Optionally configures the devices firewall rules so that incoming requests from only XClarity Administrator are accepted.
- (System x and NeXtScale severs only) Exchanges security certificates with the management controller, copying the CIM server certificate and the LDAP client certificate from the management controller into the XClarity Administrator trust store and sending the XClarity Administrator CA security certificate and LDAP trust certificates to the management controller. The management controller loads the certificates into the management-controller trust store so that the management controller can trust connections to the LDAP and CIM servers on the XClarity Administrator.

  Note: If the CIM server certificate or LDAP client certificate does not exist, it is created during the management process.
- Configures managed authentication, if applicable. For more information about managed authentication, see Managing the authentication server.
- Creates the recovery user account (`RECOVERY_ID`), when applicable. For more information about the `RECOVERY_ID` account, see Managing the authentication server.

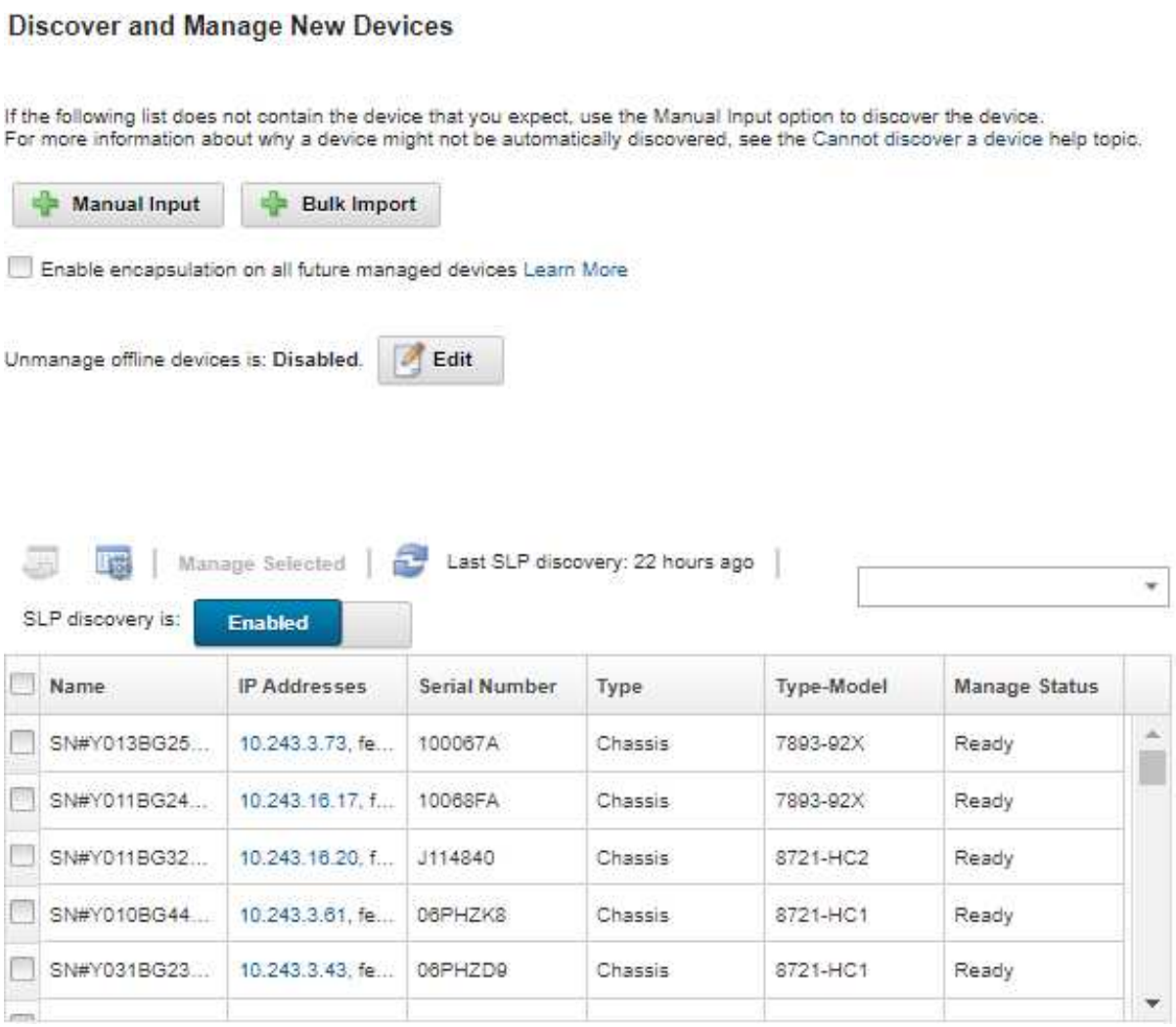
Note: The XClarity Administrator does not modify the security settings or cryptographic settings (cryptographic mode and the mode used for secure communications) during the management process. You can modify the cryptographic settings after the server is managed (see Configuring cryptography settings).

Important: If you change the IP address of a server after the server is managed by XClarity Administrator, XClarity Administrator recognizes the new IP address and continue to manage the server. however, XClarity Administrator does not recognize the IP address change for some servers. If XClarity Administrator shows that the server is offline after the IP address was changed, manage the server again using the **Force Management** option.

Procedure

To manage your rack and tower servers using XClarity Administrator, complete one of the following procedures.

- Discover and manage a large number of tower and rack servers and other devices using a bulk-import file (see Managing systems in the XClarity Administrator online documentation).
- Discover and manage rack and tower servers that are on the same IP subnet as XClarity Administrator.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage New Devices page is displayed.



You can sort the table columns to make it easier to find the servers that you want to manage. In addition, you can enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed. You can change the columns that are displayed and the default sort order by clicking the **Customize Columns** icon ( ).

2. Click the **Refresh** icon ( ) to discover all manageable devices in the XClarity Administrator domain. Discovery might take several minutes.
3. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

   Encapsulation can be enabled or disabled on specific devices after they are managed.

   Note: When the management network interface is configured to use the Dynamic Host Configuration Protocol (DHCP) and when encapsulation enabled, managing a rack server can take a long time.

   Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
4. Select one or more servers that you want to manage.

5. Click **Manage Selected**. The Manage dialog is displayed.
6. Choose to use XClarity Administrator managed authentication or local authentication for this device. Managed authentication is selected by default. To use local authentication, clear **Managed Authentication**.
7. Choose the type of credentials to use to authenticate to the device and specify the appropriate credentials:
   - **Use manually entered credentials**
     - Specify the user ID and password for authenticating to the server.
     - (Optional) Set a new password for the specified user name if the password is currently expired on the device.

     Note: To use manually entered credentials, you must select XClarity Administrator managed authentication.
   - **Use stored credentials**

     Select the stored credential to use for this managed device. You can create a new stored credential by clicking **Create New**.
   - **Use identity-management system**

     Select the identity management system that you want to use for this managed device. Then, fill in the remaining fields, including the IP address or host name of the managed server, user name, and optionally application ID, safe and folder.

     If you specify the application ID, you must also specify the safe and folder, if applicable.

     If you do not specify the application ID, XClarity Administrator uses the paths that were defined when you setup CyberArk to identify the onboarded accounts in CyberArk (see Setting up a CyberArk identity-management system).

     Note: Only ThinkSystem or ThinkAgile servers are supported. The identity management system must be configured in XClarity Administrator, and the Lenovo XClarity Controller for the managed ThinkSystem or ThinkAgile servers must be integrated with CyberArk (see Setting up a CyberArk identity-management system).

   It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

   For more information about normal and stored credentials, see Managing user accounts and Managing stored credentials.
8. Specify the recovery password if managed authentication is selected.

   When a password is specified, the recovery account (`RECOVERY_ID`) is created on the server, and all local user accounts are disabled. If there is a problem with XClarity Administrator, and it stops working for some reason, you *cannot* log in to the management controller using normal user accounts. However, you can log in using the recovery account.

   Notes:
   - The recovery password is optional if you choose to use managed authentication and is not allowed if you if you choose to use local authentication.
   - You can choose to use a local recovery account or stored recovery credentials. In either case, the user name is always `RECOVERY_ID`.

- Ensure that the password follows the security and password policies for the device. Security and password policies might vary.
- Ensure that you record the recovery password for future use.
- The recovery account is not supported for ThinkServer and System x M4 servers.

For more information about the recovery ID, see Managing the authentication server.

9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   - You can select from a list of role groups that are assigned to the current user.
   - If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    - If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    - If the managing XClarity Administrator was taken down before the devices were unmanaged.
    - If the devices were not unmanaged successfully.

    Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

- Discover and manage rack and tower servers that are not on the same IP subnet as XClarity Administrator by manually specifying IP addresses.

  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

     Encapsulation can be enabled or disabled on specific devices after they are managed.

     Note: When the management network interface is configured to use the Dynamic Host Configuration Protocol (DHCP) and when encapsulation enabled, managing a rack server can take a long time.

     Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.

3. Select **Manual Input**.
4. Specify the network addresses of the servers that you want to manage:
   - Click **Single System**, and enter a single IP address domain name, or fully-qualified domain name (FQDN).

     Note: To specify an FQDN, ensure that a valid domain name is specified on Network Access page (see Configuring network access).
   - Click **Multiple Systems**, and enter a range of IP addresses. To add another range, click the **Add** icon (). To remove a range, click the **Remove** icon ().
5. Click **OK**. The Manage dialog is displayed
6. Choose to use XClarity Administrator managed authentication or local authentication for this device. Managed authentication is selected by default. To use local authentication, clear **Managed Authentication**.
7. Choose the type of credentials to use to authenticate to the device and specify the appropriate credentials:
   - **Use manually entered credentials**
     - Specify the user ID and password for authenticating to the server.
     - (Optional) Set a new password for the specified user name if the password is currently expired on the device.

     Note: To use manually entered credentials, you must select XClarity Administrator managed authentication.
   - **Use stored credentials**

     Select the stored credential to use for this managed device. You can create a new stored credential by clicking **Create New**.
   - **Use identity-management system**

     Select the identity management system that you want to use for this managed device. Then, fill in the remaining fields, including the IP address or host name of the managed server, user name, and optionally application ID, safe and folder.

     If you specify the application ID, you must also specify the safe and folder, if applicable.

     If you do not specify the application ID, XClarity Administrator uses the paths that were defined when you setup CyberArk to identify the onboarded accounts in CyberArk (see Setting up a CyberArk identity-management system).

     Note: Only ThinkSystem or ThinkAgile servers are supported. The identity management system must be configured in XClarity Administrator, and the Lenovo XClarity Controller for the managed ThinkSystem or ThinkAgile servers must be integrated with CyberArk (see Setting up a CyberArk identity-management system).

   It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

   For more information about normal and stored credentials, see Managing user accounts and Managing stored credentials.
8. Specify the recovery password if managed authentication is selected.

When a password is specified, the recovery account (RECOVERY_ID) is created on the server, and all local user accounts are disabled. If there is a problem with XClarity Administrator, and it stops working for some reason, you *cannot* log in to the management controller using normal user accounts. However, you can log in using the recovery account.

Notes:

- The recovery password is optional if you choose to use managed authentication and is not allowed if you if you choose to use local authentication.
- You can choose to use a local recovery account or stored recovery credentials. In either case, the user name is always RECOVERY_ID.
- Ensure that the password follows the security and password policies for the device. Security and password policies might vary.
- Ensure that you record the recovery password for future use.
- The recovery account is not supported for ThinkServer and System x M4 servers.

For more information about the recovery ID, see Managing the authentication server.

9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   - You can select from a list of role groups that are assigned to the current user.
   - If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    - If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    - If the managing XClarity Administrator was taken down before the devices were unmanaged.
    - If the devices were not unmanaged successfully.

    Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

After you finish

- Discover and manage additional devices.
- Configure the system information, local storage, I/O adapters, boot topics, and firmware settings by creating and deploying server patterns (see Configuring servers using configuration patterns).

- Deploy operating-system images to servers that do not already have an operating system installed (see Installing operating systems on bare-metal servers).
- Update firmware on devices that are not in compliance with current policies (see Updating firmware on managed devices).
- Add the devices to the appropriate rack to reflect the physical environment (see Managing racks).
- Monitor hardware status and details (see Viewing the status of a managed server).
- Monitor events and alerts (see Working with events and Working with alerts).
- Clear the SEL log for a server by clicking **Hardware → Servers** from the XClarity Administrator menu bar, selecting the server, and then clicking **All Actions → Security → Clear SEL Log**.This action is supported for only ThinkSystem and ThinkAgile servers.
- Resolve stored credentials that have become expired or invalid (see Managing stored credentials).
- Enable or disable single sign-on for all managed ThinkSystem and ThinkAgile servers by clicking **Administration → Security** from the XClarity Administrator menu bar, clicking **Active Sessions**, and then enabling or disabling **Single Sign-On**.
- Disable or enable single sign-on for managed ThinkSystem and ThinkAgile servers.
  - For all managed ThinkSystem and ThinkAgile servers (globally), click **Administration → Security** from the XClarity Administrator menu bar, click **Active Sessions**, and then enable or disable **Single Sign-On**
  - For a specific ThinkSystem and ThinkAgile server, click **Hardware → Server** from the XClarity Administrator menu bar, and then click **All Actions → Security → Enable Single Sign-On** or **All Actions → Security → Disable Single Sign-On**.

  Note: Single sign-on allows a user that is already logged in to XClarity Administrator to automatically log in to the baseboard management control (XCC). Single sign-on is enabled by default when a ThinkSystem or ThinkAgile server is brought into management by XClarity Administrator (unless the server is managed with CyberArk passwords). You can configure the global setting to enable or disable single sign-on for all managed ThinkSystem and ThinkAgile servers. Enabling single sign-on for a specific ThinkSystem and ThinkAgile server overrides the global setting for all ThinkSystem and ThinkAgile servers.

Viewing the status of a managed server

You can view a summary and detailed status for the managed servers and their installed components from the Lenovo XClarity Administrator.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

The following status icons are used to indicate the overall health of the device. If the certificates do not match, “(Untrusted)” is appended to the status of each applicable device, for example Warning (Untrusted). If there is a connectivity issue or a connection to the device is not trusted, “(Connectivity)” is appended to the status of each applicable device, for example Warning (Connectivity).

- ( ) Critical
- ( ) Warning
- ( ) Pending
- ( ) Informational
- ( ) Normal

- ( ) Offline
- ( ) Unknown

A device can be in one of the following power states:
- On
- Off
- Shutting down
- Standby
- Hibernate
- Unknown

Procedure

To view the status for a managed server, complete one or more of the following actions.

- From the XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of all managed devices and other resources.

- From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack and tower servers, and compute nodes).

  You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list, enter text (such as a name or IP address) in the **Filter** field, and click the status icons to list only those servers that meet the selected criteria.

From this page, you can perform the following actions:

- View detailed information about the server and its components (see Viewing the details of a managed server).
- View a server in graphical rack or chassis view clicking **All Actions → Views → Show in Rack View** or **All Actions → Views → Show in Chassis View**.
- Launch the management controller web interface for the server by clicking the **IP address** link (see Launching the management controller interface for a server).
- Remotely manage the server (see Using remote control to manage Converged, Flex System, NeXtScale, and System x servers).
- Power the server on and off (see Powering on and off a server).
- Modify system information by selecting a server and clicking **All Actions → Inventory → Edit Properties**.
- Refresh inventory by selecting a server and clicking **All Actions → Inventory → Refresh Inventory**.
- Export detailed information about one or more servers to a single CSV file by selecting the servers and clicking **All Actions → Inventory → Export Inventory**.

  Note: You can export inventory data for a maximum of 60 devices at one time.

  Tip: When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Unmanage a server (see Unmanaging a rack or tower server).
- Reset the local storage adapters to their default manufacturing settings by clicking **All Action → Service → Reset Local Storage to Defaults**.
- Change the Location LED state on a server to on, off, or blinking by selecting the server and clicking **All Actions → Service → Toggle Location LED State**, selecting the state, and clicking **Apply**.
  - Toggling the Location LED for ThinkSystem SR635 and SR655 servers is not supported.
  - The Location LED on ThinkServer servers can be on or off. Blinking is not supported.
- Virtually reseat the server (see Virtually reseating a server in a Flex System chassis).
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Exclude events** icon ( ) (see Excluding events).
- Restart the server using a non-maskable interrupt (NMI) by clicking **All Action → Service → Trigger NMI**.

- Enable or disable firewall rule changes on a server that limit incoming requests only from XClarity Administrator by selecting the server and clicking **All Actions → Security → Enable Encapsulation** or **All Actions → Security → Disable Encapsulation**.The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

  When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

  Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.
- (Converged, Flex System, NeXtScale, System x, and ThinkSystem servers only) Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the baseboard management controller in the server by selecting a server and clicking **All Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).
- Resolve expired or invalid stored credentials for a device in the group (see Resolving expired or invalid stored credentials for a server).
- Add or remove a server from a static resource group by clicking **All Actions → Groups → Add to Group** or **All Actions → Groups → Remove from Group**.

Viewing the details of a managed server

You can view detailed information about the managed servers from Lenovo XClarity Administrator, including the firmware levels, server name, and universally unique identifier (UUID).

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

CPU usage is a measurement of the aggregated C-state residency. It is measured as a percentage of the used and maximum C0 residency, per second.

Memory usage is a measurement of the aggregated read/write volumes of all memory channels. This is calculated as a percentage of the used and maximum memory bandwidth that is available, per second.

The system-level air temperature is measured by a physical sensor at the front of the server. This temperature represents inlet air temperature for the server. Note that the air temperature that is reported by XClarity Administrator and the CMM might differ if the temperature is captured at different points in time.

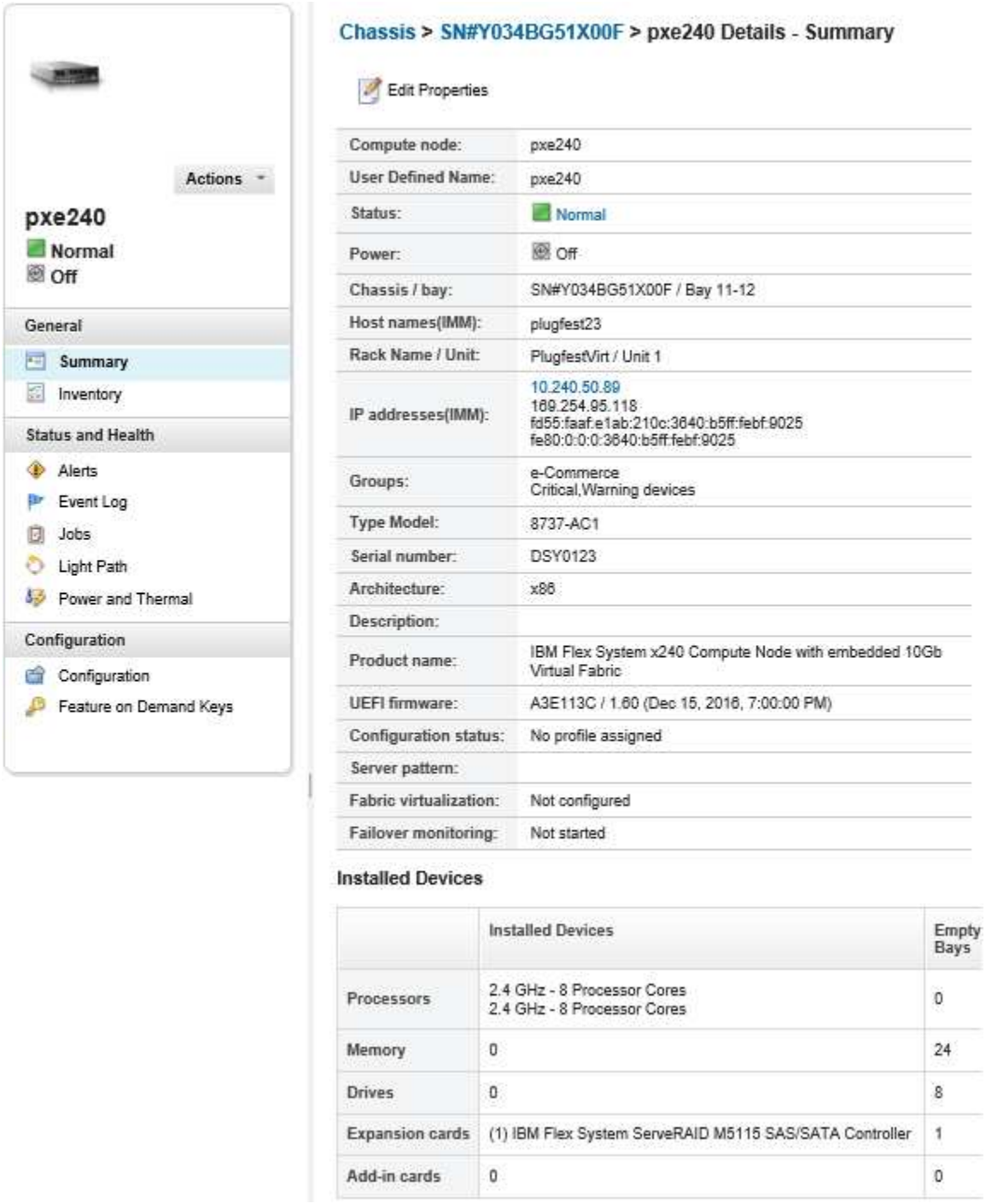
Procedure

Complete the following steps to view the details for a managed server.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find the specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a system name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Click the link for the server in the **Server** column. The status summary page for that server is displayed, showing the server properties and a list of components that are installed in that server.



Note: For System x and NeXtScale servers, the LAN over USB address is listed on this page; however, you cannot change that address from the XClarity Administrator. Instead, you must use the baseboard-management-controller interface for the server. For more information, see "Accessing the IMM2 using the LAN over USB interface" in the product documentation for the server. You can find the product documentation for your server in the BladeCenter online documentation.

Step 3. Complete one or more of the following actions:

- Click **Summary** to view a summary of the server, including system information and installed components (see Viewing the status of a managed server).

- Click **Inventory Details** to view details about the server components, including:
  - Firmware levels for the server and management controller.
  - Management-module network details, such as the hostname, IPv4 address, IPv6 address, and MAC addresses.
  - Asset details, including server name, universally unique identifier (UUID), and location.
  - Components details, including CPUs, memory, drives, and expansion cards.

  Notes:

  - All IP addresses for the server are listed. The IP address for the management controller port is listed first. If the management controller IP address is available, it is used to connect to the server.
  - If data is not available for a specific adapter, some fields for the adapter (such as product name) might be empty.
  - If a new adapter was installed in the server, the server must be rebooted for the adapter to show up in the inventory.
  - For some add-in cards, the Feature on Demand (FoD) information is displayed under the device name.
  - You can hover over links in the Type column to get to get more information about specific components, such as Intel Optain DCPMM memory.
- Click **Alerts** to display the list of current alerts for this server (see Working with alerts).

  Note: You can set threshold preferences for raising an alert and event when a certain value, such as the life of an SSD in a ThinkSystem or ThinkServer server, exceeds a warning or critical level (see Setting threshold preferences for generating alerts and events).
- Click **Event Log** to display the list of events for this server (see Monitoring events in the event log).
- Click **Jobs** to display a list of jobs associated with the server (see Monitoring jobs).
- Click **Light Path** to display the current status of the server LEDs, including Location, Fault, and Information. This is the equivalent of looking at the front panel of the server.
- Click **Power and Thermal** to display details about power use and air temperature.

  Tip: Use the refresh button on your web browser to collect the latest power and thermal data. Collecting data might take several minutes.
- Click **Configuration** to view the current configuration information for the server (including local storage, I/O adapters, SAN boot settings, and firmware settings) and its compliance with the assigned configuration pattern (see Configuring servers using configuration patterns).
- Click **Feature on Demand Keys** to view a list of Feature on Demand keys that are currently installed on the managed server (see Viewing Features on Demand keys).

After you finish

In addition to displaying summary and detailed information about a server, you can perform the following actions:

- View the rack or chassis that is associated with the server by clicking rack or chassis name from the Summary page.
- View a selected server in graphical rack or chassis view clicking **All Actions → Views → Show in Rack View** or **All Actions → Views → Show in Chassis View**.
- Launch the management controller web interface for a selected server by clicking the **IP address** link (see Launching the management controller interface for a server).

- Remotely access a server (see Using remote control to manage Converged, Flex System, NeXtScale, and System x servers).
- Power a selected server on and off (see Powering on and off a server).
- Modify system information of a selected server by clicking **Edit Properties**.
- Refresh inventory of a selected server by clicking **Actions → Inventory → Refresh Inventory**.
- Export detailed information about the servers to a CSV file clicking the **Actions → Inventory → Export Inventory**.

  Notes:

  – For more information about inventory data in the CSV file, see the GET /nodes/<*UUID_list*> in the XClarity Administrator online documentation.

  – When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Actions → Service Reset → Exclude events** (see Excluding events).
- Restart a selected server using a non-maskable interrupt (NMI) by clicking **Actions → Service → Trigger NMI**
- Change the Location LED state on a selected server to on, off, or blinking by clicking **Actions → Service → Toggle Location LED State**, selecting the state, and clicking **Apply**.

  Notes:

  – Toggling the Location LED for ThinkSystem SR635 and SR655 servers is not supported.

  – The Location LED on ThinkServer servers can be on or off. Blinking is not supported.
- Disable or enable single sign-on for a selected ThinkSystem and ThinkAgile server by clicking **All Actions → Security → Enable Single Sign-On** or **All Actions → Security → Disable Single Sign-On**.

  Single sign-on allows a user that is already logged in to XClarity Administrator to automatically log in to the baseboard management control (XCC). Single sign-on is enabled by default when a ThinkSystem or ThinkAgile server is brought into management by XClarity Administrator (unless the server is managed with CyberArk passwords). You can configure the global setting to enable or disable single sign-on for all managed ThinkSystem and ThinkAgile servers. Enabling single sign-on for a specific ThinkSystem and ThinkAgile server overrides the global setting for all ThinkSystem and ThinkAgile servers.

  Note: Single sign-on is disabled automatically when using the CyberArk identity-management system for authentication.
- Enable or disable firewall rule changes on a selected server that limit incoming requests only from XClarity Administrator by clicking **Actions → Security → Enable Encapsulation** or **Actions → Security → Disable Encapsulation**. The global encapsulation setting is disabled by default. When disabled, the device encapsulation mode is set to “normal” and the firewall rules are not changed as part of the management process.

  When the global encapsulation setting is enabled and the device supports encapsulation, XClarity Administrator communicates with the device during the management process to change the device encapsulation mode to “encapsulationLite” and to change the firewall rules on the device to limit incoming requests to those only from XClarity Administrator.

  Attention: If encapsulation is enabled and XClarity Administrator becomes unavailable before a device is unmanaged, necessary steps must be taken to disable encapsulation to establish communication with the device. For recovery procedures, see lenovoMgrAlert.mib file and Recovering management with a CMM after a management server failure.

- (non-ThinkServer servers only) Resolve issues that might arise between the Lenovo XClarity Administrator security certificate and the security certificate of the management controller in the selected server by clicking **Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).

Backing up and restoring server-configuration data

Lenovo XClarity Administrator does not include built-in backup functions for server-configuration data. Instead, use the backup functions that are available for your managed server.

- **Converged, Flex System, System x, ThinkSystem, and NeXtScale servers**
  - Back up server-configuration data

    Use the management web interface or CLI to back up the firmware.

    - From the IMM web interface, click **IMM Management → IMM Configuration**.
    - From the CLI, use the **backup** command.

    For more information about backing up servers using the IMM, see the Integrated Management Module II online documentation.

    Use tools that are provided by the operating system to back up applications that are running on the server. For more information, see the documentation that came with your operating system.

    For Flex System compute devices, ensure that you back up the settings for options that are installed on the compute nodes. You can back up all compute node settings, including the option settings, using the Advanced Setup Utility (ASU). For information about ASU, see Advanced Settings Utility (ASU) website).
  - Restore server-configuration data

    Use the management web interface or the CLI to restore the firmware. For more information about restoring servers through the BMC, see Integrated Management Module II online documentation.

    Use the documentation that is provided with the operating system and any applications that are running on the server to restore the software that is installed on the server.

    - From the IMM web interface, click **IMM Management → IMM Configuration**.
    - From the CLI, use the **restore** command.

  Note: Tip: You can find additional information about backing up and restoring chassis components in the PureFlex and Flex System Backup and Restore Best Practices Guide.
- **ThinkServer servers**The restore procedures vary for each type of ThinkServer servers. See the product documentation that is provided with your server for information about restoring the device.

Securely erasing drive data

Lenovo XClarity Administrator can securely erase data on all drives in selected ThinkSystem and ThinkAgile servers running version 22B and later. This operation permanently rewrites each drive by filling the entire drive with a binary zero, binary one, or random data, making it difficult to discover what was saved on the drive.

Attention:

- This operation *permanently* and *irreversibly* erases all data on the drives.
- There is no way to cancel this operation after the job is submitted.

Before you begin

You must have **lxc-supervisor** authority to erase drive data.

Ensure that the UEFI admin password is not set on the managed servers to be erased. If the UEFI admin password is set on any servers, the drives in those servers are not erased.

You can securely erase drive data for up to three servers at a time by default. You can configure the number of allowed servers at one time by clicking **Administration → Inventory Preferences** and setting the **Maximum number of servers that can be erased in a batch** to the desired value. You can choose a number from `3 - 100` servers.

Only one secure erase job is allowed at one time. You must wait for the current job to complete before started another secure erase job.

It might take several hours to erase very large drives.

You cannot securely erase SATA SDD volumes that are connected to Marvell RAID controllers. Instead, consider the following recommendations.

- For 7mm SATA SSDs, connect to Broadcom RAID controllers to perform secure erase.
- For M.2 SATA SSDs, connect to Marvell non-RAID controllers (such as ThinkSystem M.2 SATA/NVMe 2-Bay Enablement Kit) to perform secure erase.

About this task

You can erase data on the following drives.

- NVMe
- SAS
- SAS HBA
- SAS RAID
- SATA
- External-connected storage devices
  - Lenovo Storage D1212 (MT 4587)
  - Lenovo Storage D1224 (MT 4587)
  - Lenovo Storage D3284 (MT 6413)

The secure-erase operation creates an entry in the audit log. You can forward this events using the event forwarding function (see Forwarding events to syslog, remote SNMP manager, email, and other event services).

To troubleshoot secure erase issues, see and .

Procedure

To securely erase all drives in specific managed servers, complete the following steps.

Step 1. From the XClarity Administrator menu, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers.

Step 2. Select the server.

Step 3. Click **All Actions → Service → Drive Secure Erase (HDD/SDD)**.

Step 4. Enter your supervisor password to confirm that you want to erase all drives in the selected servers

Step 5. Click **Erase**.

If you choose to perform a mass drive erase on more than three servers, you are prompted to enter your user ID and password. Enter the same user credentials that you used to log in to XClarity Administrator.

A job is created to perform this operation. You can monitor the progress of the Jobs page by clicking **Monitoring → Jobs** from the XClarity Administrator menu. If the job did not complete successfully, click the job link to display details about the job (see Monitoring jobs).

Using remote control

From the Lenovo XClarity Administrator web interface, you can open a remote-control session to a managed server as if you were at a local console. You can use the remote-control session to perform operations such as powering on or off the server, and logically mounting a local or remote drive.

To launch a remote-control session for any device, you must have **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin**, or **lxc-hw-manager** privileges.

Using remote control to manage ThinkSystem or ThinkAgile servers

From the Lenovo XClarity Administrator web interface, you can open a remote-control session to a managed ThinkSystem or ThinkAgile server as if you were at a local console. You can use the remote-control session to perform power operations and logically mount a local or network drive.

Before you begin

Encapsulation must be disabled on the server.

To open a remote-control session to a server, the server must be in the Online or Normal state. If a server has any other access state, the remote-control session cannot connect to the server. For more information about viewing the server status, see Viewing the details of a managed server.

Review the following considerations for ThinkSystem SR635 and SR655 servers.
- Baseboard management controller firmware v2.94 or later is required.
- Only multiple-user mode is supported; single-user mode is not supported.
- Internet Explorer 11 is not supported.
- You cannot power on or power off a server from a remote-control session.

About this task

You can launch a remote-control session to a single ThinkSystem or ThinkAgile server from XClarity Administrator.

For more information about using the remote console and media features, see your ThinkSystem or ThinkAgile server documentation.

Note: For the ThinkSystem and ThinkAgile servers, a Java Runtime Environment (JRE) with Java WebStart support is not required.

Procedure

To open a remote-control session to a specific server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Select the server to which you want to open a remote-control session.

Step 3. Click the **Remote Control** icon ( ).

Step 4. Accept any security warnings from your web browser.

After you finish

If the remote-control session does not open successfully, see Remote control issues in the XClarity Administrator online documentation.

Using remote control to manage ThinkServer and NeXtScale sd350 M5 servers

From the Lenovo XClarity Administrator web interface, you can open a remote-control session to managed ThinkServer and NeXtScale sd350 M5 servers as if you were at a local console. You can use the remote-control session to perform power and reset operations, logically mount a local or network drive on the server, and capture screen shots and record video.

Before you begin

- Remote control for these servers requires a Java Runtime Environment (JRE) with Java WebStart support installed on the client side. An open-source JDK is highly recommended. If you are using a vendor's JRE or JDK, ensure that it is correctly licensed for commercial usage. The following JREs are supported.
  - Oracle JRE 7 (see Oracle Java download website)

    Attention:
    - Java 7 requires a minimum of TLSv1.2 support (see Configuring cryptography settings).
    - Support for Java 7 will be deprecated at a future date.
  - Oracle JRE 8, which requires a paid license (see Oracle Java download website)
  - Adoptium OpenJDK 8 with the IcedTea-Web v1.8 plugin (see the Adoptium OpenJDK website)
  - Amazon Corretto 8 (see Amazon Corretto 8 download website)

  Java WebStart is not included in OpenJDK or Coretto installation packages and needs to be installed separately. IcedTea-Web or OpenWebStart can be used under the GNU GPLV2 license (see the IcedTea-OpenJDK download website and OpenWebStart website).
- Remote control requires that a Features on Demand key for ThinkServer System Manager Premium Upgrade is installed on ThinkServer servers. For more information about FoD keys that are installed on your servers, see Viewing Features on Demand keys .

About this task

You can launch a remote-control session to a single ThinkServer server from XClarity Administrator.

To open a remote-control session to a server, the server must be in the Online or Normal state. If a server has any other access state, the remote-control session cannot connect to the server. For more information about viewing the server status, see Viewing the details of a managed server.

For more information about using the ThinkServer remote console and media features, see your ThinkServer server documentation.

Procedure

To open a remote-control session to a specific server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Select the server to which you want to open a remote-control session.

Step 3. Click the **Remote Control** icon ( ).

Step 4. Accept any security warnings from your web browser.

After you finish

If the remote-control session does not open successfully, see Remote control issues in the XClarity Administrator online documentation.

Using remote control to manage Converged, Flex System, NeXtScale, and System x servers

From the Lenovo XClarity Administrator web interface, you can open a remote-control session to manage Converged, Flex System, NeXtScale, and System x servers as if you were at a local console.

Before you begin

Learn more: XClarity Administrator: Remote control

- Remote control for these servers requires a Java Runtime Environment (JRE) with Java WebStart support installed on the client side. An open-source JDK is highly recommended. If you are using a vendor's JRE or JDK, ensure that it is correctly licensed for commercial usage. The following JREs are supported.
  - Oracle JRE 7 (see Oracle Java download website)

    Attention:
    - Java 7 requires a minimum of TLSv1.2 support (see Configuring cryptography settings).
    - Support for Java 7 will be deprecated at a future date.
  - Oracle JRE 8, which requires a paid license (see Oracle Java download website)
  - Adoptium OpenJDK 8 with the IcedTea-Web v1.8 plugin (see the Adoptium OpenJDK website)
  - Amazon Corretto 8 (see Amazon Corretto 8 download website)

  Java WebStart is not included in OpenJDK or Coretto installation packages and needs to be installed separately. IcedTea-Web or OpenWebStart can be used under the GNU GPLV2 license (see the IcedTea-OpenJDK download website and OpenWebStart website).
- You can launch a remote-control session on servers running the following operating systems (either 32-bit or 64-bit):
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- Remote control requires that a Features on Demand key for remote presence is installed on Converged, NeXtScale, and System x servers. If the FoD key is not detected on a server, the remote-control session displays the `Missing activation key` message for that server when displaying the list of available servers. You can determine whether remote presence is enable, disabled, or not installed on a server from the Servers page (see Viewing the status of a managed server). For more information about FoD keys that are installed on your servers, see Viewing Features on Demand keys.

- The user account that is used to start the remote-control session must be a valid user account that has been defined in the XClarity Administrator authentication server. The user account must also have sufficient user authority to access and manage a server.
- Review the security, performance and keyboard considerations before opening a remote-control session. For more information about these considerations, see Remote control considerations.
- The Remote Control dialog uses the locale and display language settings that are defined for the operating system on your local system.If your local system runs on Windows, see the Java website for information about how to change the locale setting. To change the display language, install a localized copy of Windows or install a language pack from the Windows website.

About this task

You can start multiple remote-control sessions from Lenovo XClarity Administrator. Each session can manage multiple servers.

To open a remote-control session to a server, the server must be in the Online or Normal state. If a server has any other access state, the remote-control session cannot connect to the server. For more information about viewing the server status, see Viewing the details of a managed server.

You can open an untargeted remote-control session by clicking **Provisioning → Remote Control** from the Lenovo XClarity Administrator menu bar. Then, accept any security warnings from your web browser.

Note: For Flex System x280, x480, and x880 compute nodes, you can start a remote-control session to only the primary node. If you attempt to start a remote-control session to a non-primary node in a multi-node system, the remote-control dialog starts, but no video is displayed.

Procedure

Complete the following steps to open a remote-control session to a specific Converged, Flex System, NeXtScale, and System x server.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Select the server to which you want to open a remote-control session.

Step 3. Click the **Remote Control** icon ( ).

Step 4. Accept any security warnings from your web browser.

Step 5. Optionally, choose to save the Remote Control icon to your desktop. You can use this icon to launch a remote-control session without logging in to the XClarity Administrator web interface.

Step 6. When you are prompted, select one of the following connection modes:

- **Single-user mode**. Establishes an exclusive remote-control session with the server. All other remote-control session to that server are blocked until you disconnect from the server. This option is available only if there are no other remote-control sessions established to the server.
- **Multi-user mode**. Allows multiple remote-control sessions to be established with the same server. XClarity Administrator supports up to six concurrent remote-control sessions to a single server.

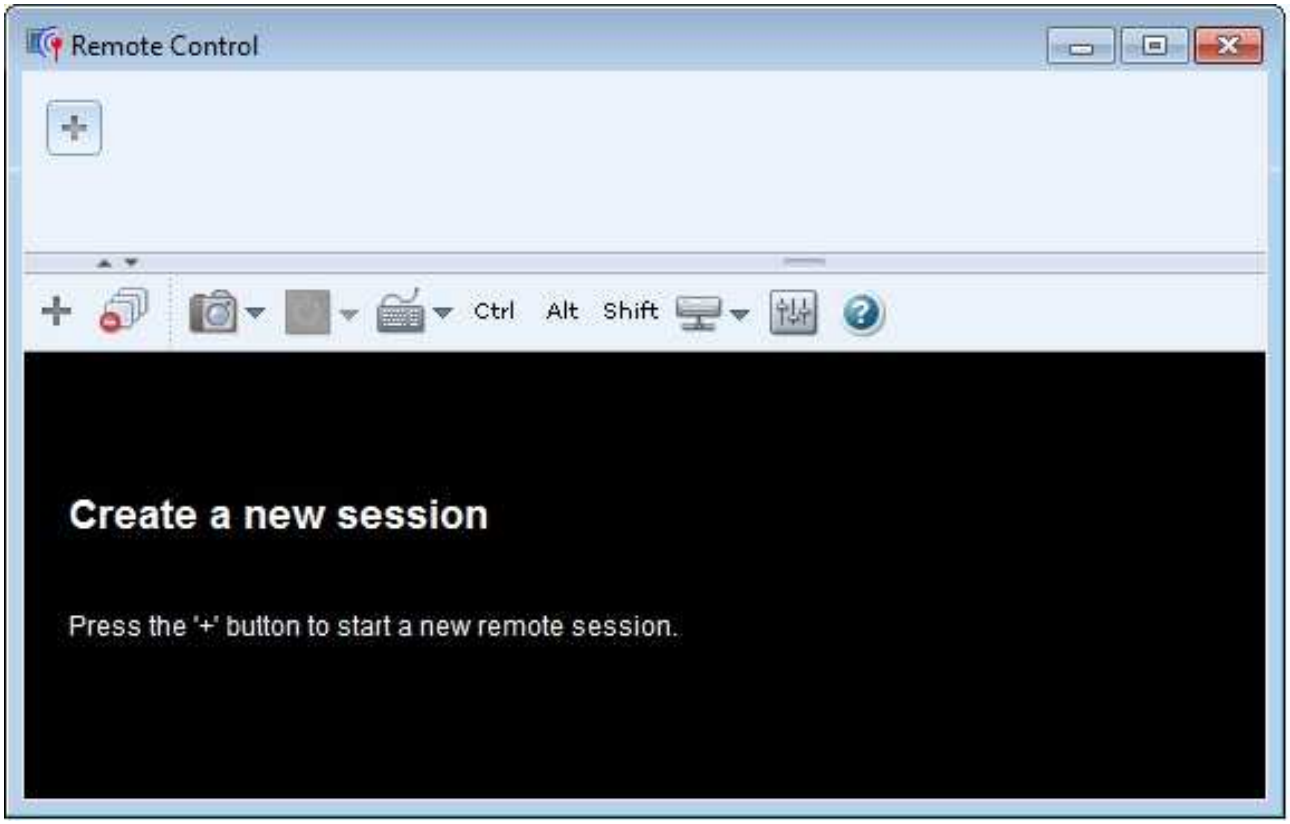
Step 7. When you are prompted, choose whether to save a shortcut to the remote-control session on your local system.

If you save the shortcut, you can then use this shortcut to open a remote-control session to the specified server without having to launch it from the XClarity Administrator web interface. However, your local system must have access to XClarity Administrator to validate the user account with the XClarity Administrator authentication server.

The shortcut contains a link that opens an empty remote-control session to which you can manually add servers.

Results

The Remote Control window is displayed.



The thumbnail area displays thumbnails of all server sessions that are currently managed through the remote-control session.

You can display multiple server sessions and move between server sessions by clicking a thumbnail, which displays the server console in the video session area. If you are accessing more servers than fit in the thumbnail area, click the **Scroll right** icon ( ) and **Scroll left** icon ( ) to scroll to additional server thumbnails. Click the **All sessions** icon ( ) to see a list of all open server sessions.

From the thumbnail area, click the **Add server** icon ( ) to add a new server to the list of servers that you are managing. For more information about adding a session, see Adding a server console to remote-control session. You can control whether the thumbnail area is displayed and how often the thumbnails are refreshed from the Thumbnail page. For more information about thumbnail settings, see Setting remote-control preferences.

After you finish

If the remote-control session does not open successfully, see Remote control issues in the XClarity Administrator online documentation.

From the Remote Control dialog, you can perform the following actions:

- Add a session to other servers to the current remote-control session (see Adding a server console to remote-control session).
- Hide or show the thumbnail area by clicking the **Toggle Thumbnails** icon ( ).
- Display the remote-control session as a window or full screen by clicking the **Screen** icon ( ) and then clicking **Toggle on full screen** or **Toggle off full screen**.
- Use Ctrl, Alt, and Shift keys in a remote-control session (see Using Ctrl, Alt, and Shift keys).
- Define custom key sequences, known as softkeys (seeDefining softkeys).
- Take a screen capture of the currently selected server session, and save that screen capture in a variety of formats by clicking the **Screen** icon ( ), and then clicking **Screenshot**.
- Mount remote media (such as CD, DVD, or USB device, disk image, or CD (ISO) image) to the selected server, or move a mounted device to another server (see Mounting or moving remote media).
- Upload images to a server from remote media (see Uploading an image to the server).
- Power the server on or off from a remote console (see Powering on and off a server from a remote control session).
- Change remote-control preferences (see Setting remote-control preferences).

Remote control considerations

Be aware of security, performance, and keyboard considerations that are related to accessing managed servers using a remote-control session.

Security considerations

The user account that is used to start the remote-control session must be a valid user account that has been defined in the Lenovo XClarity Administrator authentication server. The user account must also have sufficient user authority to access and manage a server.

By default, multiple remote-control sessions can be established to a server. However, when you start a remote-control session, you have the option to start the session in single-user mode, which establishes an exclusive session with the server. All other remote-control sessions to that server are blocked until you disconnect from the server.

Note: This option is available only if there are currently no other remote-control sessions established to the server.

To use Federal Information Processing Standard (FIPS) 140, you must enable it manually by completing the following steps on your local system:

1. Find the provider name of the FIPS 140 certified cryptographic provider that is installed on your local system.

   Tip: For more information about FIPS 140 compliance, see the FIPS 140 Compliant Mode for SunJSSE website.
2. Edit the file `$(java.home)/lib/security/java.security`.

3. Modify the line that includes `com.sun.net.ssl.internal.ssl.Provider` by appending the provider name of your FIPS 140 certified cryptographic provider. For example, change:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
   to:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Performance considerations

If a remote-control session becomes slow or unresponsive, close all video and remote media sessions that you have established with the selected server to reduce the number of open server connections. In addition, you might increase performance by changing the following preferences. For more information, see Setting remote-control preferences.

- **KVM**
  - Decrease the percentage of video bandwidth that is used by the application. The image quality of the remote-control session will be reduced.
  - Decrease the percentage of frames that are refreshed by the application. The refresh rate of the remote-control session will be reduced.
- **Thumbnails**
  - Increase the thumbnail refresh interval rate. The application will refresh thumbnails at a slower rate.
  - Turn off the display of thumbnails completely.

The size of the remote-control session window and the number of active sessions might affect workstation resources, such as memory and network bandwidth, which can influence performance. The remote-control session uses a soft limit of 32 open sessions. If more than 32 sessions are open, performance might be severely degraded, and the remote-control session might become unresponsive. You might see performance degradation with fewer than 32 open sessions if resources, including network bandwidth and local memory, are not sufficient.

Keyboard considerations

The remote-control session supports the following keyboard types:
- Belgian 105-key
- Brazilian
- Chinese
- French 105-key
- German 105-key
- Italian 105-key
- Japanese 109-key
- Korean
- Portuguese
- Russian
- Spanish 105-key
- Swiss 105-key
- UK 105-key
- US 104-key

For information about keyboard preferences, see Setting remote-control preferences.

Adding a server console to remote-control session

You can add one or more servers consoles to the current remote-control session.

Procedure

To add one or more servers consoles to the current remote-control session, complete the following steps.

Step 1. From the Remote Control window, click the **New Session** icon ( ).

A dialog is displayed with a list of available chassis and rack servers that are managed by Lenovo XClarity Administrator and that your user account has permission to manage.

Tip: If no servers are shown in the list, see Remote control issues in the XClarity Administrator online documentation for procedures to potentially resolve the issue.

Step 2. Select one or more servers to which you want to connect.

You can filter the servers that are displayed by selecting a system type from the **Type** drop-down list and entering text (such as a system name or enclosure name) in the **Filter** field.

You can select **Select all** to select all server in the list.

Step 3. Optional: **Optional:** Select **Single-user mode** to open an exclusive session to each selected server.

If you select this option, all other remote-control sessions to the selected servers are blocked until you disconnect from the selected servers. This option is available only if there are no other remote-control sessions established to the selected servers.

If you do not select this option, the multi-user mode is used by default.

Step 4. Click **Connect**.

Powering on and off a server from a remote control session

You can power on and off a server from a remote-control session.

Procedure

Complete the following steps to power on and off a server.

Step 1. From the Remote Control window, click the thumbnail for the server that you want to power on or off.

Step 2. Click the **Power** icon ( ), and then click one of the following power actions:

- **Power on**
- **Power Off Normally**
- **Power Off Immediately**
- **Restart Normally**
- **Restart Immediately**
- **Trigger NMI**
- **Restart to System Setup** (Lenovo Converged, Flex System, NeXtScale, and System x servers only)

Tip: The **Power** icon is green if the server is currently powered on.

Defining softkeys

You can define your own custom key sequences, called *softkeys*, for the current remote-control session.

Before you begin

To display the current list of softkey definitions, click the **Keyboard** icon ( ).

Softkey definitions are stored on the system from which you started the remote-control session. Therefore, if you launch the remote-control session from another system, you have to define the softkeys again.

You can choose to export user settings (which includes softkeys) from the **User Settings** tab on the Preferences dialog. For more information, see Importing and exporting user settings.

Note: If you use an international keyboard and define softkeys that require the Alternate Graphics key (AltGr), ensure that the operating system on the workstation that you use to invoke the remote-control application is the same type of operating system as the one on the server that you are remotely accessing. For example, if the server is running Linux, ensure that you invoke the remote-control session from a workstation that is running Linux.

Procedure

Complete the following procedure to add a softkey.

Step 1. From the Remote Control window, click the **Keyboard** icon ( ), and then click **Add softkey**. The **Softkey Programmer** tab on the Preference dialog is displayed.

Step 2. Click **New**.

Step 3. Type the key sequence that you want to define.

Step 4. Click **OK**. The new softkey is added to the softkey list.

Using Ctrl, Alt, and Shift keys

Some operating systems intercept certain keys instead of passing them to the remote server. You can use the sticky key buttons to send keystrokes directly to the server that you are managing.

Procedure

To send a Ctrl or Alt key combinations, click **Ctrl** or **Alt** in the toolbar, place the cursor in the video session area, and press a key on the keyboard.

For example, to send a Ctrl+Alt+Del key combination, complete the following steps:

1. Click **Ctrl** in the toolbar.
2. Click **Alt** in the toolbar.
3. Left-click anywhere inside the video session area.
4. Press the Delete key on the keyboard.

Note: If mouse-capture mode is enabled, press the left Alt key to move the cursor outside of the video session area. Although mouse-capture mode is disabled by default, you can enable it from the Toolbar page (see Setting remote-control preferences).

When you click **Ctrl**, **Alt**, or **Shift** in the toolbar to make the key active, the key remains active until you press a keyboard key or click the button again.

Mounting or moving remote media

You can use the remote- media feature to mount remote media (such as a CD, DVD, or USB device, disk image, or CD (ISO) image) that is on the local system to the selected server. You can also upload an image to the local storage that is available on the baseboard management-controller (BMC).

Before you begin

Only one user at a time can mount and upload data to the local storage on the management controller. Other users are prevented from accessing the local storage on the management controller while it is mounted or while data is being uploaded to the local storage.

On a server that is running the Linux operating system, mounting more than one ISO image is not supported.

Procedure

Complete the following steps to mount or move remote media.

Step 1. From the Remote Control window, click the **Remote Media** icon ( ).

Step 2. Click one of the following actions:

- **Mount remote media**

  This action makes local media resources available to the currently selected server. A media resource can be mounted to only one server at a time within a single remote-control session.

  When you click **Mount remote media**, the following options are available:

  – **Select an image to be mounted**. The image is available for the currently selected server until you unmount the device or close the remote-control session. Multiple images can be mounted to a single server, and each image can be mounted to multiple servers.

  – **Select a drive, such as a CD, DVD, or USB device, that is to be mounted**. The device is available to the currently selected server until you unmount the drive or close the remote-control session. Multiple devices can be mounted to a single server, but each device can be mounted to only one server at a time.

    Note: If you select a drive, be sure to unmount the drive before you remove media from the drive.

  – **Upload the image to the IMM**. Use this option to store an image in local storage on the management controller for the selected server. The image remains on the management controller even if you end the remote-control session or if the server is restarted.

    You can store approximately 50 MB of data on the management controller.

    You can upload multiple images to the management controller provided that the total space that is used for all images is less than 50 MB.

    Each image that is uploaded to the management controller is automatically mounted to the server. After you have uploaded an image to the management controller, you can also move that uploaded image to the management controller for a different server. When you move the image, the previously uploaded image is removed from the current server and uploaded to a selected server.

- **Move remote media**

  This action moves a previously mounted media resource between servers.

  Complete the following steps to make a resource available to a server:

  1. Select one or more resources.
  2. Click **Add** to move the resources to the **Selected Resources** list.
  3. Click **Mount** to mount the resources for use by the server. The remote-control session defines a device for the resource and maps that device to a mount point for the currently selected server. You have the option to write-protect the mounted media.

Uploading an image to the server

You can upload an image to the local storage that is available on the baseboard management-controller (BMC) for the selected server.

About this task

The image remains on the management controller even if you end the remote-control session or if the server is restarted.

You can store approximately 50 MB of data on the management controller.

You can upload multiple images to the management controller provided that the total space that is used for all images is less than 50 MB.

Each image that is uploaded to the management controller is automatically mounted to the server. After you have uploaded an image to the management controller, you can also move that uploaded image to the management controller for a different server. When you move the image, the previously uploaded image is removed from the current server and uploaded to a selected server.

Procedure

Complete the following steps to upload an image to the server.

Step 1. From the Remote Control window, click the **Remote Media** icon ( ).

Step 2. Click **Mount remote media**.

Step 3. Click **Upload the image to the IMM**.

Importing and exporting user settings

You can choose to import or export user settings for the current remote-control session.

About this task

When you export user settings, all user settings for the current remote-control session are stored in a properties file on your local system. You can copy this properties file to another system and import those settings into the remote-control application to use the settings.

Procedure

Complete the following steps to import or export user settings for the current remote-control session.

Step 1. From the Remote Control window, click the **Preference** icon ( ).

Step 2. Click the **User Settings** tab.

Step 3. Click **Import** to import settings from an exported file, or click **Export** to save the all current user settings in a properties file on the local system.

Setting remote-control preferences

You can modify preference settings for the current remote-control session.

Procedure

Complete the following steps to modify remote-control preferences.

Step 1. To modify the remote control preferences, click the **Preferences** icon ( ). All changes take effect immediately.

- **KVM**
  - **Percentage of Video Bandwidth**. Increasing the bandwidth improves the quality in the appearance of the remote-control session but might affect the performance of the remote-control session.

- **Percentage of Frames Refreshed**. Increasing the frame-refresh percentage increases how often the remote-control session is updated but might affect the performance of the remote-control session.
- **Keyboard type**. Select the type of keyboard that you are using for the remote-control session. The keyboard type that you select must match the keyboard settings in the local system and match the keyboard settings on the remote host.

  Note: If you select an international keyboard and you need to enter key combinations that require the Alternate Graphics key (AltGr), ensure that the operating system on the workstation that you use to invoke the remote-control session is the same type of operating system as the one on the server that you want to remotely access. For example, if the server is running Linux, ensure that you invoke the remote-control application from a workstation that is running Linux.
- **Scale image to window**. Select this option to scale the video image that is received from the server to the size of the video session area.

- **Security**
  - **Prefer single-user mode connections**. Specify whether single-user mode connections is the default choice when connecting to a server. When a connection is made in single-user mode, only one user can be connected to a server at a time. If this box is not selected, the default function is to connect to the server in multi-user mode.
  - **Require (secure) tunneling connections**. Select this option to access a server through the management node. You can use this option to access a server from a client that is not on the same network as the server.

    Note: The remote-control application always attempts to connect directly to the server from the local system where remote control was launched. If you select this option, the remote-control application accesses the server through Lenovo XClarity Administrator if the client workstation cannot access the server directly.
- **Toolbar**

  Note: Click **Restore defaults** to restore all settings on this page to the default settings
  - **Pin the toolbar to the window**. By default, the toolbar is hidden above the remote-control session window and displays only when you move your mouse pointer over it. If you select this option, the toolbar is pinned to the window and is always displayed between the thumbnail panel and the remote-control session window.
  - **Show keyboard buttons**. Specify whether to display the keyboard-button icons (CapsLock, NumLock, and ScrollLock) on the toolbar.
  - **Show power control**. Specify whether to display the power-control options on the toolbar.
  - **Show sticky key buttons**. Specify whether to display the sticky-key button icons (Ctrl, Alt, and Delete) on the toolbar.
  - **Hide local mouse pointer**. Specify whether to display the local mouse pointer when you position the cursor in the server session that is currently displayed in the video session area.
  - **Enable mouse-capture mode**. By default, mouse-capture mode is disabled. This means that you can freely move the cursor in and out of the video session area. If you enable mouse-capture mode, you must press the left Alt key before you can move the cursor out of the video session area. If mouse-capture mode is enabled, you can specify whether to use the Ctrl+Alt keys to exit mouse-capture mode. The default is to use the left Alt key.
  - **Specify toolbar background opacity**. Lowering the opacity percentage displays more of the video session area through the toolbar background.

    Note: This option is available only when the toolbar is not pinned to the window.

- **Thumbnails**
  - **Show thumbnails**. Select this option to show the thumbnail area in the remote-control session.
  - **Specify thumbnail refresh interval**. Decreasing the interval for refreshing thumbnails increases how often the server thumbnails are updated.
- **General**
  - **Debug mode**. Specify whether to set debug mode for the remote-control application. The settings determine the granularity of events that are logged in the log files. By default, only severe events are logged. For more information about log-file locations, see Viewing remote-control logs and traces.
  - **Inherit system appearance settings**. This setting changes the appearance to match color schemes that are configured for the local server (running Windows). You must restart the remote-control application for these settings to take effect.
  - C**reate desktop icon**. This setting creates a desktop icon on your local system so that you can start the remote-control application directly from your system. You must still have access to the management software from your system.
  - **Synchronize with management server**. This setting ensures that the server data that is displayed in the remote-control application matches the server data that is displayed from management software.

Viewing remote-control logs and traces

When you start a remote-control session, log files are created. The types of events that are logged in these files are based on the debug mode, which is set from **General** tab on the Preferences dialog. You can use these log files to resolve issues.

Procedure

Remote-control log files are stored in the following locations.

Operating system	Log directory
Windows 7 and 8	`%USERPROFILE%\lenovo\remoteaccess` For example: `C:\Users\win_user\lenovo\remoteaccess`

For more information about collecting diagnostic files and sending files to Lenovo Support, see Working with service and support in the Lenovo XClarity Administrator online documentation.

Managing access to operating-systems on managed servers

You can manage access to operating systems on the managed servers.

Before you begin

You must have **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** or **lxc-hw-admin** authority to manage and deploy device drivers and to perform power actions on managed servers from the Windows Driver Updates pages.

About this task

Before Lenovo XClarity Administrator can update OS device drivers on a managed system, you must provide information to access the host operating system, including the OS IP address and stored administrator

credential for accessing the host operating system. For more information about updating OS device drivers, see Updating Windows device drivers on managed servers.

XClarity Administrator uses stored credentials to authenticate with the host operating system. For more information about creating stored credentials in XClarity Administrator, see Managing stored credentials.

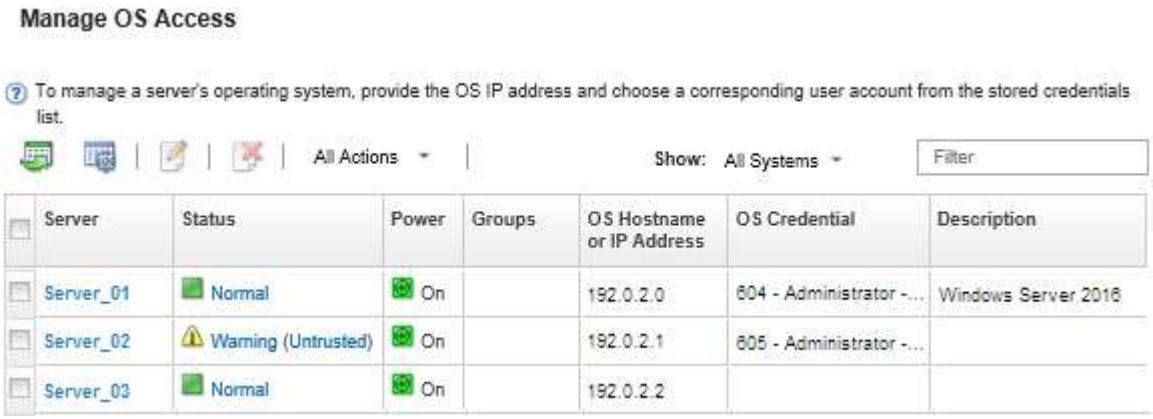
Tip: XClarity Administrator does not automatically validate the information that you specify on this page.

Procedure

Complete the following steps to modify the operating-system properties.

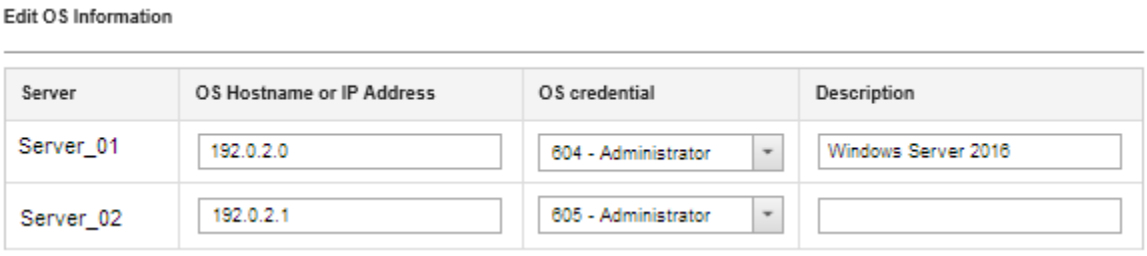
Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Access** to display the Manage OS Access page.

You can sort the table columns to make it easier to find the specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a system name or IP address) in the **Filter** field to further filter the servers that are displayed.



Step 2. Select the servers to be updated.

Step 3. Click **Edit OS information** icon ( ) to display the Edit OS information dialog.



Step 4. For each target server, specify the following information:
- IP address or host name of the host operating system
- (Optional) Stored credential for accessing the host operating system
- (Optional) Description of the host operating system

Step 5. Click **Save**.

After you finish

You can perform the following actions for managing operating-system access.

- Clear operating-system information (IP address, credentials, and description) by selecting the server, and clicking the **Remove OS Information** icon ( ).
- Test the authentication on Windows servers by clicking **Provisioning → Windows Driver Updates: Apply**, selecting the target server, and then clicking **Check Authentication**.
- View deployment information for the operating system on a specific server by hovering over the server name.

  Note: Deployment information is available only for operating systems that were successfully deploying by the XClarity Administrator instance. Deployment information is not available for failed deployments and for deployments there were performed by other means, including another XClarity Administrator instance.

Viewing Features on Demand keys

You can view a list of Features on Demand keys that are currently installed on the managed servers.

About this task

You cannot purchase, install, or manage Features on Demand key from the Lenovo XClarity Administrator web interface. For information about acquiring and installing Features on Demand keys, see Features on Demand in the XClarity Administrator online documentation.

Procedure

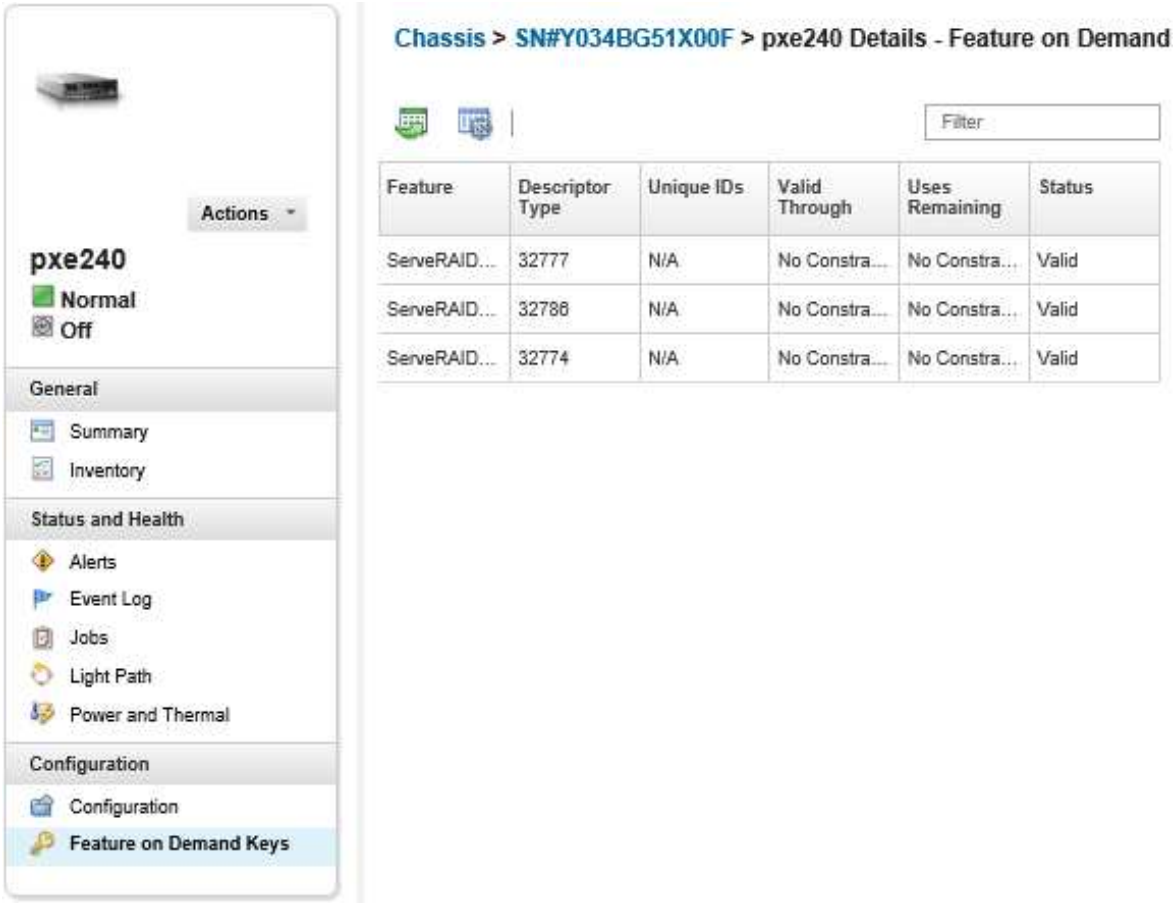
Complete the following steps to display a list of FoD keys that are installed in a specific managed server.

Step 1. From the XClarity Administrator menu, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack and tower servers and compute nodes).

Step 2. Click the server name in the **Server** column. The status summary page for that server is displayed, showing the server properties and a list of components that are installed in that server.

Step 3. Click **Inventory Details** under General in the left navigation, and expand each hardware component section to view the FoD unique IDs for those components.

Step 4. Click **Features on Demand keys** under Configuration in the left navigation to view information about all FoD keys that are installed on the server.



Managing energy and temperature

You can monitor and manage the power consumption and temperature of Converged, NeXtScale, System x, and ThinkServer servers, and improve energy efficiency using Lenovo XClarity Energy Manager.

Learn more: Lenovo XClarity Energy Manager

About this task

XClarity Administrator is a standalone user interface that you can use to monitor and manage the power consumption and temperature of supported servers, including:

- Monitoring energy consumption, estimating the power demand, and reallocating power to servers as needed.
- Monitoring the temperature and cooling capacity of servers.
- Sending notifications when certain events occur or when thresholds are exceeded.
- Limiting the amount of energy that a device consumes using policies.
- Optimizing energy efficiency by monitoring real-time inlet temperatures, identifying low-usage servers based on out-of-band power data, measuring power rangers for different server models, and evaluating how servers accommodate new workloads based on the availability of resources.
- Reducing the power consumption to a minimum level to prolong service time during an emergency power event (such as a data-center power failure).

For more information about how to download, install, and use XClarity Administrator, see Lenovo XClarity Energy Manager website.

Powering on and off a server

You can power on and off a server from Lenovo XClarity Administrator.

Before you begin

- For Red Hat® Enterprise Linux (RHEL) v7 and later, restarting the operating system from a graphical mode suspends the server by default. Before you can perform the **Restart Normally** or **Restart Immediately** actions from XClarity Administrator, you must manually configure the operating system to change the behavior of the power button to power off. For instructions, see the Red Hat Data Migration and Administration Guide: Changing behavior when pressing the power button in graphical target mode.
- For SUSE Linux Enterprise Server (SLES), powering off the operating system requires you to enter the root password on the SLES session. Before you can perform the **Power Off Normally** or **Power Off Immediately** actions from XClarity Administrator, you must manually power off the server using the local SLES interface and select the **Remember authentication** option when you enter the password, or check your security policy to see if mandatory authentication can be disabled.
- When enabled, the Wake-on-LAN boot option can interfere with XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.
- The power action **Restart to System Setup** restarts the server and then opens the BIOS/UEFI Startup utility in a remote-control session rather than a normal operating-system boot.
- The power actions **Power Off Normally** and **Power Off Immediately** depend on the configurations of the operating system that is installed on the device and work only if the operating system is configured to support them.
- You can restart the device with non-maskable interrupt (NMI) by clicking **All Actions → Service → Trigger NMI**.

Procedure

Complete the following procedure to power on or off a server.

Step 1. From the XClarity Administrator menu, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

Step 2. Select the server.

Step 3. Click **All Actions → Power Actions**, and then click one of the following power actions:
- **Power On** powers on the device.
- **Power Off Normally** shuts down the operating system and powers off the device.
- **Power Off Immediately** powers off the device.
- **Restart Normally** shuts down the operating system and restarts the device.
- **Restart Immediately** restarts the device
- **Restart to System Setup** restarts the device to BIOS/UEFI (F1) Setup. This is supported for non-ThinkServer servers that are supported without limitations.
- **Restart Management Controller** restarts the BMC.
- **Restart immediately and attempt PXE Network Boot** restarts the server immediately and boots the server to the Preboot Execution Environment (PXE) network. This is supported for Lenovo Flex System, System x, and ThinkSystem servers.

  Note: PXE-boot related UEFI settings must be configured on the server.

Virtually reseating a server in a Flex System chassis

You can simulate removing and reinserting a server in a Flex System chassis by restarting the server using a non-maskable interrupt (NMI).

About this task

During the virtual reseat, all existing network connections to the server are lost, and the power state of the server changes. Before performing a virtual reseat, ensure that you have saved all user data.

Attention:

- Do not perform a virtual reseat unless you are instructed by Lenovo Support.
- Performing a virtual reseat might result in the loss of data. Before reseating the server, perform necessary operations to protect user data.
- Instead of performing a virtual reseat, consider powering off the server. For information about power actions, see Powering on and off a server).

Procedure

Complete the following steps to virtually reseat a server in a Flex System chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers.

You can sort the table columns to make it easier to find the server that you want to reseat. In addition, you can select a device type from the **All Devices** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Select the server in the table.

Step 3. Click **All Actions → Service → Virtual Reseat**.

Step 4. Click **Virtual Reseat**.

Launching the management controller interface for a server

You can launch the management controller web interface for a specific server from Lenovo XClarity Administrator.

Before you begin

To access ThinkSystem SR635 SR655 servers through XClarity Administrator, a user must have **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin**, or **lxc-os-admin** authority (see Managing the authentication server).

When using single sign-on, you can launch the management interface for a managed servers from XClarity Administrator without having the log in. Single sign-on is supported for ThinkSystem and ThinkAgile servers (except SR635 and SR655). ThinkSystem SR645 and SR665 servers require XCC firmware 21A or later.

To login directly to the XCC using local or external LDAP user accounts without logging in to the XClarity Administrator, use the URL `https://{XCC_IP_adderss}/#/login`.

Procedure

Complete the following steps to launch the management controller interface for a server.

Note: Launching any management controller interface from Lenovo XClarity Administrator using the Safari web browser is not supported.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Servers** to display the Servers page.

You can sort the table columns to make it easier to find specific servers. In addition, you can select a system type from the **All Systems** drop-down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Click the link for the server in the **Server** column. The status summary page for that server is displayed.

Step 3. Click **All Actions → Launch → Management Web Interface**. The management controller web interface for the server is started.

Tip: You can also click the IP address in the **IP Addresses** column to launch the management controller interface.

Step 4. Log in to the management controller interface using your XClarity Administrator user credentials.

After you finish

For more information about using the management controller interface for a server, see Integrated Management Module II online documentation and XClarity Controller online documentation.

Modifying the system properties for a server

You can modify the system properties for a specific server.

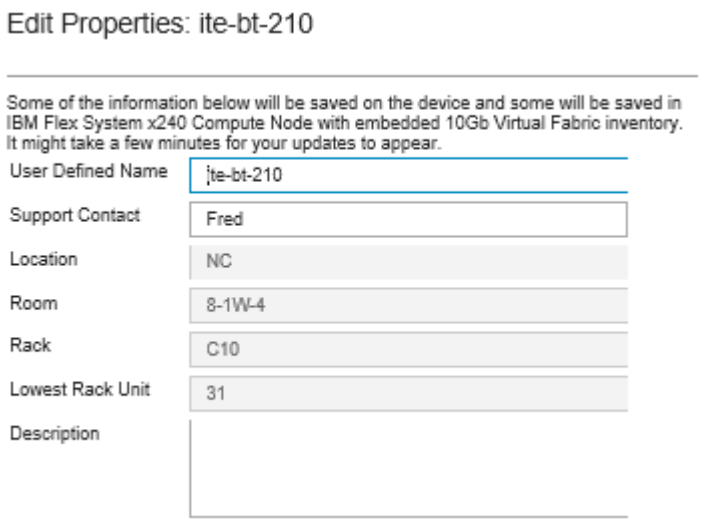
Procedure

Complete the following steps to modify the system properties.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Servers** to display the Servers page.

Step 2. Select the server to be updated.

Step 3. Click **All Actions → Inventory → Edit Properties** to display the Edit dialog.



Step 4. Change the following information, as needed.
- User-defined name for the server
- Support contact
- Description

Note: The location, room, rack, and lowest rack unit properties are updated by XClarity Administrator when you add or remove devices from a rack in the web interface (see Managing racks).

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface.

Resolving expired or invalid stored credentials for a server

When a stored credential becomes expired or inoperable on a device, the status for that device is shown as “Offline.”

Procedure

To resolve expired or invalid stored credentials for a server.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

Step 2. Click the **Power** table column header to group all offline server at the top of the table.

In addition, you can select a system type from the All Systems drop-down list and enter text (such as a system name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 3. Select the server to be resolved.

Step 4. Click **All Actions → Security → Edit Stored Credentials**.

Step 5. Change the password for the stored credential or select another stored credential to use for the managed device.

Note: If you managed more than one device using the same stored credentials and you change the password for the stored credentials, that password change affects all devices that are currently using the stored credentials.

Recovering a failed server after deploying a server pattern

If a server fails after you deploy a server pattern, you can recover the server by unassigning the profile from the failed server and then reassigning that profile to a standby server.

Procedure

Complete the following steps to recover the failed server that uses Lenovo XClarity Administrator managed authentication.

Step 1. Identify the failed server.

Step 2. Unassign the server profile from the failed server (see Deactivating a server profile).

Attention: The failed server must be powered off to deactivate the assigned virtual addresses *before* you re-assign the profile. When you unassign the server profile, select **Power off server** on the Unassign Server Profile dialog to power off the failed server (see Powering on and off a server).

Step 3. Assign the server profile to a standby server (see Activating a server profile).

Step 4. Activate the profile by either powering on the standby server if it is currently powered off or by restarting the standby server if it is currently powered on (see Powering on and off a server).

Step 5. Migrate the VLAN settings on the attached switches to the standby server.

Step 6. Ensure that the failed server is powered off.

Step 7. Replace or repair the failed server. If you repair the server, perform the following steps to ensure that the newly repaired server is reset to default settings:

a. Reset the BMC to factory defaults by using the management web interface for the server. For information about resetting the BMC, see Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by resetting the management controller.
b. Clear the Unified Extensible Firmware Interface (UEFI) information, including any I/O adapter virtual addresses by using the UEFI menus. For information, see the UEFI documentation.

Recovering boot settings after server pattern deployment

If one or more servers do not start after you deployed a new server pattern to those servers, the problem might be that the boot settings were overwritten with the default boot settings that are in the server pattern. For operating systems that are installed in UEFI mode, restoring the default settings might require additional configuration steps to restore the boot configuration.

Procedure

Complete the following manual recovery procedure for each affected server to restore the original boot settings.

- For a server with Red Hat Enterprise Linux installed:
  1. If you are accessing the server remotely, establish a remote-control session to the server (see Using remote control to manage Converged, Flex System, NeXtScale, and System x servers).
  2. Restart the server by clicking **Tools → Power → On**. When the UEFI splash screen for the server is displayed in the Remote Control session, press F1 to display the Setup Utility.
  3. Select **Boot Manager**.
  4. Select **Add Boot Option**.
  5. Select **UEFI Full Path Option**.
  6. From the list that is displayed, select the entry that includes `SAS`.
  7. Select **EFI**.
  8. Select **redhat**.
  9. Select **grub.efi**.
  10. Select the **Input the Description** field.
  11. Type `Red Hat Enterprise Linux`.
  12. Select **Commit Changes**.
  13. Make `Red Hat Enterprise Linux` the first option in the Boot Order, and remove all other options in the Boot Order.
  14. Press Escape, and then select **Save changes then exit this menu**.
  15. Press Escape, and then select **Exit the Configuration Utility and Reboot**. The compute node restarts.
- For a server with Microsoft Windows Server 2008 installed:
  1. Power on the server, and when prompted, press F1 to enter setup.
  2. Select **Boot Manager**.
  3. Select **Boot from File**.
  4. Select the GUID Partition Tables (GPT) System Partition where you installed Microsoft Windows Server 2008.
  5. Select **EFI**.
  6. Select **Microsoft**.

7. Select **Boot**.
8. Select **bootmgfw.EFI**.

Note: For more information, see RETAIN tip 5079636.

Recovering rack or tower server management after a management server failure

If a rack or tower server is being managed by Lenovo XClarity Administrator, and if XClarity Administrator fails, you can restore the management functions until the XClarity Administrator is restored or replaced.

About this task

To recover management for a Flex System server, see Recovering management with a CMM after a management server failure.

Recovering rack or tower server management after a management server failure by force management

You can recover server management by managing the server again using the force-management option

Procedure

If the replacement Lenovo XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the `RECOVERY_ID` account and password and the **Force management** option (see Managing servers).

Recovering a System x or NeXtScale M4 server that was not unmanaged correctly by using the management controller

You can recover management of a System x or NeXtScale M4 server by using the baseboard management-controller (BMC).

Procedure

Complete the following steps to recover server management. of a server that uses Lenovo XClarity Administrator managed authentication.

Step 1. Log in to the management-controller web interface using the user account and password that you created before the server was managed by XClarity Administrator

Step 2. Clear SNMP trap settings.

a. Click the **IMM Management → Network**.

b. Click the **SNMP** tab.

c. Click the **Communities** tab,

d. Locate the community entry for the previous XClarity Administrator, fox example.
- **LXCA IP address:** 10.240.198.84
- **LXCA host:** LXCA_maqCBIt86d
- **Community 2:**
- **Community name:** LXCA_maqCBIt86d
- **Access type:** Trap
- **Allow specific hosts to receive traps on this community:** 10.240.198.84

e. Remove the value in the fields for the community entry.

f. Click **Apply**.

Step 3. Clear the user accounts.

a. Click the **IMM Management → Users**.

b. Click the **User Accounts** tab.

c. Delete all user accounts that are XClarity Administrator, including user accounts with the following prefixes:
- DISABLE_*
- LXCA_*
- OBSOLETE_*
- SNMPCFGUSER

After you finish

After XClarity Administrator is restored or replaced, you can manage the System x or NeXtScale server again (see Managing servers). All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by resetting the management controller

You can recover management of a ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server by resetting the baseboard management-controller in the server to factory defaults.

Procedure

Complete the following steps to recover management of a server that uses Lenovo XClarity Administrator managed authentication.

Step 1. If Encapsulation is enabled on the device, connect to the target management controller from a system that is configured to use the IP address of the failed XClarity Administrator virtual appliance.

Step 2. Reset the management controller to the factory defaults.

a. Log in to the management controller web interface for the server using the recovery user account and password that you created before the server was managed by XClarity Administrator.

b. Click the **IMM Management tab**.

c. Click **IMM Reset to factory defaults**.

d. Click **OK** to confirm the reset action.

Important: After the BMC configuration is complete, the BMC is restarted. If this is a local server, your TCP/IP connection is broken and you must reconfigure the network interface to restore connectivity.

Step 3. Log on to the management controller web interface for the server again.

- The BMC is initially configured to attempt to obtain an IP address from a DHCP server. If it cannot, it uses the static IPv4 address `192.168.70.125`.
- The IMMBMC is set initially with a user name of `USERID` and password of `PASSWORD` (with a zero). This default user account has Supervisor access. Change this user name and password during your initial configuration for enhanced security.

Step 4. Reconfigure the network interface to restore connectivity. For more information, see the Integrated Management Module II online documentation.

After you finish

After XClarity Administrator is restored or replaced, you can manage the server again (see Managing servers). All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

If the server was configured using Configuration Patterns, you can deactivate and then re-activate the server profile that was assigned to the server to apply the configuration (see Working with server profiles).

Recovering ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management after a management server failure by using cimcli

You can recover management of a ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server by using the **cimcli** utility to clear the CIM subscriptions.

Before you begin

OpenPegasus with the cimcli utility must be installed on a system that has network access to the target server. For information about downloading, configuring, and compiling OpenPegasus, see the OpenPegasus Release RPMs for Linux website.

Note: For Red Hat Enterprise Linux (RHEL) Server 7 and later, OpenPegasus source and binary RPMs are included as part of the Red Hat distribution. The `top-pegasus-test.x86_64` package includes the cimcli utility.

About this task

After the server is recovered, you can manage the server again. All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

Procedure

Complete the following steps from a server that uses Lenovo XClarity Administrator managed authentication and on which OpenPegasus is installed to recover server management.

Step 1. If Encapsulation is enabled on the device:

a. Connect to the target server from a system that is configured to use the IP address of the failed XClarity Administrator virtual appliance.

b. Disable Encapsulation by opening an SSH session to the device and running the following command:

```
encaps lite off
```

Step 2. Run the following commands to determine the CIM instances for CIM_ListenerDestinationCIMXML, CIM_Indicationfilter and CIM_IndicationSubscription.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

where, <*IP_address*>, <*user_ID*> and <*password*> are the IP address, user ID and password for the management controller. For example:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
```

```
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Step 3. Run following command to delete each the CIM instance for CIM_ListenerDestinationCIMXML, CIM_Indicationfilter and CIM_IndicationSubscription, one at a time.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

where, <*IP_address*>, <*user_ID*> and <*password*> are the IP address, user ID and password for the management controller, and <*cim_instance*> is the information returned for each CIM instance in the previous step, surrounded by single quotes. For example:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

After you finish

After Lenovo XClarity Administrator is restored or replaced, you can manage the System x or NeXtScale server again (see Managing servers). All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

Recovering ThinkServer server management after a management server failure by using the management controller interface

You can recover management of a ThinkServer server from the management controller interface.

Procedure

Complete the following steps to recover the server management.

Step 1. Log in to the management controller web interface for the server as an administrator (see Launching the management controller interface for a server).

Step 2. Remove the IPMI accounts created by Lenovo XClarity Administrator by selecting Users in the main menu and then removing all the user accounts with the “LXCA_” prefix.

Alternatively, you can rename the account user name, and remove the “LXCA_” prefix.

Step 3. Remove SNMP trap destinations by selecting **PEF Management** in the main menu, click the **LAN Destination** tab, and remove the entry that points to the IP address of the XClarity Administrator instance.

Step 4. Verify you have valid NTP settings by selecting **NTP Settings** in the main menu, and then either configuring the date and time manually or providing a valid NTP server address.

Unmanaging a rack or tower server

You can remove a rack or tower server from management by Lenovo XClarity Administrator. This process is called *unmanaging*.

Before you begin

You can enable XClarity Administrator to automatically unmanage devices that are offline for a specific amount of time. This is disabled by default. To enable the automatic unmanagment of offline devices, click **Hardware → Discover and Manage New Devices** from the XClarity Administrator menu, and then click **Edit** next to **Unmanage offline devices is Disabled**. Then, select **Enable unmanage offline devices** and set the time interval. By default, devices are unmanaged after being offline for 24 hours.

Before you unmanage a rack or tower server, ensure that there are no active jobs running against the server.

If you want to remove the server pattern and any virtual addresses on the rack or tower server, deactivate the server profile before unmanaging the server (see Deactivating a server profile).

When Call Home is enabled in XClarity Administrator, Call Home is disabled on all managed chassis and servers to avoid duplicate problem records from being created. If you intend to discontinue using XClarity Administrator to manage your devices, you can re-enable Call Home on all managed devices from the XClarity Administrator in lieu of re-enabling Call Home for each individual device at a later time (see Re-enabling call home on all managed devices in the XClarity Administrator online documentation).

About this task

When you unmanage a rack or tower server, Lenovo XClarity Administrator performs the following actions:

- Clears the configuration used for centralized user management.
- Removes the baseboard-management-controller security certificate from the XClarity Administrator trust store.
- If Encapsulation is enabled on the device, configures the devices firewall rules to the settings before the device was managed.

- Removes the CIM subscriptions to the XClarity Administrator configuration so that XClarity Administrator no longer receives events from the rack or tower server.
- Disables Call Home on the rack or tower server if Call Home is currently enabled on XClarity Administrator.
- Discards events that were sent from the rack or tower server. You can retain these events by forwarding the events to an external repository, such as a syslog (see Forwarding events).

When you unmanaged a rack or tower server, XClarity Administrator retains certain information about the server. That information is reapplied when you manage the same rack or tower server again.

Important: If you unmanaged a ThinkServer server and then manage that server using another XClarity Administrator instance, information about the server is lost.

Tip: All demo devices that are optionally added during initial setup are nodes in a chassis. To unmanage the demo devices, unmanage the chassis using the **Force unmanage even if the device is not reachable** option.

Procedure

To umanage a rack or tower server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click the **Hardware → Servers** to display the Servers page.

Step 2. Select one or more rack or tower servers to be unmanaged.

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

Step 4. Optional: **Optional:** Select **Force unmanage even if the device is not reachable**.

Important: When unmanaging demo hardware, ensure that you select this option.

Step 5. Click **Unmanage**.The Unmanage dialog shows the progress of each step in the unmanagement process.

Step 6. When the unmanagement process is complete, click **OK**.

Recovering a rack or tower server that was not unmanaged correctly

If a Converged, NeXtScale, System x, or ThinkServer server was not unmanaged correctly, you must recover the server before you can remanage it.

Recovering a rack or tower server that was not unmanaged correctly by force management

You can recover server management by managing the server again using the force-management option

Procedure

If the replacement Lenovo XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the `RECOVERY_ID` account and password and the **Force management** option (see Managing servers).

Recovering a System x or NeXtScale M4 server that was not unmanaged correctly by using the management controller

You can recover System x or NeXtScale M4 server management by using the management controller.

Procedure

Complete the following steps to recover server management.

Step 1. Log in to the management-controller web interface using the user account and password that you created before the server was managed by XClarity Administrator

Step 2. Clear SNMP trap settings.

a. Click the **IMM Management → Network**.

b. Click the **SNMP** tab.

c. Click the **Communities** tab,

d. Locate the community entry for the previous XClarity Administrator, fox example.
- **LXCA IP address:** 10.240.198.84
- **LXCA host:** LXCA_maqCBIt86d
- **Community 2:**
- **Community name:** LXCA_maqCBIt86d
- **Access type:** Trap
- **Allow specific hosts to receive traps on this community:** 10.240.198.84

e. Remove the value in the fields for the community entry.

f. Click **Apply**.

Step 3. Clear the user accounts.

a. Click the **IMM Management → Users**.

b. Click the **User Accounts** tab.

c. Delete all user accounts that are XClarity Administrator, including user accounts with the following prefixes:
- DISABLE_*
- LXCA_*
- OBSOLETE_*
- SNMPCFGUSER

Step 4. Manage the server using Lenovo XClarity Administrator.

a. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.

b. Select **Manual Input**.

c. Click **Single System**, enter the IP address of the server that you want to manage, and click **OK**.

d. Specify the user ID and password for the authenticating to the server.

e. Click **Manage**.

A dialog is displayed that shows the progress of this management process. Monitor the progress to ensure that the process completes successfully.

f. When the process is complete, click **OK**.

Recovering a ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server that was not unmanaged correctly by resetting the management controller to factory defaults

You can recover ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server management by resetting the baseboard management-controller (BMC) in the server to factory defaults.

Procedure

Complete the following steps to recover server management.

Step 1. If Encapsulation is enabled on the device, connect to the target management controller from a system that is configured to use the IP address of the failed XClarity Administrator virtual appliance.

Step 2. Reset the management controller to the factory defaults.

a. Log in to the management controller web interface for the server using the recovery user account and password that you created before the server was managed by XClarity Administrator.

b. Click the **IMM Management tab**.

c. Click **IMM Reset to factory defaults**.

d. Click **OK** to confirm the reset action.

Important: After the BMC configuration is complete, the BMC is restarted. If this is a local server, your TCP/IP connection is broken and you must reconfigure the network interface to restore connectivity.

Step 3. Log on to the management controller web interface for the server again.

- The BMC is initially configured to attempt to obtain an IP address from a DHCP server. If it cannot, it uses the static IPv4 address `192.168.70.125`.
- The IMMBMC is set initially with a user name of `USERID` and password of `PASSWORD` (with a zero). This default user account has Supervisor access. Change this user name and password during your initial configuration for enhanced security.

Step 4. Reconfigure the network interface to restore connectivity. For more information, see the Integrated Management Module II online documentation.

Step 5. Manage the server using Lenovo XClarity Administrator.

a. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.

b. Select **Manual Input**.

c. Click **Single System**, enter the IP address of the server that you want to manage, and click **OK**.

d. Specify the user ID and password for the authenticating to the server.

e. Click **Manage**.

A dialog is displayed that shows the progress of this management process. Monitor the progress to ensure that the process completes successfully.

f. When the process is complete, click **OK**.

Step 6. If the server was configured using Configuration Patterns, re-activate the server profile that was assigned to the server.

a. From the XClarity Administrator menu bar, click **Provisioning → Server Profiles**. The Configuration Patterns: Server Profiles page is displayed.

b. Select the server profile, and click the **Deactivate server profile** icon ( ).

c. Click **Power off the ITE** to power off the server. When the server is powered back on, virtual address assignments revert back to the burned in defaults.

d. Click **Deactivate**. The state of the profile changes to “Inactive” in the Profile Status column. Note: Servers retain their identification information (for example, hostname, IP address, virtual MAC address) when a profile is deactivated.

e. Select the server profile again, and click the **Activate server profile** icon ( ).

f. Click **Activate** to activate the server profiles on the server. The state of the profile changes to “Active” in the Profile Status column.

Step 7. If a compliance policy was assigned to the server, reassign the compliance policy.

a. From the XClarity Administrator menu bar, click **Provisioning → Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed with a list of managed devices.

b. Select the appropriate policy for the server from the drop-down menu in the **Assigned Policy** column.

Recovering a ThinkSystem, Converged, NeXtScale, or System x M5 or M6 server that was not unmanaged correctly by using the cimcli

You can recover ThinkSystem, Converged, NeXtScale, or System x server management by using the **cimcli** to clear the CIM subscriptions.

Before you begin

OpenPegasus with the cimcli utility must be installed on a system that has network access to the target server. For information about downloading, configuring, and compiling OpenPegasus, see the OpenPegasus Release RPMs for Linux website.

Note: For Red Hat Enterprise Linux (RHEL) Server 7 and later, OpenPegasus source and binary RPMs are included as part of the Red Hat distribution. The `top-pegasus-test.x86_64` package includes the cimcli utility.

About this task

After the server is recovered, you can manage the server again. All information about the server (such as network settings, server policies, and firmware compliance policies) is retained.

Procedure

Complete the following steps from a server that uses Lenovo XClarity Administrator managed authentication and on which OpenPegasus is installed to recover server management.

Step 1. If Encapsulation is enabled on the device:

a. Connect to the target server from a system that is configured to use the IP address of the failed XClarity Administrator virtual appliance.

b. Disable Encapsulation by opening an SSH session to the device and running the following command:

```
encaps lite off
```

Step 2. Run the following commands to determine the CIM instances for CIM_ListenerDestinationCIMXML, CIM_Indicationfilter and CIM_IndicationSubscription.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

where, <*IP_address*>, <*user_ID*> and <*password*> are the IP address, user ID and password for the management controller. For example:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"
```

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Step 3. Run following command to delete each the CIM instance for CIM_ListenerDestinationCIMXML, CIM_Indicationfilter and CIM_IndicationSubscription, one at a time.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

where, <*IP_address*>, <*user_ID*> and <*password*> are the IP address, user ID and password for the management controller, and <*cim_instance*> is the information returned for each CIM instance in the previous step, surrounded by single quotes. For example:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Step 4. Manage the server using Lenovo XClarity Administrator.

a. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.

b. Select **Manual Input**.

c. Click **Single System**, enter the IP address of the server that you want to manage, and click **OK**.

d. Specify the user ID and password for the authenticating to the server.

e. Click **Manage**.

   A dialog is displayed that shows the progress of this management process. Monitor the progress to ensure that the process completes successfully.

f. When the process is complete, click **OK**.

Recovering a ThinkServer server management that was not unmanaged correctly by using the management controller interface

You can recover management of a ThinkServer server by using the management controller web interface.

Procedure

Complete the following steps to recover the server management.

Step 1. Log in to the management controller web interface for the server as an administrator (see Launching the management controller interface for a server).

Step 2. Remove the IPMI accounts created by Lenovo XClarity Administrator by selecting Users in the main menu and then removing all the user accounts with the “LXCA_” prefix.

Alternatively, you can rename the account user name, and remove the “LXCA_” prefix.

Step 3. Remove SNMP trap destinations by selecting **PEF Management** in the main menu, click the **LAN Destination** tab, and remove the entry that points to the IP address of the XClarity Administrator instance.

Step 4. Verify you have valid NTP settings by selecting **NTP Settings** in the main menu, and then either configuring the date and time manually or providing a valid NTP server address.

Chapter 9. Managing storage devices

Lenovo XClarity Administrator can manage several types of storage devices, including Lenovo Storage, Flex System storage systems, and tape libraries.

Learn more: XClarity Administrator: Discovery

Before you begin

Attention: Review the Storage management considerations before managing a storage device.

Note: Flex System storage devices are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed Flex System storage devices independent of the chassis.

Certain ports must be available to communicate with devices. Ensure that all required ports are available before you attempt to manage storage devices. For information about ports, see Port availability in the XClarity Administrator online documentation.

Ensure that the minimum required firmware is installed on each storage device that you want to manage using XClarity Administrator. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.

Important: Ensure that the following requirements are met before discovering and managing rack storage devices (other than ThinkSystem DE series). For more information, see Cannot discover a device and Cannot manage a device in the XClarity Administrator online documentation.

- The network configuration must allow SLP traffic between XClarity Administrator and the rack storage device.
- Unicast SLP is required.
- Multicast SLP is required if you want XClarity Administrator to discover the Lenovo Storage devices automatically. In addition, SLP must be enabled on the rack storage device.

About this task

XClarity Administrator can automatically discover storage devices in your environment by probing for manageable devices that are on the same IP subnet as XClarity Administrator. To discover storage devices that are in other subnets, specify an IP address or range of IP addresses, or import information from a spreadsheet.

After the storage devices are managed by XClarity Administrator, XClarity Administrator polls each managed storage device periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed storage device and perform management actions (such as configuring system settings, updating firmware, and powering on and off).

A device can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device on the initial XClarity Administrator, and then manage it with the new XClarity Administrator. If an error occurs during the unmanagement process, you can select the **Force management** option during management on the new XClarity Administrator.

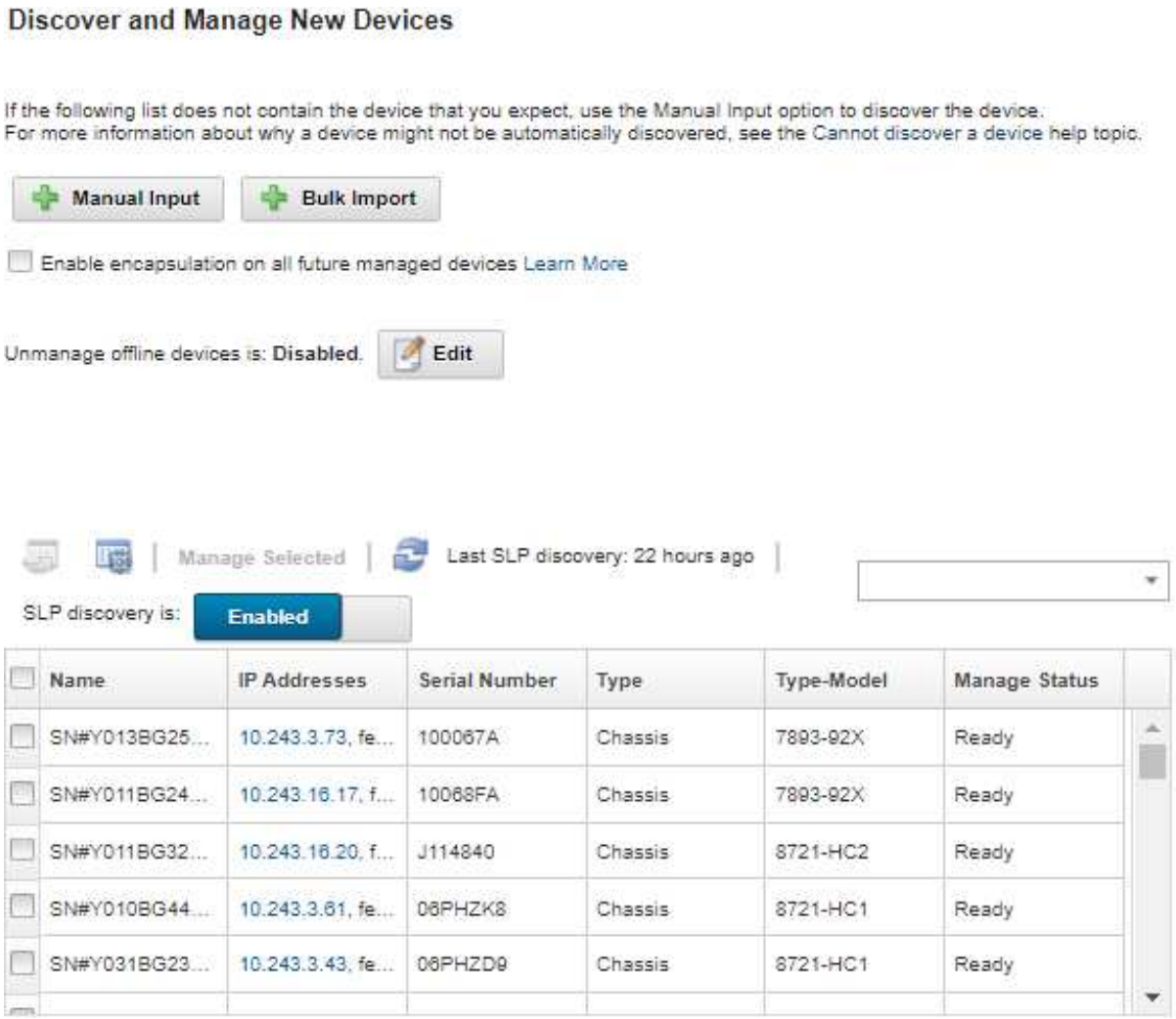
© Copyright Lenovo 2015, 2022

Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a device is already managed by another manager until after it attempts to manage the device.

Procedure

Complete one of the following procedures to manage storage devices using XClarity Administrator.

- Discover and manage a large number of storage devices and other types of devices using a bulk-import file (see Managing systems in the XClarity Administrator online documentation).
- Discover and manage storage devices that are on the same IP subnet as XClarity Administrator.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage New Devices page is displayed.



     You can sort the table columns to make it easier to find the storage devices that you want to manage. In addition, you can enter text (such as a name or IP address) in the **Filter** field to further filter the storage systems that are displayed. You can change the columns that are displayed and the default sort order by clicking the **Customize Columns** icon ( ).
  2. Click the **Refresh** icon ( ) to discover all manageable devices in the XClarity Administrator domain. Discovery might take several minutes.
  3. Select one or more storage devices that you want to manage.

4. Click **Manage Selected**. The Manage dialog is displayed.
5. Specify the user ID and password for authenticating to the storage device.

   Tip: It is recommended to use a supervisor or administrator account to manage the device. If an account with lower-level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).
6. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   – You can select from a list of role groups that are assigned to the current user.

   – If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.
7. Click **Manage**.

   A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.
8. When the process is complete, click **OK**.

   The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

   If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

   – If the managing XClarity Administrator failed and cannot be recovered.

     Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

   – If the managing XClarity Administrator was taken down before the devices were unmanaged.

   – If the devices were not unmanaged successfully.

   Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

- Discover and manage storage devices that are not on the same IP subnet as XClarity Administrator by manually specifying IP addresses.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Select **Manual Input**.
  3. Specify the network addresses of the storage devices that you want to manage:

     – Click **Single System**, and enter a single IP address domain name, or fully-qualified domain name (FQDN).

       Note: To specify an FQDN, ensure that a valid domain name is specified on Network Access page (see Configuring network access).

     – Click **Multiple Systems**, and enter a range of IP addresses. To add another range, click the **Add** icon (). To remove a range, click the **Remove** icon ().
  4. Click **OK**.

5. Specify the user ID and password for authenticating to the storage device.

   Tip: It is recommended to use a supervisor or administrator account to manage the device. If an account with lower-level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

6. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   – You can select from a list of role groups that are assigned to the current user.

   – If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

7. Click **Manage**.

   A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the progress.

8. When the process is complete, click **OK**.

   The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

   If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

   – If the managing XClarity Administrator failed and cannot be recovered.

     Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

   – If the managing XClarity Administrator was taken down before the devices were unmanaged.

   – If the devices were not unmanaged successfully.

   Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

After you finish

- Discover and manage additional devices.
- Update firmware on devices that are not in compliance with current policies (see Updating firmware on managed devices).
- Add the new devices to the appropriate rack to reflect the physical environment (see Managing racks).
- Monitor hardware status and details (see Viewing the status of storage devices).
- Monitor events and alerts (see Working with events and Working with alerts).

Storage management considerations

Before managing a storage device, review the following important considerations.

For information about port requirements, see Port availability in the Lenovo XClarity Administrator online documentation.

Important: Ensure that the following requirements are met before discovering and managing rack storage devices (other than ThinkSystem DE series). For more information, see Cannot discover a device and Cannot manage a device in the XClarity Administrator online documentation.

- The network configuration must allow SLP traffic between XClarity Administrator and the rack storage device.
- Unicast SLP is required.
- Multicast SLP is required if you want XClarity Administrator to discover the Lenovo Storage devices automatically. In addition, SLP must be enabled on the rack storage device.

For Lenovo Storage devices, the system-level air temp is measured by the temperature sensor closest to the mid-plane of the system and reflects the ambient temperature after the airflow passes through the drives. Note that the air temperature that is reported by XClarity Administrator and the management controller might differ if the temperature is captured at different points in time.

For Lenovo DE Series storage devices, both management controllers must be reachable on the network during initial management.

For some storage devices, SNMP traps are in English only.

Viewing the status of storage devices

You can view a summary and detailed status for the managed storage devices from Lenovo XClarity Administrator.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

The following status icons are used to indicate the overall health of the device. If the certificates do not match, “(Untrusted)” is appended to the status of each applicable device, for example Warning (Untrusted). If there is a connectivity issue or a connection to the device is not trusted, “(Connectivity)” is appended to the status of each applicable device, for example Warning (Connectivity).

- ( ) Critical
- ( ) Warning
- ( ) Pending
- ( ) Informational
- ( ) Normal
- ( ) Offline
- ( ) Unknown

Procedure

To view the status for a managed storage device, complete one or more of the following actions.

- From the Lenovo XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of all managed storage devices and other resources.

- From the Lenovo XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all storage devices that are installed in managed chassis.

  You can sort the table columns to make it easier to find the storage devices that you want to manage. In addition, enter text (such as a system name or IP address) in the **Filter** field and click the status icons to list only those storage devices that meet the selected criteria.

  From this page, you can perform the following actions:

  - View detailed information about the storage device and its components (see Viewing the details of a storage device).
  - View a storage device in graphical rack or chassis view by clicking **All Actions → Views → Show in Rack View** or **All Actions → Views → Show in Chassis View**.
  - Launch the management controller web interface for the storage device by clicking the **IP address** link (see Launching the management controller interface for a storage device).

- Power the storage controller in the storage device on and off (see Powering on and off a storage device).
- Modify system information by selecting a storage device and clicking **All Actions → Inventory → Edit Properties**.
- Refresh inventory by selecting a storage device and clicking **All Actions → Inventory → Refresh Inventory**.
- Export detailed information about one or more storage devices to a single CSV file by selecting the storage devices and clicking **All Actions → Inventory → Export Inventory**.

  Note: You can export inventory data for a maximum of 60 devices at one time.

  Tip: When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Unmanaged the storage device (see Unmanaging a storage device).
- (Flex System storage devices only) Virtually reseat the storage controller in the storage device (see Virtually reseating storage controllers in a Flex System storage device).
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Exclude events** icon ( ). (see Excluding events).
- Resolve issues that might arise between the Lenovo XClarity Administrator security certificate and the security certificate of the CMM in the chassis where the storage device is installed by selecting a storage device and clicking **All Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).
- Add or remove a storage device from a static resource group by clicking **All Actions → Groups → Add to Group** or **All Actions → Groups → Remove from Group**.

Viewing the details of a storage device

You can view detailed information about managed storage devices from Lenovo XClarity Administrator, including the IP address, product name, serial number, and details about each canister.

About this task

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

For Lenovo Storage devices, the system-level air temp is measured by the temperature sensor closest to the mid-plane of the system and reflects the ambient temperature after the airflow passes through the drives. Note that the air temperature that is reported by XClarity Administrator and the management controller might differ if the temperature is captured at different points in time.

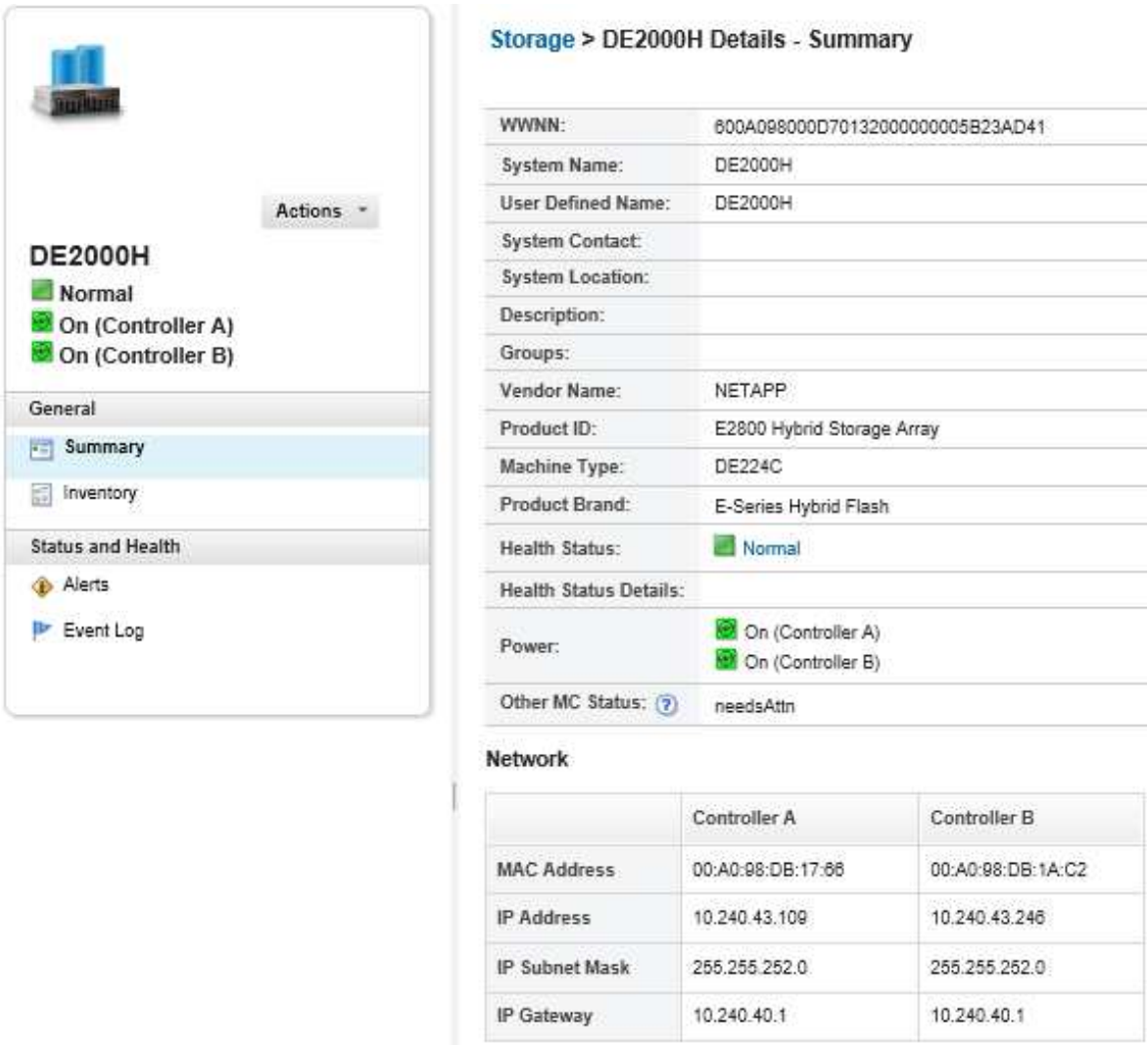
Procedure

To view the details of a specific managed storage device, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all storage devices that are installed in managed chassis.

You can sort the table columns to make it easier to find specific storage devices. In addition, enter text (such as a system name or IP address) in the **Filter** field to further filter the storage devices that are displayed.

Step 2. Click the storage device name in the **Storage** column. The Summary page is displayed, showing the properties and a list of components that are installed in that storage device.



Step 3. Complete one or more of the following actions to view storage details. The data that is displayed might differ based on the type of storage device.

- Click **Summary** to view a summary of the server and its installed components, including system information and installed devices (see Viewing the status of storage devices).

- Click **Inventory Details** to view details about the storage device components, including:
  - Firmware levels for the storage device.
  - Details of the management-controller network, such as the hostname, IPv4 address, IPv6 address, and MAC addresses.
  - Asset details of the storage device.
  - Details about each canister in the storage device.

  Tip: If an expansion node, such as the Flex System Storage Expansion Node or the Flex System PCIe Expansion Node is installed in the chassis and connected to a storage device, inventory details for the expansion node is displayed as well.
- Click **Alerts** to display alerts in the alerts list that are related to the storage device (see Working with alerts).
- Click **Event Log** to display the events in the event log that are related to the storage devicestorage device (see Working with events).
- Click **Jobs** to display a list of jobs that are associated with the storage device (see Monitoring jobs).
- Click **Light Path** to display the current state of each LED on the storage device.
- Click **Power and Thermal** to display the power and thermal characteristics for the storage device.

  Tip: Use the refresh button on your web browser to collect the latest power and thermal data. Collecting data might take several minutes.

After you finish

In addition to displaying summary and detailed information about a storage device, you can perform the following actions:

- View a storage device in graphical rack or chassis view by clicking **Actions → Views → Show in Rack View** or **Actions → Views → Show in Chassis View**.
- Export detailed information about the storage device to a CSV file clicking the **Actions → Inventory → Export Inventory**.

  Notes:

  - For more information about inventory data in the CSV file, see the GET /storage/<*UUID_list*> REST API in the Lenovo XClarity Administrator online documentation.
  - When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Launch the management controller web interface for the storage device by clicking the **IP address** link (see Launching the management controller interface for a storage device).
- Power a storage controller in the storage device on and off (see Powering on and off a storage device).
- Virtually reseat the storage controller in the storage device (see Virtually reseating a server in a Flex System chassis).
- Modify system information by selecting a storage device and clicking **Edit Properties**.
- Refresh inventory by selecting a storage device and clicking **Actions → Inventory → Refresh Inventory**.
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Actions → Service Reset → Exclude Events** (see Excluding events).
- Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the CMM in the chassis where the storage device is installed by selecting a storage device

and clicking **Actions → Service → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).

Backing up and restoring storage-configuration data

Lenovo XClarity Administrator does not include built-in backup functions for storage-configuration data. Instead, use the backup functions that are available for your managed storage device.

See the product documentation that is provided with your storage device for information about recovering the device.

- For Lenovo Storage devices, see the Lenovo Storage S2200/S3200 product documentation.
- For Lenovo ThinkSystem storage devices, see the ThinkSystem Storage product documentation.

Powering on and off a storage device

You can power on and off a storage device from Lenovo XClarity Administrator.

About this task

For Flex System storage devices, when a storage controller is powered off, data is first stored on the internal drive and the storage device enters a standby state. In standby state, volumes that are provided by the storage device are no longer accessible.

To power on a ThinkSystem DM Series storage device, ensure that storage controller that is used for management is online and that its IP address is able to communicate directly to the service processor of the powered-off storage controller over the external network.

Procedure

Complete the following steps to power on and off a managed storage device.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all storage devices that are installed in managed chassis.

You can sort the table columns to make it easier to find specific storage device. In addition, enter text (such as a system name or IP address) in the **Filter** field to further filter the storage devices that are displayed.

Step 2. Select the storage device to be powered on or off.

Step 3. Click **All Actions**, and then click one of the following power actions:

- **Power On Controller A**
- **Power On Controller B**

- **Power off Controller A**
- **Power off Controller B**
- **Restart Controller A**
- **Restart Controller B**

Virtually reseating storage controllers in a Flex System storage device

You can perform a virtual reseat, which simulates the removal and reinsertion of a storage controller (canister) in the storage device bay

About this task

During the virtual reseat, all existing network connections to the storage device are lost, and the power state of the storage device changes. Before performing a virtual reseat, ensure that you have saved all user data.

Procedure

Complete the following steps virtually reseat a storage controller.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all storage devices.

You can sort the table columns to make it easier to find specific storage devices. In addition, enter text (such as a system name or IP address) in the **Filter** field to further filter the storage devices that are displayed.

Step 2. Select the Flex System storage device.

Step 3. Click **All Actions → Service**, and then click **Virtual Reseat Controller A** or **Virtual Reseat Controller B**.

Step 4. Click **Virtual Reseat**.

Launching the management controller interface for a storage device

You can launch the management controller web interface for the chassis in which the storage device is installed from Lenovo XClarity Administrator.

Procedure

To launch a management controller web interface, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Storage**. The Storage page is displayed with a tabular view of all managed storage devices.

You can sort the table columns to make it easier to find specific storage devices. In addition, enter text (such as a device name or IP address) in the **Filter** field to further filter the storage devices that are displayed.

Step 2. Select the storage device.

Step 3. Click **Actions → Launch → Management Web Interface**. The management controller web interface is started.

Step 4. Log in to the management controller interface.

Note: For Flex System storage devices, use the XClarity Administrator user credentials.

Modifying the system properties for a storage device

You can modify the system properties for a specific storage device.

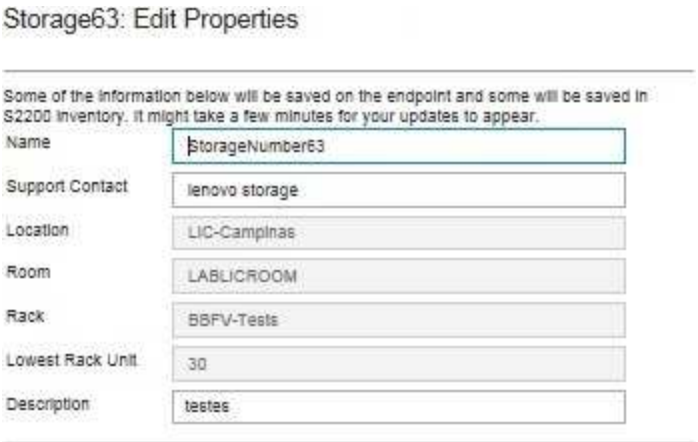
Procedure

To modify the system properties, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Storage** to display the Storage page.

Step 2. Select the storage device to be updated.

Step 3. Click **All Actions → Inventory → Edit Properties** to display the Edit dialog.



Step 4. Change the following information, as needed.
- Name
- Support contact

- Description

Note: XClarity Administrator updates the location, room, rack, and lowest rack unit properties when you add or remove devices from a rack in the web interface (see Managing racks).

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface.

Recovering management of a rack storage device after a management server failure

If a rack storage device was not unmanaged correctly, you must recover the storage device before you can remanage it. You can recover management by clearing specific parts of the storage-device configuration that was previously set by Lenovo XClarity Administrator.

Procedure

Complete one of the following steps to recovery a rack storage device.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the **Force management** option (see Managing storage devices).
- Remove all user accounts with the prefix “LXCA_” and optionally remove user accounts with the prefix “SYSMGR_” and type “SNMPv3” from the storage device.

After you finish

After XClarity Administrator is restored or replaced, you can manage the storage device again (see Managing storage devices). All information about the storage device (such as system properties) is retained.

Recovering management of a Lenovo ThinkSystem DE Series storage device after a management server failure

If a Lenovo ThinkSystem DE series storage device was not unmanaged correctly, you must recover the storage device before you can remanage it. You can recover management by clearing specific parts of the storage-device configuration that was previously set by Lenovo XClarity Administrator.

Procedure

Complete one of the following steps to recovery a Lenovo ThinkSystem DE Series storage device.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the **Force management** option (see Managing storage devices).
- Remove the “LXCA_REMOTE_MANAGMENT_VERIFICATION” key-pair register from the storage device key-pair API.

After you finish

After XClarity Administrator is restored or replaced, you can manage the storage device again (see Managing storage devices). All information about the storage device (such as system properties) is retained.

Unmanaging a storage device

You can remove a storage device from management by Lenovo XClarity Administrator. This process is called *unmanaging*.

Before you begin

Before you unmanage a storage device, ensure that there are no active jobs running against the switch.

About this task

When you unmanaged a storage device, XClarity Administrator retains certain information about the storage device. That information is reapplied when you manage the same storage device again.

Tip: All demo devices that are optionally added during initial setup are nodes in a chassis. To unmanage the demo devices, unmanage the chassis using the **Force unmanage even if the device is not reachable** option.

Procedure

To umanage a storage device, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Storage** to display the Storage page.

Step 2. Select one or more storage devices from the lists of managed switch.

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

Step 4. Optional: **Optional:** Select **Force unmanage even if the device is not reachable**.

Important: When unmanaging demo hardware, ensure that you select this option.

Step 5. Click **Unmanage**.The Unmanage dialog shows the progress of each step in the unmanagement process.

Step 6. When the unmanagement process is complete, click **OK**.

Recovering a rack storage device that was not unmanaged correctly

If Lenovo XClarity Administrator is managing a rack storage device, and if XClarity Administrator fails, you can recover the management functions until the management server is restored or replaced. You can recover system management by clearing specific parts of the storage-device configuration that was previously set by XClarity Administrator.

Procedure

Complete one of the following steps to recovery a rack storage device.

- If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the **Force management** option (see Managing storage devices).
- Remove all user accounts with the prefix “LXCA_” and optionally remove user accounts with the prefix “SYSMGR_” and type “SNMPv3” from the storage device.

After you finish

After XClarity Administrator is restored or replaced, you can manage the storage device again (see Managing storage devices). All information about the storage device (such as system properties) is retained.

Chapter 10. Managing switches

Lenovo XClarity Administrator can manage network switches.

Learn more:

- XClarity Administrator: Discovery
- XClarity Administrator: Managing switches

Before you begin

Attention: Review the switch management considerations before managing a switch. For information, see Switch management considerations.

Note: Flex switches are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed Flex switches independent of a chassis.

Certain ports must be available to communicate with the switches. Ensure that all required ports are available before you attempt to manage a switch. For information about ports, see Port availability in the XClarity Administrator online documentation.

Ensure that the minimum required firmware is installed on each switch that you want to manage using XClarity Administrator. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.

Ensure that you create stored credentials in XClarity Administrator before you manage rack switches. XClarity Administrator uses only stored credentials to authenticate to the rack switches. The stored credential must match an active user account on the device. You can create stored credentials from the management dialogs or from the Stored Credentials page. For more information, see Managing stored credentials.

Management using loopback interfaces is supported for all RackSwitch devices. Ensure that XClarity Administrator has connectivity to the loopback interface, either by adding a static route or advertising the address via a routing protocol. Note that routing cannot be performed between the management port and *any* data ports (including loopback).

For Lenovo ThinkSystem DB series switches:

- FOS 8.2.3 or later is required
- Ensure that you configure the SNMPv3 user at index 1 on the switch *before* managing the switch by running the following command on the switch: **snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname rw**
- Ensure that REST is enabled on the switch. To enable REST, run the following command: **mgmtapp --enable rest**
- Ensure that the number of allowed REST sessions is 10. To set the REST session count, run the following command: **mgmtapp --config -maxrestsession 10**
- Lenovo ThinkSystem DB series switches are not discoverable using service discovery protocols. To manage these switches, use the **Manual Input** option, clear **User service discovery protocols to identify device type**, and then select “Lenovo ThinkSystem DB Series Switch” from the **Device Type** list. For more details, see the procedure below about discovering and managing switches that are not on the same IP subnet as XClarity Administrator.

© Copyright Lenovo 2015, 2022

For NVIDIA switches:

- Cumulus 4.3 or later is required
- NVIDIA switches are not discoverable using service discovery protocols. To manage these switches, use the **Manual Input** option, clear User service discovery protocols to identify device type, and then select "NVIDIA Switch" from the **Device Type** list. For more details, see the procedure below about discovering and managing switches that are not on the same IP subnet as XClarity Administrator.

About this task

XClarity Administrator can automatically discover RackSwitch switches in your environment by probing for manageable devices that are on the same IP subnet as XClarity Administrator. To discover switches that are in other subnets, specify an IP address or range of IP addresses, or import information from a spreadsheet.

Note: If you upgraded from XClarity Administrator v2.0 to v2.1, the upgrade process converted the manual credential to individual stored credentials for all managed rack switches. Manual credentials are not supported for rack switches in XClarity Administrator v2.1 and later.

After the switches are managed by XClarity Administrator, XClarity Administrator polls each managed switch periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed switch and perform management tasks such as launching the management console, and powering on and off.

If the XClarity Administrator looses communication with the switch (for example, due to power loss or network failure or if the switch is offline) while collecting inventory during the management process, the management completes successfully; however, some inventory information might be incomplete. Either wait for the switch to come online and for XClarity Administrator to poll the switch for inventory or manually collect inventory on the switch from the Switches page by selecting the switch and clicking **All Actions → Inventory → Refresh inventory**.

Note: Switches can be stacked. A *stacked switch* is a group of switches that operate as a single network switch. The stack includes a *master switch* and one or more *member switches*. For Flex switches, you can view and monitor each switch in the stack and collect diagnostic data; however, you cannot perform management tasks (such as firmware updates and server configuration) on any stacked switch. These XClarity Administrator management tasks are disabled for all stacked switches, including the master switch. You can update firmware on the stacked switch directly from master switch CLI. For RackSwitch switches you can view and monitor only the master switch information. The member switches are not discovered by XClarity Administrator.

Management tasks are also disabled for Flex switches that are in protected mode.

A device can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device on the initial XClarity Administrator, and then manage it with the new XClarity Administrator. If an error occurs during the unmanagement process, you can select the **Force management** option during management on the new XClarity Administrator.

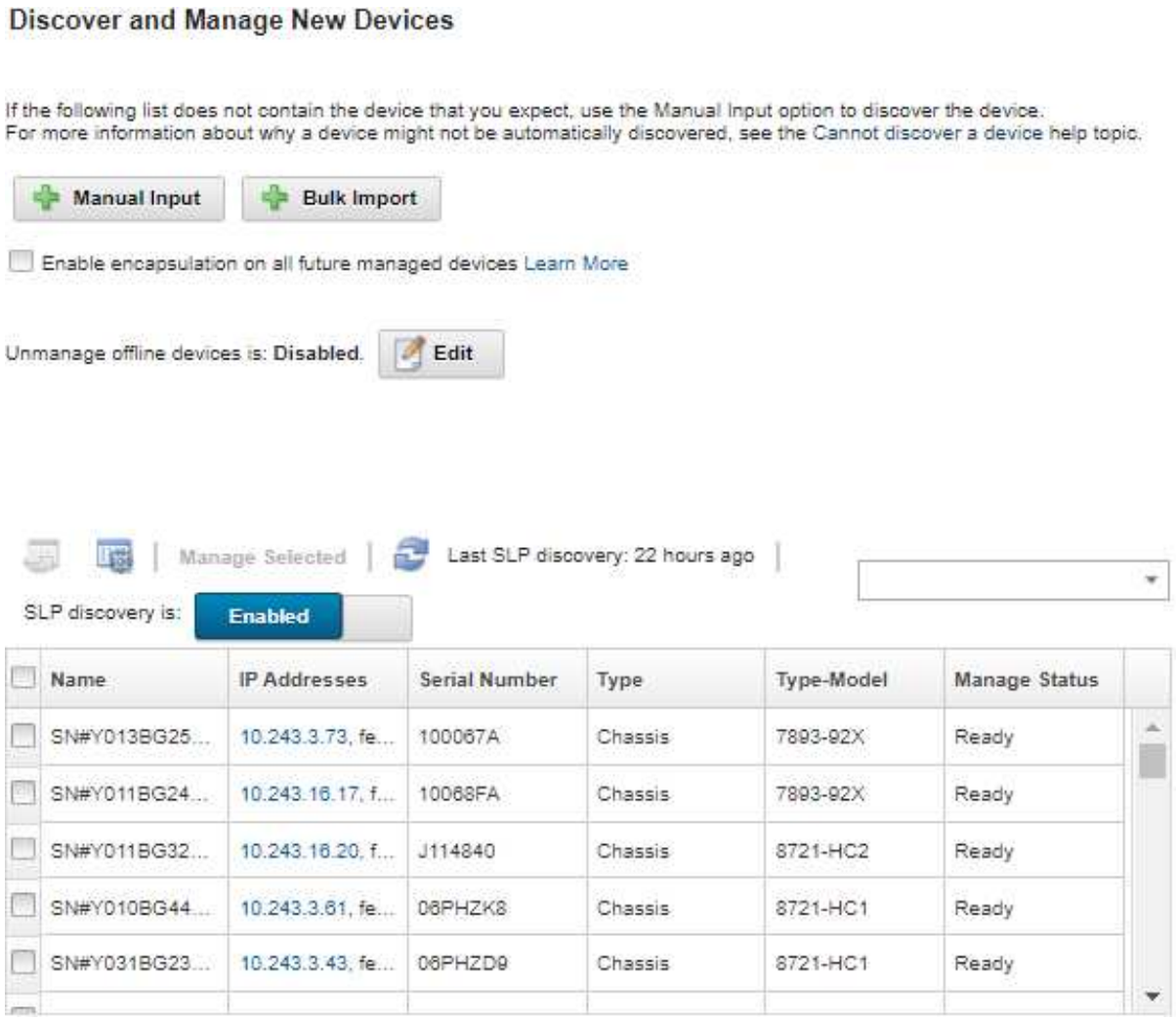
Note: When scanning the network for manageable devices, XClarity Administrator does not know whether a device is already managed by another manager until after it attempts to manage the device.

When a switch is managed either directly using SSH or indirectly through a CMM, the switch is identified as managed by XClarity Administrator, necessary configuration is performed for interaction, and inventory is collected.

Procedure

Complete one of the following procedures to manage your RackSwitch switches using XClarity Administrator.

- Discover and manage a large number of switches and other devices using a bulk-import file (see Managing systems in the Lenovo XClarity Administrator online documentation).
- Discover and manage RackSwitch switches that are on the same IP subnet as XClarity Administrator.
  1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage New Devices page is displayed.



     You can sort the table columns to make it easier to find the switches that you want to manage. In addition, you can enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed. You can change the columns that are displayed and the default sort order by clicking the **Customize Columns** icon ( ).
  2. Click the **Refresh** icon ( ) to discover all manageable devices in the XClarity Administrator domain. Discovery might take several minutes.
  3. Select one or more switches that you want to manage.
  4. Click **Manage Selected**.

5. Specify the stored credentials for authenticating to the switches.

   Tip:

   – Click **Manage Stored Credentials** to create and managed stored credentials in XClarity Administrator (see Managing stored credentials).

   – It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

6. (Switches running ENOS only) If set, specify the “enable” password that is used to enter Privileged Exec Mode on the switch.

   When you manage a RackSwitch switch running ENOS, access to Privileged Exec Mode on the switch is required. This is used by XClarity Administrator when issuing the “enable” command to the switch. By default, there is no password set for this command on the switch. However, if the switch administrator configured a password for this command for added security, it must be specified for XClarity Administrator to manage the switch successfully.

7. Optional: (Switches running ENOS only) Choose whether to enable HTTPS on the switch by clicking **Advanced** and then selecting **Enable HTTPS**. This is enabled by default.

   Notes:

   – For switches running CNOS, HTTPS must be enabled on the switch before management (see Switch management considerations).

   – If you choose not to enable HTTPS, the current setting on the switch is used.

   – When the switch is ununmanaged, XClarity Administrator restores HTTPS to the original setting.

8. Optional: Choose whether to replace the NTP configuration on the switch with the NTP configuration and time zone settings that are defined for Lenovo XClarity Administrator by clicking **Advanced** and then selecting **Configure NTP clients to use the NTP settings from the management server**. This is enabled by default.

   Notes:

   – If you choose *not* to replace the NTP configuration and time zone, the timestamp for log entries and events might become out of synch between the managed switch and the management server.

   – When the switch is ununmanaged, XClarity Administrator restores NTP configuration and time zone to the original settings.

9. Click **Change** to change the role groups that are to be assigned to the devices.

   Notes:

   – You can select from a list of role groups that are assigned to the current user.

   – If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

10. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the job progress.

11. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

- If the managing XClarity Administrator failed and cannot be recovered.

  Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

- If the managing XClarity Administrator was taken down before the devices were unmanaged.
- If the devices were not unmanaged successfully.

Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

- Discover and manage RackSwitch switches that are not on the same IP subnet as XClarity Administrator by manually specifying IP addresses:
  1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
  2. Select **Manual Input**.
  3. Specify the network addresses of the switches that you want to manage:
     - Click **Single System**, and enter a single IP address domain name, or fully-qualified domain name (FQDN).

       Note: To specify an FQDN, ensure that a valid domain name is specified on Network Access page (see Configuring network access).

     - Click **Multiple Systems**, and enter a range of IP addresses. To add another range, click the **Add** icon ( ). To remove a range, click the **Remove** icon ( ).
  4. If the device type is not discoverable using service discovery protocols, clear User service discovery protocols to identify device type, and then select the type of device to be managed from the drop-down list.

     Service discovery protocols, such as SLP and SSDP, enable XClarity Administrator to automatically discover the type of the device that is about to be managed and then use the appropriate mechanism to manage the device. Some device types do not support service discovery protocols, and in some environments, service discovery protocols are purposely turned off. In either case, you must choose the appropriate device type to complete the manage process. The following device types must be explicitly identified.
     - Lenovo ThinkSystem DB Series Switch
     - NVIDIA Mellanox Switch
  5. Click **OK**.
  6. Specify the stored credentials for authenticating to the switches.

     Tip:

     - Click **Manage Stored Credentials** to create and managed stored credentials in XClarity Administrator (see Managing stored credentials).
     - It is recommended to use a supervisor or administrator account to manage the device. If an account with lower level authority is used, management might fail, or management might succeed but other future XClarity Administrator operations on the device might fail (particularly if the device is managed without managed authentication).

7. (Switches running ENOS only) If set, specify the “enable” password that is used to enter Privileged Exec Mode on the switch.

   When you manage a RackSwitch switch running ENOS, access to Privileged Exec Mode on the switch is required. This is used by XClarity Administrator when issuing the “enable” command to the switch. By default, there is no password set for this command on the switch. However, if the switch administrator configured a password for this command for added security, it must be specified for XClarity Administrator to manage the switch successfully.

8. Optional: (Switches running ENOS only) Choose whether to enable HTTPS on the switch by clicking **Advanced** and then selecting **Enable HTTPS**. This is enabled by default.

   Notes:

   – For switches running CNOS, HTTPS must be enabled on the switch before management (see Switch management considerations).
   – If you choose not to enable HTTPS, the current setting on the switch is used.
   – When the switch is ununmanaged, XClarity Administrator restores HTTPS to the original setting.

9. Optional: Choose whether to replace the NTP configuration on the switch with the NTP configuration and time zone settings that are defined for Lenovo XClarity Administrator by clicking **Advanced** and then selecting **Configure NTP clients to use the NTP settings from the management server**. This is enabled by default.

   Notes:

   – If you choose *not* to replace the NTP configuration and time zone, the timestamp for log entries and events might become out of synch between the managed switch and the management server.
   – When the switch is ununmanaged, XClarity Administrator restores NTP configuration and time zone to the original settings.

10. Click **Change** to change the role groups that are to be assigned to the devices.

    Notes:

    – You can select from a list of role groups that are assigned to the current user.
    – If you do not change the role groups, the default role groups are used. For more information about the default role groups, see Changing the default permissions.

11. Click **Manage**.

    A dialog is displayed that shows the progress of this management process. To ensure that the process completes successfully, monitor the job progress.

12. When the process is complete, click **OK**.

    The device is now managed by XClarity Administrator, which automatically polls the managed device on a regular schedule to collect updated information, such as inventory.

    If management was not successful due to one of the following error conditions, repeat this procedure using the **Force management** option.

    – If the managing XClarity Administrator failed and cannot be recovered.

      Note: If the replacement XClarity Administrator instance uses the same IP address as the failed XClarity Administrator, you can manage the device again using the RECOVERY_ID account and password (if applicable) and the **Force management** option.

    – If the managing XClarity Administrator was taken down before the devices were unmanaged.
    – If the devices were not unmanaged successfully.

Attention: Devices can be managed by only one XClarity Administrator instance at a time. Management by multiple XClarity Administrator instances is not supported. If a device is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the device from the original XClarity Administrator, and then manage it with the new XClarity Administrator.

After you finish

- Discover and manage additional devices.
- Add the newly managed devices to the appropriate rack to reflect the physical environment (see Managing racks).
- Monitor hardware status and details (see Viewing the status of switches).
- Monitor events (see Working with events).

Switch management considerations

Before managing a switch, review the following important considerations.

For information about port requirements, see Port availability in the Lenovo XClarity Administrator online documentation.

RackSwitch devices can be managed using either a management port or one of the data ports. Rackswitch devices running CNOS can be managed only on interfaces that belong to either “management” or “default” VRF.

Note: Managing RackSwitch devices using IPv6 link local through a data port or management port is not supported.

XClarity events and SNMP trap configuration

When a RackSwitch device running ENOS (any version) is managed, the SNMP trap source is set to the interface that has the IP address that is used for management.

When a RackSwitch device running CNOS v10.8.1 or later is managed, the SNMP trap source VRF is checked and changed to match the port that is used for management.

For RackSwitch devices running CNOS earlier than v10.8.1, XClarity Administrator requires the SNMP trap source to be the VRF that is connected to the port that is used for management. The default value “all” allows either management or data ports to be used. If the switch configuration does not use the default value, it must be changed to match the port that is used for management.

- If the management port is used for management, set the SNMP trap source VRF to “all” or “management.”
- If one of the data ports is used for management, set the SNMP trap source VRF to “all” or “default.”

RackSwitch switches running CNOS

HTTPS must be enabled for management, and SLP must be enabled for discovery.

Note: HTTPS is enabled by default on CNOS. If you changed the default configuration of restApi (using the **feature restApi http** command), you can change it back to HTTPS using the **feature restApi** command. To check the current status, use the **display restApi server** command. The output reflects the current status. If the port number is followed by “(HTTP)”, it means HTTPS is *disabled*. Otherwise, the port should be 443.

When a RackSwitch device is unmanaged, XClarity Administrator might not restore the “prefer” option to the value that it was before the device was managed depending on the CNOS firmware version.

RackSwitch switches running ENOS

- If RackSwitch switches are on a different network than XClarity Administrator, the network must be configured to allow inbound UDP through ports 161 and 162 so that XClarity Administrator can receive events and manage those devices.
- SSH must be enabled for management, and SLP must be enabled for discovery. HTTPS is optional; however, must be enabled to launch the switch web interface
- Depending on the firmware version of the RackSwitch switch, you might need to enable multicast SLP forwarding and SSH on each RackSwitch switch manually using the following commands before the switch can be discovered and managed by XClarity Administrator. For more information, see the Rack switches in the System x online documentation.
  - `ip slp enable`
  - `ssh enable`
- When a RackSwitch switch is managed, XClarity Administrator modifies the following configuration settings. Changing these settings on a managed switch might disrupt connectivity and prevent management actions from performing correctly. When a RackSwitch switch is unmanaged, the configuration settings are restored to their original values (before management).
  - snmp-server access 32
  - snmp-server group 16
  - snmp-server notify 16
  - snmp-server target-parameters 16
  - snmp-server target-address 16
  - snmp-server trap-source <*IP interface*>
  - snmp-server user 16
  - snmp-server vesrion <*v3only or v1v2v3*>
  - ntp enable
  - ntp primary-server <*hostname or IP address*> MGT
  - ntp secondary-server <*hostname or IP address*> MGT
  - ntp interval 1500
  - ntp offset 500
  - access https enable

  You can use XClarity Administrator to modify the following configuration settings by modifying the support contact information, name, or location properties for the switch. The location is modified when adding the switch to a rack.
  - hostname "<*device_name*>"
  - snmp-server location "Location:<*location*>,Room:<*room*>,Rack:<*rack*>,LRU:<*lru*>"
  - snmp-server contact "<*contact_name*>"

Viewing the status of switches

You can view the status of all switches that Lenovo XClarity Administrator manages.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

About this task

The following status icons are used to indicate the overall health of the device. If the certificates do not match, “(Untrusted)” is appended to the status of each applicable device, for example Warning (Untrusted). If

there is a connectivity issue or a connection to the device is not trusted, “(Connectivity)” is appended to the status of each applicable device, for example Warning (Connectivity).

- ( ) Critical
  - One or more temperature sensors are in the failure range.
  - Fan modules or fans are not working correctly, as follows:
    - RackSwitch G8124-E: One or more fans are running at less than or equal to 100 RPM.
    - RackSwitch G8052: Fewer than three fan modules are in good state. If the fans in that module are running at more than 500 RPM, a fan module is considered good.
    - RackSwitch G8264, G8264CS, G8332, G8272: Fewer than four fan modules are in good state. If the fans in that module are running at more than 500 RPM, a fan module is considered good.
    - RackSwitch G8296: Fewer than three fan mare in good state. If the fans in that module are running at more than 480 RPM, a fan module is considered good.
    - RackSwitch G7028, G7052: Fewer than three fan modules are in good state. If the fans in that module are running at more than 500 RPM, a fan module is considered good.
  - One power supply is off.
- ( ) Warning
  - One or more temperature sensors are in the warning range.
  - A panic dump exists in flash.
- ( ) Pending
- ( ) Informational
- ( ) Normal
  - All temperature sensors are in the normal range.
  - All fan modules or fans are working correctly.
  - Both power supplies are on.
  - No panic dump in flash.
- ( ) Offline
- ( ) Unknown

A device can be in one of the following power states:

- On
- Off
- Shutting down
- Standby
- Hibernate
- Unknown

Procedure

To view the status for a managed switch, complete one or more of the following actions.

- From the XClarity Administrator menu bar, click **Dashboard**. The dashboard page is displayed with an overview and status of the all managed switches and other resources.

- From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all managed switches.

  You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field and click the status icons to list only those switches that meet the selected criteria.

  From this page, you can perform the following actions:

  – View detailed information about the switch (see Viewing the details of a switch).

  – View a Flex switch in graphical rack or chassis view by clicking **All Actions → Views → Show in Rack View** or **All Actions → Views → Show in Chassis View**.

  – View a RackSwitch switch in graphical rack view by clicking **All Actions → Views → Show in Rack View**.

- Launch the management controller web interface for the switch by clicking the **IP address** link (see Launching the management controller interface for a switch).
- Launch the switch SSH console (see Launching a remote SSH session for a switch).
- Power the switch on and off (see Powering on and off a switch).
- (RackSwitch switches only) Modify system information by selecting a switch and clicking **All Actions → Inventory → Edit Properties**.
- Refresh inventory by selecting a server and clicking **All Actions → Inventory → Refresh Inventory**.
- Export detailed information about one or more switches to a single CSV file by selecting the switches and clicking **All Actions → Inventory → Export Inventory** (see Excluding events).

  Note: You can export inventory data for a maximum of 60 devices at one time.

  Tip: When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking the **Exclude events** icon ( ) (see Excluding events).
- (Flex switches only) Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the CMM in the chassis where the switch is installed by selecting a switch and clicking **All Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).
- Add or remove a switch from a static resource group by clicking **All Actions → Groups → Add to Group** or **All Actions → Groups → Remove from Group**.

Viewing the details of a switch

You can view detailed information about a managed switch from Lenovo XClarity Administrator, including the firmware levels and IP addresses.

Learn more:

- XClarity Administrator: Inventory
- XClarity Administrator: Monitoring

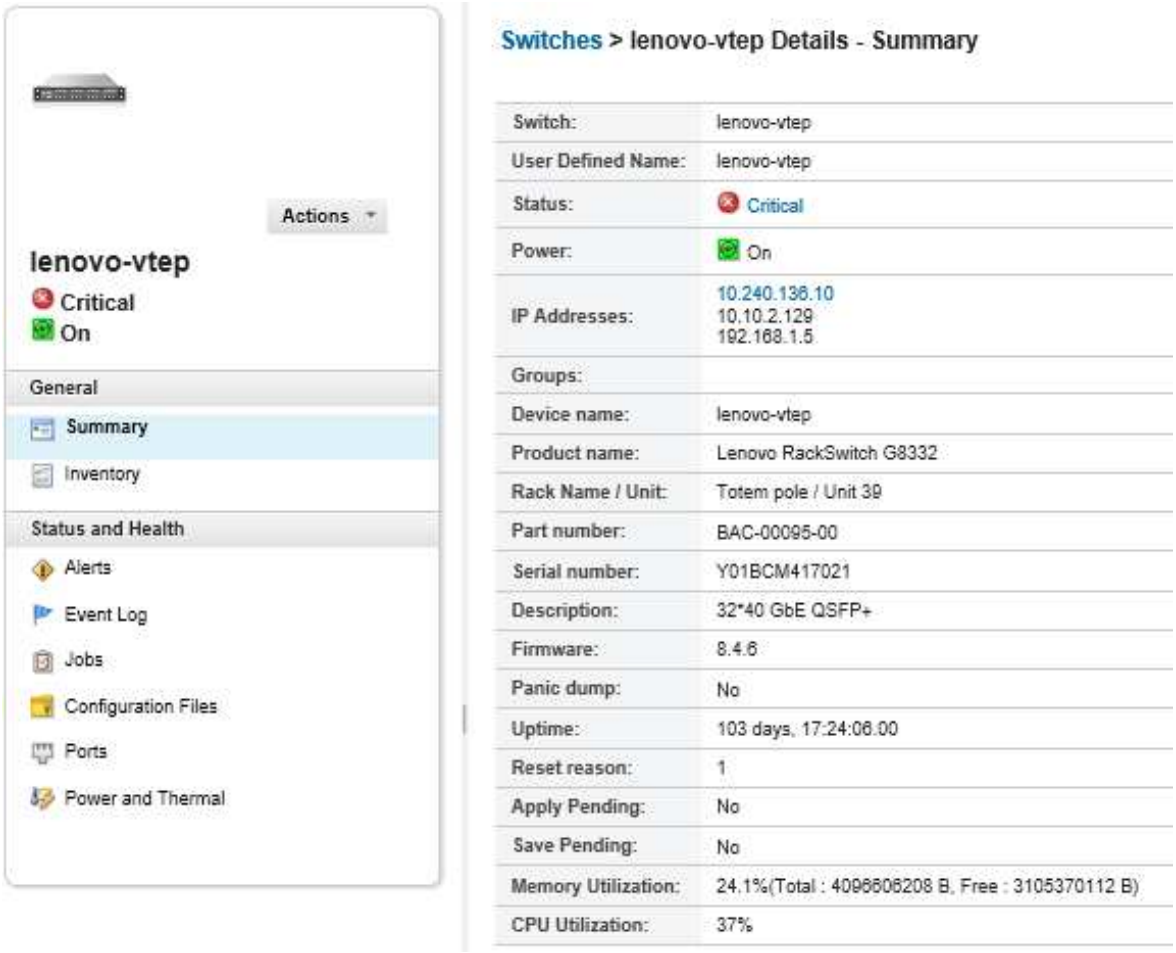
Procedure

To view the details of a specific switch that is managed by XClarity Administrator, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

Step 2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.



Step 3. Complete one or more of the following steps to view detailed inventory information:

Note: Some details might not be available for all switches.

- Click **Summary** to view a summary of the switch, including system information and firmware (see Viewing the status of storage devices).
- Click **Inventory Details** to view details about the switch components, including:
  - Firmware levels for the switch

  - Details of the management-controller network, such as the hostname, IPv4 address, IPv6 address, and MAC addresses
  - Asset details of the switch
- Click **I/O Connectivity** to display connectivity details for the selected switch and the associated network adapters that are installed in switch.
- Click **Alerts** to display alerts in the alerts list that are related to the switch (see Working with alerts).
- Click **Event Log** to display the events in the event log that are related to the switch (see Working with events).
- Click **Configuration Files** to backup and restore the switch configuration (see Backing up and restoring switch-configuration data).
- Click **Deployment History** to view information about switch-configuration templates that have been deployed to switch (see Viewing switch-configuration deployment history).
- Click **Jobs** to display configuration-data files for the switch (see Monitoring jobs).
- Click **Ports** to display the status and configuration of all ports in a managed switch , and to enable or disable switch ports.

  Note: For Flex switches, click the **Refresh** icon ( ) to collect the current port data. Collecting data might take several minutes.
- Click **Light Path** to display the current state of each LED on the switch.
- Click **Power and Thermal** to display information about temperature, power supplies, and fans.

  Tip: To collect the latest power and thermal data, Use the refresh button on your web browser. Collecting data might take several minutes.

After you finish

In addition to displaying summary and detailed information about a switch, you can perform the following actions:

- View a Flex switch in graphical rack or chassis view by clicking **Actions → Views → Show in Rack View** or **Actions → Views → Show in Chassis View**.
- View a RackSwitch switch in graphical rack view by clicking **Actions → Views → Show in Rack View**.
- Launch the management controller web interface for the switch by clicking the **IP address** link (see Launching the management controller interface for a switch).
- Launch the switch SSH console (see Launching a remote SSH session for a switch).
- Power the switch on and off (see Powering on and off a switch).
- (RackSwitches only) Modify system information by selecting a switch and clicking **Edit Properties**.
- Export detailed information about the switch to a CSV file by clicking the **Actions → Inventory → Export Inventory**.

  Notes:
  - For more information about inventory data in the CSV file, see the GET /switches/<*UUID_list*> REST API in the XClarity Administrator online documentation.
  - When importing a CSV file into Microsoft Excel, Excel treats text values that contain only numbers as numeric values (for example, for UUIDs). Format each cell as text to correct this error.
- Exclude events that are of no interest to you from all pages on which events are displayed by clicking **Actions → Service Reset → Excluded Events** (see Excluding events).

- Resolve issues that might arise between the XClarity Administrator security certificate and the security certificate of the RackSwtich or the CMM in the chassis where the Flex System switch is installed by selecting a switch and clicking **Actions → Security → Resolve Untrusted Certificates** (see Resolving an untrusted server certificate).

Powering on and off a switch

You can power on and off and restart a Flex System or RackSwitch switch from Lenovo XClarity Administrator.

Procedure

Complete the following steps to power on or off a managed switch.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

Step 2. Select the switch to be powered on or off or restarted.

Step 3. Click **All Actions**, and then click one of the following power actions:
- **Power on** (Flex System switches only)
- **Power Off** (Flex System switches only)
- **Restart**. The switch is restarted after all currently running operations are complete. Operations that are started while the switch is restarting are rejected.

Enabling and disabling switch ports

You can enable or disable specific ports on a RackSwitch or Flex System switch

Procedure

To enable or disable switch ports, complete the following steps.

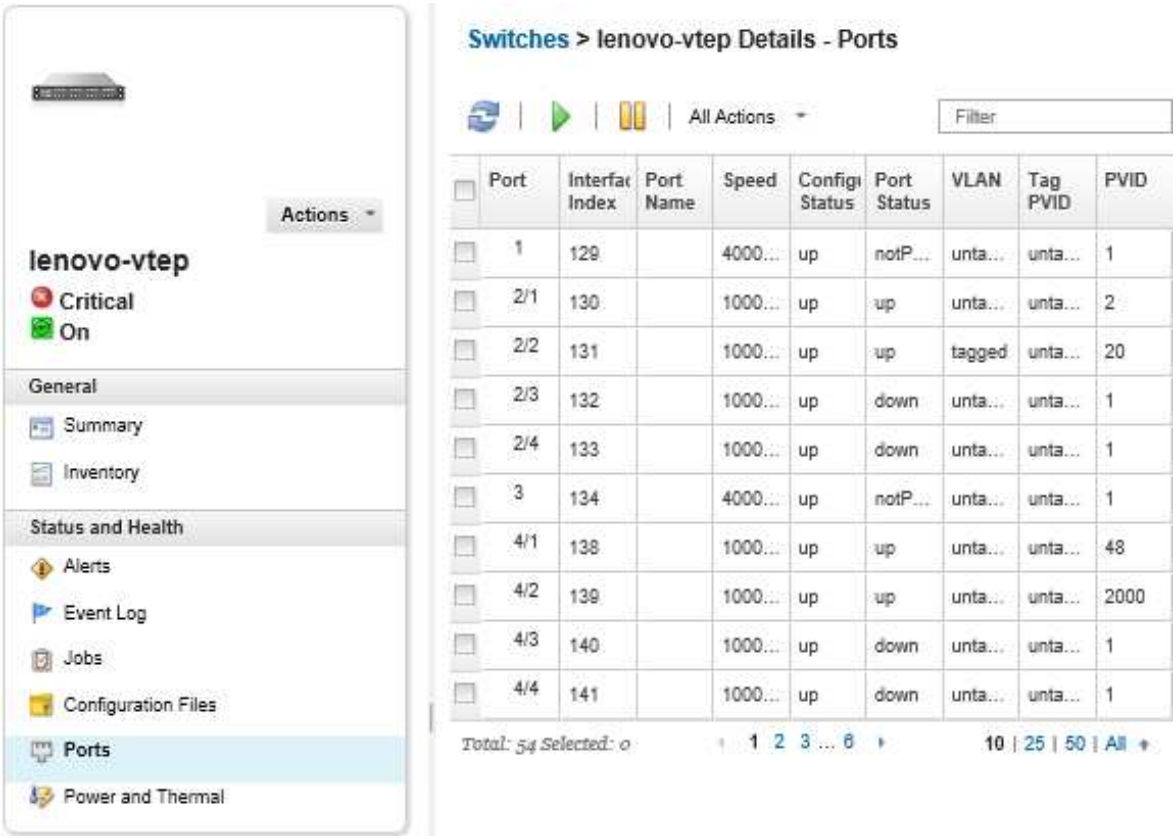
Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

Step 2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.

Step 3. Click **Ports** in the left navigation to display the status and configuration of all ports in the switch:

Note: For Flex switches, click the **Refresh** icon ( ) to collect the current port data. Collecting data might take several minutes



Step 4. Select the port, and then click the **Enable** icon ( ) or **Disable** icon ( ).

Backing up and restoring switch-configuration data

You can use Lenovo XClarity Administrator to back up and restore configuration data for your RackSwitch and Flex System switches. You can also export switch-configuration files to your local system and import switch-configuration files into XClarity Administrator.

Backing up switch-configuration data

You can back up configuration data for a Flex System or RackSwitch switch. When backing up a switch, the configuration data is imported into Lenovo XClarity Administrator from the target switch as a switch-configuration file.

Procedure

To back up configuration data for a managed switch, complete the following steps.

- For a single switch:
  1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

     You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

  2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.
  3. Click **Configuration** to view the configuration files for the switch.
  4. Click **Back up configuration data** icon ( ) to back up the switch configuration.
  5. (Optional) Specify a name for the switch-configuration file.

     For CNOS devices, the file name can contain alphanumeric characters and the following special characters: underscore (_), hyphen (-) and period (.). For ENOS switches, the file name can contain alphanumeric characters and any special characters.

     If a file name is not specified, the following default name is used: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."
  6. (Optional) Add a comment that describes the backup.
  7. Click **Back up** to back up with switch-configuration data immediately or click **Schedule** to schedule this backup to run at a later time.

     If you chose to schedule a backup, you can select **Overwrite** to back up the switch-configuration data into the same file at each job run, overwriting its contents. If you choose not to overwrite file, the file names of subsequent backups are appended with a unique number (for example, MyBackup_33.cfg).

     Note: When scheduling a backup, you cannot choose dynamic file names or comments for each scheduled job.
- For multiple switches:

1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.
2. Select one or more switches.
3. Click **All Actions → Configuration → Backup configuration file**.
4. (Optional) Specify a name for the switch-configuration file.

   For CNOS devices, the file name can contain alphanumeric characters and the following special characters: underscore (_), hyphen (-) and period (.). For ENOS switches, the file name can contain alphanumeric characters and any special characters.

   If a file name is not specified, the following default name is used: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."
5. (Optional) Add a comment that describes the backup.
6. Click **Back up** to back up with switch-configuration data immediately or click **Schedule** to schedule this backup to run at a later time.

   If you chose to schedule a backup, you can select **Overwrite** to back up the switch-configuration data into the same file at each job run, overwriting its contents. If you choose not to overwrite file, the file names of subsequent backups are appended with a unique number (for example, MyBackup_33.cfg).

   Note: When scheduling a backup, you cannot choose dynamic file names or comments for each scheduled job.

After you finish

When the backup process is complete, the switch-configuration file is added to the **Configuration Files** tab on the switch details page.

From this page, you can perform the following actions on selected switch-configuration file:

- Restore the switch configuration by selecting the switch-configuration file and clicking the **Restore configuration data** icon ( ).
- Delete switch configuration files from XClarity Administrator by clicking the **Delete** icon ( ).
- Export switch-configuration files to your local system by selecting the files and clicking the **Export configuration file** icon ( ).
- Import switch-configuration files to XClarity Administrator by clicking the **Import configuration file** icon ( ).

Restoring switch-configuration data

You can restore configuration data that has been backed up or imported into Lenovo XClarity Administrator for a Flex System or RackSwitch switch. The switch-configuration file is downloaded from XClarity Administrator to the target switch, and the configuration takes effect automatically.

Configuration files are associated with a specific switch. You can restore a configuration file only on the switch with which it is associated. You cannot use a configuration file that was backed up for one switch to restore the configuration on another switch.

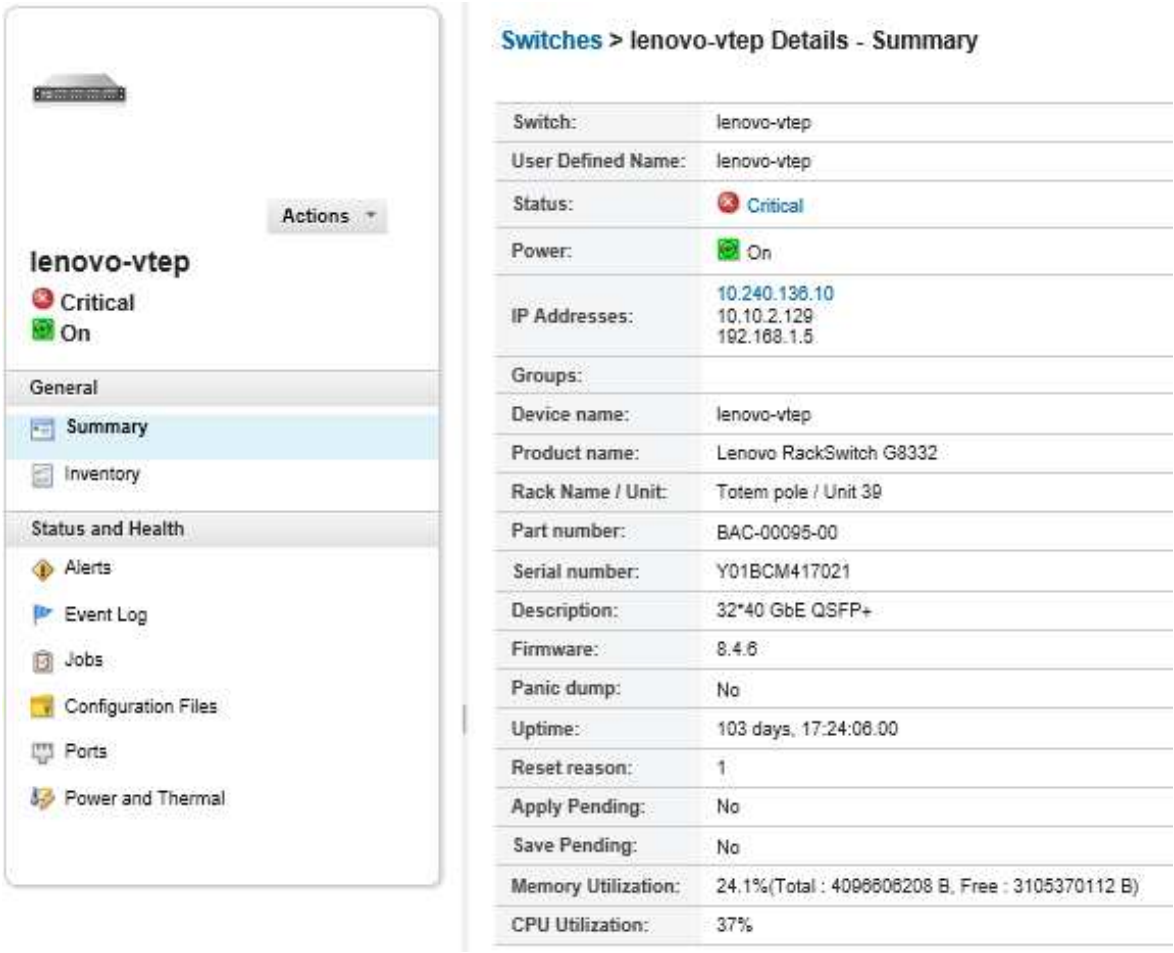
Procedure

To restore configuration data on a managed switch, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

Step 2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.



Step 3. Click **Configuration Files** to view the configuration files for the switch.

Step 4. Select the configuration file that you want to restore on the switch, and click **Restore configuration data** icon ( ). The Restore dialog is displayed.

Step 5. (Switches running CNOS only) Choose whether to restart the switch after the restore operation completes.

If you choose not to restart the switch automatically, you must manually restart the CNOS switch to activate the restored configuration data. If you wait too long and a save operation occurs (for example, if a port is enabled or disabled), the restore operation is aborted and the running configuration data is used.

Step 6. Click **Restore** to restore with configuration data on the switch immediately, or click **Schedule** to schedule this restore job to run at a later time.

Note: Take care when scheduling a recurring restore jobs. If your switch resets to an earlier configuration, check the Scheduled Jobs page for scheduled restore jobs.

Exporting and importing switch-configuration files

You can export switch-configuration files to your local system and import switch-configuration files into Lenovo XClarity Administrator.

Procedure

To back up configuration data for a managed switch, complete the following steps.

- Export switch-configuration files
  1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

     You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

  2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.
  3. Click **Configuration** to view the configuration files for the switch.
  4. Select the switch-configuration files to export.
  5. Click **Export configuration file** icon ( ) to back up the switch configuration.
- Import switch-configuration files
  1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

2. Click the switch in the **Switches** column. The Summary page is displayed, showing the properties and a list of components that are installed in that switch.
3. Click **Configuration** to view the configuration files for the switch.
4. Click **Import configuration file** icon ( ) to back up the switch configuration.
5. Enter the switch-configuration file name or click **Browse** to find the boot file that you want to import.
6. **Optional:** Enter a description for the switch-configuration file.
7. Click **Import**.

   If you close the web browser tab or window in which the file is being uploaded before the upload completes, the import fails.

Launching the management controller interface for a switch

You can launch the management controller web interface for a RackSwitch or Flex System switch running ENOS from Lenovo XClarity Administrator.

Procedure

Complete the following steps to launch the management controller interface for a switch.

Note: Launching any management controller web interface from XClarity Administrator using the Safari web browser is not supported.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

Step 2. Select the switch, and click **All Actions → Launch → Management Web Interface**. The management controller web interface for the switch is displayed.

Tip: You can also launch the management controller interface by clicking the IP address link in the **IP Address** column, and on the switch summary and switch details pages.

Step 3. Log in to the management controller interface.

Tip: For Flex switches, use your XClarity Administrator user credentials. For XClarity Administrator switches, use the switch credentials.

Launching a remote SSH session for a switch

You can launch a remote SSH session for a managed RackSwitch or Flex switch from Lenovo XClarity Administrator. From the remote SSH session, you can use the command-line interface to perform management tasks that are not provided by XClarity Administrator.

Before you begin

Ensure that the switch is configured to enable SSH. For RackSwitch switches, SSH is enabled when the switch is managed by XClarity Administrator. For Flex switches, SSH is typically enabled by default. If not enabled, SSH must be enabled before the switch is managed by XClarity Administrator.

Procedure

Complete the following steps to launch a remote SSH session for a managed switch.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all switches that are installed in managed chassis.

You can sort the table columns to make it easier to find the switches that you want to manage. In addition, enter text (such as a name or IP address) in the **Filter** field to further filter the switches that are displayed.

Step 2. Select the switch to launch an SSH session.

Step 3. Click **All Actions → Launch → SSH Console**.

Step 4. If required, log in to the switch using your user ID and password.

Modifying the system properties for a switch

You can modify the system properties for a specific Flex System or RackSwitch switch.

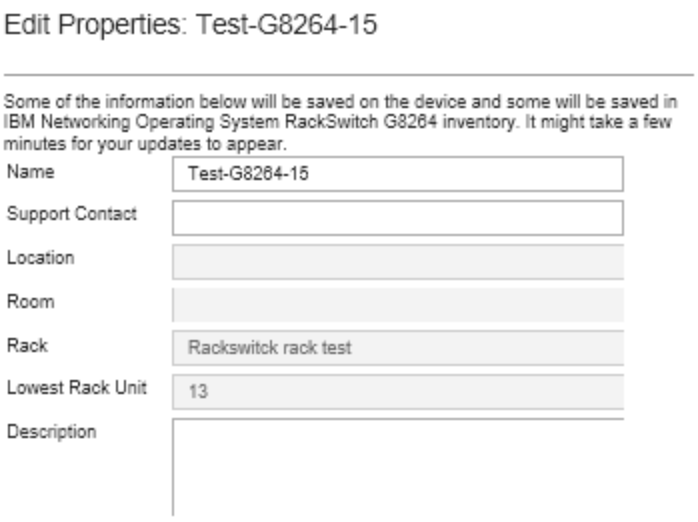
Procedure

Complete the following steps to modify the system properties.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Switches** to display the Switches page.

Step 2. Select the switch to be updated.

Step 3. Click **All Actions → Inventory → Edit Properties** to display the Edit dialog.



Step 4. Change the following information, as needed.
- Switch name
- Support contact
- Description

Note: The location, room, rack, and lowest rack unit properties are updated by XClarity Administrator when you add or remove devices from a rack in the web interface (see Managing racks).

Step 5. Click **Save**.

Note: When you change these properties, there might be a short delay before the changes appear in the XClarity Administrator web interface.

Resolving expired or invalid stored credentials for a switch

When a stored credential becomes expired or inoperable on a device, the status for that device is shown as “Offline.”

Procedure

To resolve an expired or invalid stored credential for a switch, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Switches**. The Switches page is displayed with a tabular view of all managed switches.

Step 2. Click the **Power** column header to group all offline switches at the top of the table.

You can sort the table columns to make it easier to find the switch that you want to manage. In addition, you can enter text (such as a system name or IP address) in the **Filter** field to further filter the switches that are displayed.

Step 3. Select the switch to be resolved.

Step 4. Click **All Actions → Security → Edit Stored Credentials**.

Step 5. Change the password for the stored credential or select another stored credential to use for the managed device.

Note: If you managed more than one device using the same stored credentials and you change the password for the stored credentials, that password change affects all devices that are currently using the stored credentials.

Recovering management with a switch after a management server failure

You can recover management of a switch that was not unmanaged cleanly (for example, due to connectivity issues during unmanagement or failure of the managing Lenovo XClarity Administrator).

Procedure

- Manage the switch again using the **Force management** option (see Managing switches).

- To permanently remove XClarity Administrator specific configuration on a switch that was not unmanaged cleanly and will not be managed again, complete these steps.
  - Manage the switch again using the **Force management** option (see Managing switches), and then unmanage the switch to clean up the configuration (see Unmanaging a switch).
  - (ENOS) Log in to the switch using the switch console port or an SSH or telnet session, and run the following configuration commands in the order specified to clear the switch configuration.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Unmanaging a switch

You can remove a switch from management by Lenovo XClarity Administrator. This process is called *unmanaging*.

Before you begin

You can enable XClarity Administrator to automatically unmanage devices that are offline for a specific amount of time. This is disabled by default. To enable the automatic unmanagment of offline devices, click **Hardware → Discover and Manage New Devices** from the XClarity Administrator menu, and then click **Edit** next to **Unmanage offline devices is Disabled**. Then, select **Enable unmanage offline devices** and set the time interval. By default, devices are unmanaged after being offline for 24 hours.

Before you unmanage a switch, ensure that there are no active jobs running against the switch.

About this task

When you unmanaged a switch, XClarity Administrator retains certain information about the switch. That information is reapplied when you manage the same switch again.

Tip: All demo devices that are optionally added during initial setup are nodes in a chassis. To unmanage the demo devices, unmanage the chassis using the **Force unmanage even if the device is not reachable** option.

Procedure

To unmanaged a switch, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Hardware → Switches** to display the Switches page.

Step 2. Select one or more switches from the lists of managed switch.

Step 3. Click **Unmanage Switch**. The Unmanage dialog is displayed.

Step 4. Optional: **Optional:** Select **Force unmanage even if the device is not reachable**.

Important: When unmanaging demo hardware, ensure that you select this option.

Step 5. Click **Unmanage**.The Unmanage dialog shows the progress of each step in the unmanagement process.

Step 6. When the unmanagement process is complete, click **OK**.

Recovering a switch that was not unmanaged correctly

If a switch is being managed by Lenovo XClarity Administrator, and if XClarity Administrator fails, you can recover the management functions until the management server is restored or replaced.

Procedure

- Manage the switch again using the **Force management** option (see Managing switches).
- To permanently remove XClarity Administrator specific configuration on a switch that was not unmanaged cleanly and will not be managed again, complete these steps.
  - Manage the switch again using the **Force management** option (see Managing switches), and then unmanage the switch to clean up the configuration (see Unmanaging a switch).
  - (ENOS) Log in to the switch using the switch console port or an SSH or telnet session, and run the following configuration commands in the order specified to clear the switch configuration.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Chapter 11. Configuring servers using configuration patterns

Server patterns are used to quickly provision or preprovision multiple servers (rack and tower servers and compute nodes) from a single set of defined configuration settings.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Configuration patterns

Before you begin

After the 90-day free trial expires, you can continue to use XClarity Administrator to manage and monitor your hardware for free; however, you must purchase full-function-enablement licenses for each managed server that supports XClarity Administrator advanced functions to continue using the server configuration function. Lenovo XClarity Pro provides entitlement to service and support and the full-function-enablement license. For more information about purchasing Lenovo XClarity Pro, contact your Lenovo representative or authorized business partner. For more information, see Installing the full-function enablement license in the XClarity Administrator online documentation.

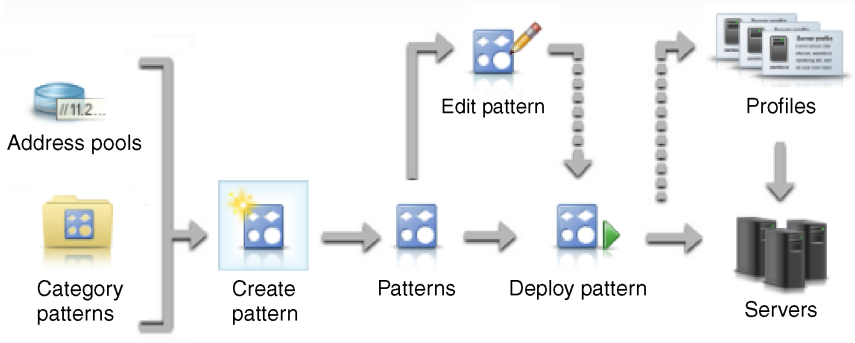
Review Configuration considerations for important information about configuration support for specific servers and devices.

About this task

You can use server patterns in XClarity Administrator to configure local storage, I/O adapters, boot order, and other baseboard management controller and Unified Extensible Firmware Interface (UEFI) settings on managed servers. Server patterns also integrate support for virtualizing I/O addresses, so you can virtualize server fabric connections or repurpose servers without disruption to the fabric. You can also initiate SAN-zoning change requests in advance of receiving new hardware by virtualizing (preconfiguring) Fibre Channel addresses.

Procedure

The following figure illustrates the workflow for configuring managed servers. The solid arrows indicate actions taken by you. The dashed arrows indicate actions that are performed automatically by XClarity Administrator.



Step 1. **Create address pools.**An *address pool* is a defined set of address ranges. Lenovo XClarity Administrator uses address pools to assign IP and I/O addresses to individual servers when the server patterns are deployed to those servers.

© Copyright Lenovo 2015, 2022

For more information about creating address pools, see Defining address pools.

Step 2. **Create category patterns.**

A *category pattern* groups together related firmware settings and can be reused in multiple server patterns. You can create patterns for the following firmware categories:

- System information
- Management interfaces
- Devices and I/O ports
- FC boot targets
- I/O adapter ports

For more information about category patterns, see Working with server patterns.

Step 3. **Create a server pattern.**

A *server pattern* represents pre-OS server configurations, including local storage configuration, I/O adapter configuration, boot settings, and other baseboard management controller and UEFI firmware settings. A server pattern is used as an overall pattern to quickly configure multiple servers at one time.

You can define multiple server patterns to represent different configurations that are used in your data center.

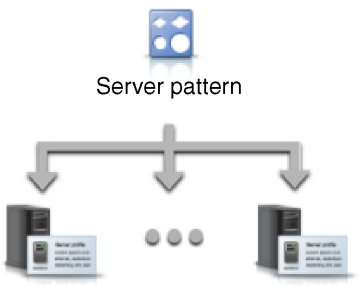
When defining a server pattern, select category patterns and address pools as needed to construct the desired configuration for a specific group of servers. A category pattern groups together related configuration settings that can be reused by multiple server patterns.

You can create a server pattern from scratch for Converged, Flex System, NeXtScale, and System x servers to define the desired configuration before the hardware arrives. Or, you can create a server pattern from an existing managed server. When you create a server pattern from an existing server, XClarity Administrator learns category patterns from the selected server.

For more information about creating server patterns, see Creating a server pattern.

Step 4. **Deploy the server pattern.**

You can deploy a server pattern to one or more individual servers or to groups of servers. For example, you can deploy a server pattern to a chassis so all the compute nodes in that chassis are configured the same. During deployment, XClarity Administrator creates a server profile for each server to which the server pattern was deployed. Each *server profile* represents the specific configuration for a single server. It inherits settings from the server pattern and also contains server-specific information (such as assigned IP addresses and MAC addresses). Because the server profile inherits settings from the server pattern, if you change the server pattern, changes are automatically updated in the server profile. This way, you can maintain common configurations in one place.



Note: The settings on a server can become out of compliance with its server profile if settings are changed without using Configuration Patterns or if an issue occurred during deployment, such a firmware issue or an invalid setting. You can determine the compliance status of each server from the Configuration Patterns: Server Profiles page.

You can deploy a server pattern to:

- **Existing servers**. A server profile is created for each server. The server profile is activated after the associated server is rebooted.
- **Empty bays in an existing chassis**. A server profile is created for each empty bay. The server profile that is associated with the empty bay can then be activated after the compute node is physically installed.
- **Placeholder for a chassis that you do not yet have**. You can pre-provision compute nodes in a chassis that you do not yet have by defining a *placeholder chassis* to act as a target for the server pattern before the hardware arrives. The placeholder chassis bundles all of the server profiles that are created for each empty compute-node bay. So, when the hardware arrives, you can assign the server profiles to all compute nodes in the new chassis by deploying the placeholder chassis to the new chassis. Each server profile is activated after the associated compute node is rebooted.

Note: You can deploy a server pattern to multiple servers; however, multiple patterns cannot be deployed to a single server.

For more information about deploying a server pattern, see Deploying a server pattern to a server and Deploying a placeholder chassis.

Step 5. **Edit the server pattern.**

You use server patterns to control a common configuration from a single place. You no longer update settings directly on servers. Instead, you update category patterns and server patterns, and the changes are automatically deployed to all associated profiles and their servers.

For more information about editing a server pattern, see Modifying a server pattern.

Configuration considerations

Before you begin configuring servers through Lenovo XClarity Administrator, review the following important considerations.

- If a server profile includes earlier firmware levels and you update firmware to later levels, XClarity Administrator compares the stored profile settings to the server settings, and reports “Not Compliant.” Hover the cursor over the “Not Compliant” status to determine the reason for the non-compliance.

  You can manually change the status of Not Compliant” devices to “Compliant” without redeploying the profile by selecting the devices, and then clicking **All Actions → Make Compliant**.
- After upgrading firmware (such as UEFI, BMC or I/O controllers) on a server, some configurations might change (for example, when adding new items, deleting existing items, or changing the behaviors or value range of an item). As a result, the server profile might become non-compliant or applying the server pattern might fail if it is created using a previous firmware level. In this case, it is recommended that you choose to learn a new pattern based on the updated firmware or edit the failed pattern to exclude the configuration of specific items, and then apply that pattern to the server.
- XClarity Administrator v2.8 does not support configuration patterns for ThinkSystem SR635 and SR655 servers in the following situations.

  - If XClarity Administrator v2.7 manages ThinkSystem SR635 and SR655 servers running 20A firmware, and you upgrade to 20B firmware using the baseboard management controller before upgrading to XClarity Administrator v2.8
  - If XClarity Administrator v2.7 manages ThinkSystem SR635 and SR655 servers running 20B firmware before upgrading to XClarity Administrator v2.8
  - If XClarity Administrator v2.8 manages ThinkSystem SR635 and SR655 servers running 20A firmware, and you upgrade to 20B firmware using the baseboard management controller
- The QLogic 8200 2-Port 10GbE SFP+ VFA adapter has invalid values for these settings: iSCSIFirstTargetParameters_iSCSIName, iSCSISecondTargetParameters_iSCSIName and IPv6LinkLocalAddress. You must manually correct these values in the system setup before learning the configuration pattern from the server or correct the values in the learned configuration pattern.
- For Flex System x240 and x440 Compute Nodes with embedded RAID adapters, server patterns that define RAID configuration definitions can be deployed only to one or more servers that do not have existing RAID configurations. If a server pattern is deployed to a server that has an existing RAID configuration, the existing arrays and volumes are not overwritten. To apply the RAID configuration that is defined in the server pattern, you must first clear the servers existing RAID configuration (see Resetting storage adapters to default values), and then redeploy the server profile by selecting the server and clicking **More → Deploy Server Profile**.
- The onboard storage controllers in Flex System x220, Flex System x222, and ThinkSystem servers support software-based RAID. However, configuration of software RAID using Configuration Patterns is not supported.
- When configuring RAID using Configuration Patterns, if the server is powered off, the server boots to BIOS/UEFI Setup automatically before activating the server profile.
- For ThinkServer servers, Configuration Patterns are not supported.
- Certain I/O devices cannot be configured using server patterns. For more information, see XClarity Administrator Support – Compatibility webpage.
- If advanced features (such as SPAR, Easy Connect, and stack) are enabled on Flex switches EN4093R, CN4093, SI4093, or SI4091, network configurations might not be applied correctly on internal ports.
- By default, Flex switch SI4093 is shipped with SPAR enabled. If you want to deploy network settings using port patterns to internal ports on these switches, you must manually remove the switch internal ports from SPAR or remove the SPAR configurations from the switch.
- It is recommended that you *do not* use XClarity Administrator to configure the Converged and ThinkAgile appliances using Configuration Patterns.
- Ensure that all available ports are enabled on the installed adapters before creating the Configuration Patterns from an existing server so that all available ports and settings are included in the pattern. Then, if needed, you can disable any ports using the appropriate settings defined in the pattern. If ports are disabled when the pattern is created, the pattern might not be created correctly, and the pattern might not deploy successfully.

Defining address pools

An *address pool* is a defined set of address ranges. Lenovo XClarity Administrator uses address pools to assign IP and I/O addresses to individual servers when the server patterns are deployed to those servers.

About this task

XClarity Administrator supports IP and I/O address pools.

IP address pools

IP address pools define ranges of IP addresses for use when configuring the baseboard management controller network interface of your servers. You can use or customize predefined address pools or you can create new pools as needed. When creating server patterns, you can choose which IP address pool to use during deployment. When the server pattern is deployed, IP addresses are allocated from the selected pool and assigned to individual management controllers.

Note: If you are satisfied with your management-controller network configuration, do not use this option.

Attention:

- Ensure that you select an IP address subrange that does not conflict with existing I/O addresses in your data center.
- Ensure that the IP addresses in the specified ranges are part of the same subnetwork and are reachable by XClarity Administrator.
- Ensure that the IP addresses in the specified ranges are unique for each XClarity Administrator domain and existing IP management tools to prevent address conflicts.

The overall address pool range is derived from the specified routing prefix length and the gateway or initial range. You can create pools of different sizes based on the specific routing prefix length, but overall pool ranges must be unique within the XClarity Administrator domain. Ranges are then created from the overall pool range.

Address ranges can be used to separate hosts (for example, by operating system type, workload types, and business type). Address ranges can also be tied to organizational network rules.

Ethernet address pools

Ethernet address pools are collections of unique MAC addresses that can be assigned to network adapters when configuring servers. You can use or customize predefined address pools as needed, or you can create new pools. When creating server patterns, you can choose which Ethernet address pool is to be used during deployment. When the server pattern is deployed, addresses are allocated from the selected pool and assigned to individual adapter ports.

The following predefined MAC addresses pool is available:

- Lenovo MAC address pool

For a list of MAC address ranges in this pool, see Ethernet address (MAC) pools.

Fibre Channel address pools

Fibre Channel address pools are collections of unique WWNN and WWPN addresses that can be assigned to Fibre Channel adapters when configuring servers. You can use or customize predefined address pools as needed, or you can create new pools. When creating server patterns, you can choose which Fibre Channel address pool is to be used during deployment. When the server pattern is deployed, addresses are allocated from the selected pool and assigned to individual adapter ports.

The following predefined Fibre Channel addresses pools are available:

- Lenovo WWN addresses
- Brocade WWN addresses
- Emulex WWN addresses
- QLogic WWN addresses

For a list of WWN address ranges in these pools, see Fibre Channel address (WWN) pools.

The range of addresses in the address pools must be unique within the XClarity Administrator domain. XClarity Administrator ensures that the defined ranges and assigned addresses are unique within its management domain.

Important: In large environments with multiple XClarity Administrator instances, ensure that unique address ranges are used by each XClarity Administrator to prevent address duplication.

Ethernet and Fibre Channel address pools are used with I/O adapter virtual addressing to assign organizationally unique I/O addresses. When you create a server pattern for a compute node, you can enable virtual addressing as part of the devices and I/O adapter configuration. When virtual addressing is enabled, addresses are assigned from the Ethernet and Fibre Channel address pools to prevent address conflicts.

Restriction: Virtual addressing is supported for only Flex System compute nodes. Standalone rack and tower servers are not supported.

For information about creating server patterns, see Creating a server pattern.

Creating an IP address pool

An *IP address pool* defines a range of IP addresses for use when configuring the baseboard-management-controller network interface of your servers. When the associated server pattern is deployed, IP addresses are allocated from the specified pool and assigned to individual servers.

About this task

The data in the Overall Network Information table on the New IP Address Pool dialog is derived from the specified subnet mask and gateway or initial range. You can create pools of different sizes based on the specific subnet mask, but overall pool ranges must be unique within the management domain. Ranges are then created from the overall pool range. All ranges must be part of the same sub network and are bound by the limits shown in the Overall Network Information table.

The pool and ranges have Lenovo XClarity Administrator scope. In large environments with multiple XClarity Administrator instances, create unique pools and ranges for each XClarity Administrator to avoid address conflicts and to avoid address conflicts with existing IP management tools. Ranges can also be used to separate hosts (for example, by operating system type, workload type, and business function) and to tie organization network rules.

Procedure

Complete the following steps to create an IP address pool.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Address Pools**. The Configuration Patterns: Address Pools page is displayed.

Step 2. Click the **IP Address Pools** tab.

Step 3. Click the **Create** icon ( ). The New IP Address Pools Wizard dialog is displayed.

Step 4. Fill in the following information.

- Name and description for the address pool.
- Choose to use IPv4 or IPv6 addresses.
- Select a subnet mask (for IPv4) or a routing prefix length (for IPv6).
- Specify the gateway address.The network information values are derived from the specified subnet mask and gateway or initial range and are filled in the table.
- Add one or more ranges of addresses:
  1. Click **Add Range** to add a range of addresses. The New Add IP Address Range dialog is displayed.
  2. Enter a range name, first address, and range size.The last address is calculated automatically.

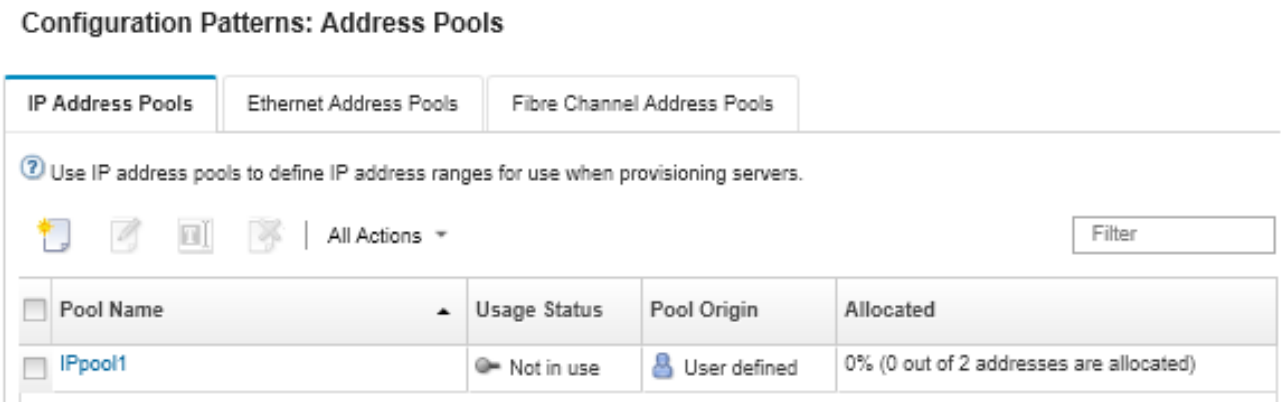
3. Click **OK**.The range is added to the **Define IP pool address ranges** table, and the fields in the summary section are updated automatically.

You can edit the range by clicking the **Edit** icon ( ) or remove the range by clicking the **Remove** icon ( ).

Step 5. Click **Create**.

After you finish

The new IP address pool is listed in the table on the IP Address Pools page:



From this page, you can perform the following actions on a selected address pool:

- Modify the address pool by clicking the **Edit** icon ( ).
- Rename the address pool by clicking the **Rename** icon.
- Delete the address pool by clicking the **Delete** icon ( ).
- View details about the address pool, including a mapping between the virtual addresses and the installed adapter's ports and reserved virtual addresses, by clicking the pool name in the **Pool Name** column.

Creating an Ethernet address pool

Ethernet address pools are collections of unique media access control (MAC) addresses that can be assigned to network adapters. You can use or customize predefined address pools as needed, or you can create new address pools. When you create a server pattern, if you enable virtual addressing for Ethernet adapters, you can choose which Ethernet address pool is to be used when the pattern is deployed. When the associated server pattern is deployed, MAC addresses are allocated from the selected address pool and assigned to individual network adapters in the servers.

Procedure

Complete the following steps to create an Ethernet address pool.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Address Pools**. The Configuration Patterns: Address Pools page is displayed.

Step 2. Click the **Ethernet Address Pools** tab.

Step 3. Click the **Create** icon ( ). The New Ethernet (MAC) Address Pools dialog is displayed.

Step 4. Enter a name and description for the address pool.

Step 5. Add one or more ranges of addresses:

a. Click **Add Range** to add a range of addresses. The Ethernet (MAC) Address Range dialog is displayed.

b. Enter a range name, first MAC address, and range size.

   The last MAC address is calculated automatically.

c. Click **Add**.

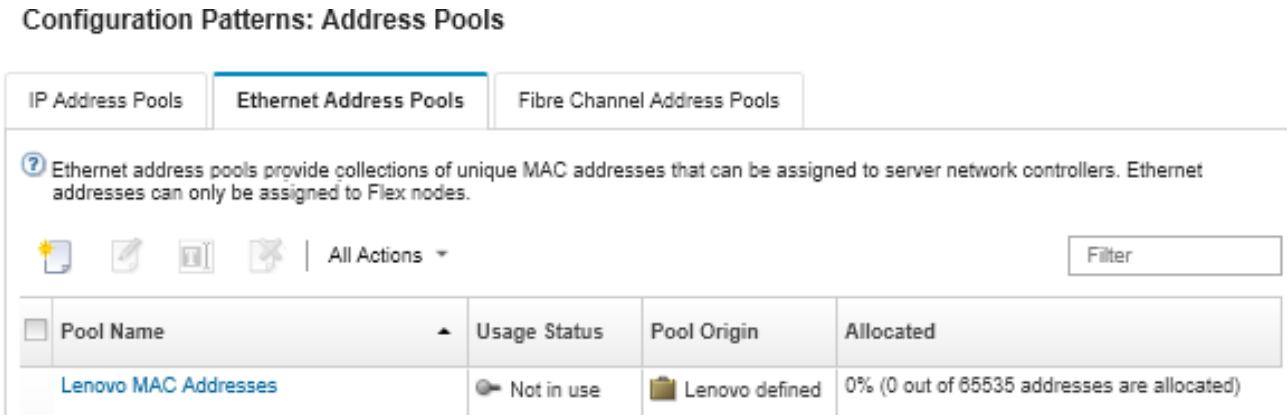
   The range is added to the **Define Ethernet (MAC) pool address ranges** table, and the fields in the summary section are updated automatically.

   You can edit the range by clicking the **Edit** icon ( ) or remove the range by clicking the **Remove** icon ( ).

Step 6. Click **Save**.

After you finish

The new Ethernet address pool is listed in the Ethernet Address Pools page.



From this page, you can perform the following actions on a selected address pool:

- Modify the address pool by clicking the **Edit** icon ( ).
- Rename the address pool by clicking the **Rename** icon.
- Delete the address pool by clicking the **Delete** icon ( ).
- View details about the address pool, including a mapping between the virtual addresses and the installed adapter's ports and reserved virtual addresses, by clicking the pool name in the **Pool Name** column.

Ethernet address (MAC) pools

Ethernet address pools are collections of unique media access control (MAC) addresses that can be assigned to network adapters. You can use the following predefined address pool in your server patterns.

Table 3. Lenovo MAC address pool

Predefined range	Starting address	Ending address
Range 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
Range 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
Range 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
Range 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
Range 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34

Table 3. Lenovo MAC address pool (continued)

Predefined range	Starting address	Ending address
Range 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
Range 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
Range 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
Range 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Creating a Fibre Channel address pool

Fibre Channel address pools are collections of unique World Wide Node Name (WWNN) and World Wide Port Name (WWPN) addresses that can be assigned to Fibre Channel adapters. You can use or customize predefined address pools as needed, or you can create new pools. When creating server patterns, if you enable virtual addressing for Ethernet adapters, you can choose which Fibre Channel address pool is to be used when the pattern is deployed. When the associated server pattern is deployed, WWNN and WWPN addresses are allocated from the pool and assigned to individual servers.

Procedure

Complete the following steps to create a Fibre Channel address pool.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Address Pools**. The Configuration Patterns: Address Pools page is displayed.

Step 2. Click the **Fibre Channel Address Pools** tab.

Step 3. Click the **Create** icon ( ). The Fibre Channel Address Pools dialog is displayed.

Step 4. Enter a name and description for the address pool.

Step 5. Add one or more ranges of addresses:

a. Click **Add Range** to add a range of addresses. The Fibre Channel (WWN) Address Range dialog is displayed.

b. Enter a range name, range size, and the first address for each fabric.

The last addresses are calculated automatically.

c. Click **Add**.

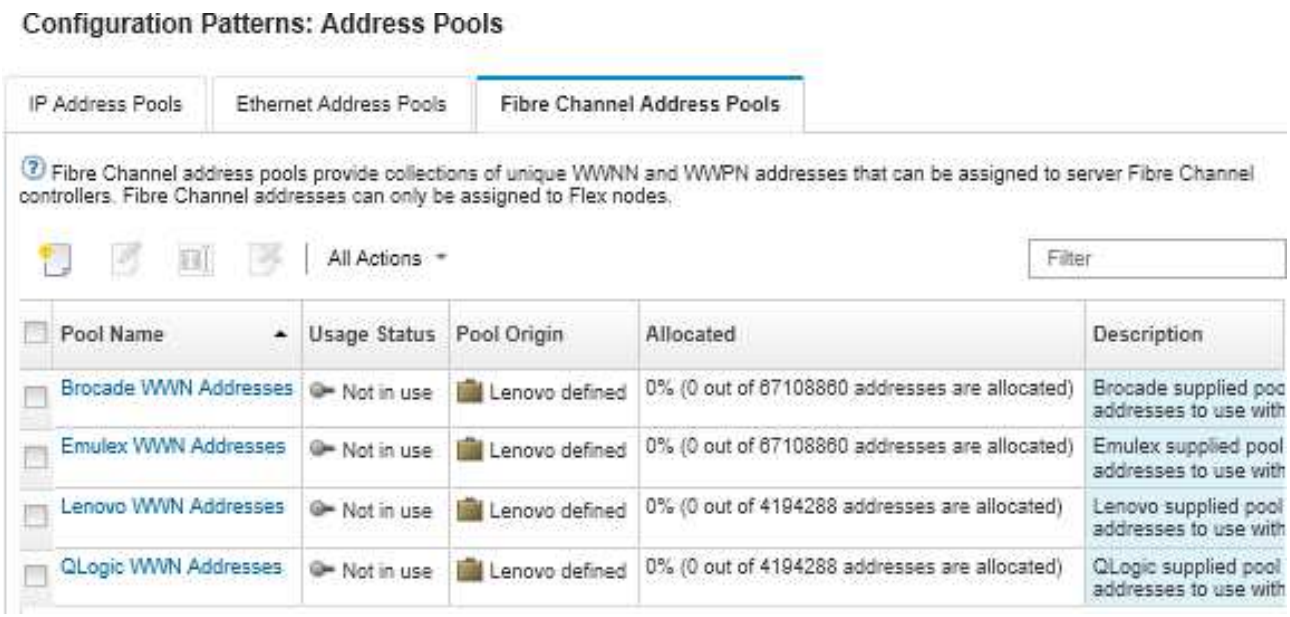
The range is added to the **Define Fibre Channel pool address ranges** table, and the fields in the summary section are updated automatically.

You can edit the range by clicking the **Edit** icon ( ) or remove the range by clicking the **Remove** icon ( ).

Step 6. Click **Save**.

After you finish

The new Fibre Channel address pool is listed in the Fibre Channel Address Pools table.



From this page, you can perform the following actions on a selected address pool:

- Modify the address pool by clicking the **Edit** icon ( ).
- Delete the address pool by clicking the **Delete** icon ( ).
- View details about the address pool, including a mapping between the virtual addresses and the installed adapter's ports and reserved virtual addresses, by clicking the pool name in the **Pool Name** column.

Fibre Channel address (WWN) pools

Fibre Channel address pools are collections of unique World Wide Node Name (WWNN) and World Wide Port Name (WWPN) addresses that can be assigned to Fibre Channel adapters. You can use the following predefined address pools in your server patterns.

Table 4 "Brocade WWN address pool" on page 318 lists the Brocade World Wide Name (WWN) address pools. Each Brocade range contains 1,864,135 addresses.

Table 5 "Emulex WWN address pool" on page 319 lists the EmulexWWN address pools. Each Emulex range contains 1,864,135 addresses.

Table 6 "Lenovo WWN address pool" on page 320 lists the Lenovo WWN address pools. Each Lenovo WWN range contains 116,508 addresses.

Table 7 "QLogic WWN address pool" on page 321 lists the QLogic WWN address pools. Each QLogic WWN range contains 116,508 addresses.

Table 4. Brocade WWN address pool

Prede-fined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Fabric A				
Range 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C:71:C6
Range 2	2B:FA:00:05:1E:1C:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C:71:C7	2B:FC:00:05:1E:38:E3:8D

Table 4. Brocade WWN address pool (continued)

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Range 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54
Range 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
Range 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E:38:E2
Range 6	2B:FA:00:05:1E:8E:38:E3	2B:FA:00:05:1E:AA:AA:A9	2B:FC:00:05:1E:8E:38:E3	2B:FC:00:05:1E:AA:AA:A9
Range 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA:AA:AA	2B:FC:00:05:1E:C7:1C:70
Range 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
Range 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF:FF:FE
Fabric B				
Range 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C:71:C6
Range 2	2B:FB:00:05:1E:1C:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C:71:C7	2B:FD:00:05:1E:38:E3:8D
Range 3	2B:FB:00:05:1E:38:E3:8E	2B:FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38:E3:8E	2B:FD:00:05:1E:55:55:54
Range 4	2B:FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71:C7:1B	2B:FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71:C7:1B
Range 5	2B:FB:00:05:1E:71:C7:1C	2B:FB:00:05:1E:8E:38:E2	2B:FD:00:05:1E:71:C7:1C	2B:FD:00:05:1E:8E:38:E2
Range 6	2B:FB:00:05:1E:8E:38:E3	2B:FB:00:05:1E:AA:AA:A9	2B:FD:00:05:1E:8E:38:E3	2B:FD:00:05:1E:AA:AA:A9
Range 7	2B:FB:00:05:1E:AA:AA:AA	2B:FB:00:05:1E:C7:1C:70	2B:FD:00:05:1E:AA:AA:AA	2B:FD:00:05:1E:C7:1C:70
Range 8	2B:FB:00:05:1E:C7:1C:71	2B:FB:00:05:1E:E3:8E:37	2B:FD:00:05:1E:C7:1C:71	2B:FD:00:05:1E:E3:8E:37
Range 9	2B:FB:00:05:1E:E3:8E:38	2B:FB:00:05:1E:FF:FF:FE	2B:FD:00:05:1E:E3:8E:38	2B:FD:00:05:1E:FF:FF:FE

Table 5. Emulex WWN address pool

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Fabric A				
Range 1	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:1C:71:C6	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:1C:71:C6
Range 2	2F:FE:00:00:C9:1C:71:C7	2F:FE:00:00:C9:38:E3:8D	2F:FC:00:00:C9:1C:71:C7	2F:FC:00:00:C9:38:E3:8D

Table 5. Emulex WWN address pool (continued)

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Range 3	2F:FE:00:00:C9:38:E3:8E	2F:FE:00:00:C9:55:55:54	2F:FC:00:00:C9:38:E3:8E	2F:FC:00:00:C9:55:55:54
Range 4	2F:FE:00:00:C9:55:55:55	2F:FE:00:00:C9:71:C7:1B	2F:FC:00:00:C9:55:55:55	2F:FC:00:00:C9:71:C7:1B
Range 5	2F:FE:00:00:C9:71:C7:1C	2F:FE:00:00:C9:8E:38:E2	2F:FC:00:00:C9:71:C7:1C	2F:FC:00:00:C9:8E:38:E2
Range 6	2F:FE:00:00:C9:8E:38:E3	2F:FE:00:00:C9:AA:AA:A9	2F:FC:00:00:C9:8E:38:E3	2F:FC:00:00:C9:AA:AA:A9
Range 7	2F:FE:00:00:C9:AA:AA:AA	2F:FE:00:00:C9:C7:1C:70	2F:FC:00:00:C9:AA:AA:AA	2F:FC:00:00:C9:C7:1C:70
Range 8	2F:FE:00:00:C9:C7:1C:71	2F:FE:00:00:C9:E3:8E:37	2F:FC:00:00:C9:C7:1C:71	2F:FC:00:00:C9:E3:8E:37
Range 9	2F:FE:00:00:C9:E3:8E:38	2F:FE:00:00:C9:FF:FF:FE	2F:FC:00:00:C9:E3:8E:38	2F:FC:00:00:C9:FF:FF:FE
Fabric B				
Range 1	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:1C:71:C6	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:1C:71:C6
Range 2	2F:FF:00:00:C9:1C:71:C7	2F:FF:00:00:C9:38:E3:8D	2F:FD:00:00:C9:1C:71:C7	2F:FD:00:00:C9:38:E3:8D
Range 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54
Range 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B
Range 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E:38:E2
Range 6	2F:FF:00:00:C9:8E:38:E3	2F:FF:00:00:C9:AA:AA:A9	2F:FD:00:00:C9:8E:38:E3	2F:FD:00:00:C9:AA:AA:A9
Range 7	2F:FF:00:00:C9:AA:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA:AA:AA	2F:FD:00:00:C9:C7:1C:70
Range 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
Range 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF:FF:FE

Table 6. Lenovo WWN address pool

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Fabric A				
Range 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C7:1B
Range 2	20:80:00:50:76:01:C7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C7:1C	21:80:00:50:76:03:8E:37

Table 6. Lenovo WWN address pool (continued)

Predefined range	WWNN starting address	WWNN ending address	WWPN starting address	WWPN ending address
Range 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
Range 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
Range 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E3:8B
Range 6	20:80:00:50:76:08:E3:8C	20:80:00:50:76:0A:AA:A7	21:80:00:50:76:08:E3:8C	21:80:00:50:76:0A:AA:A7
Range 7	20:80:00:50:76:0A:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A:AA:A8	21:80:00:50:76:0C:71:C3
Range 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
Range 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:FF:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:FF:FB
Fabric B				
Range 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C7:1B
Range 2	20:81:00:50:76:21:C7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C7:1C	21:81:00:50:76:23:8E:37
Range 3	20:81:00:50:76:23:8E:38	20:81:00:50:76:25:55:53	21:81:00:50:76:23:8E:38	21:81:00:50:76:25:55:53
Range 4	20:81:00:50:76:25:55:54	20:81:00:50:76:27:1C:6F	21:81:00:50:76:25:55:54	21:81:00:50:76:27:1C:6F
Range 5	20:81:00:50:76:27:1C:70	20:81:00:50:76:28:E3:8B	21:81:00:50:76:27:1C:70	21:81:00:50:76:28:E3:8B
Range 6	20:81:00:50:76:28:E3:8C	20:81:00:50:76:2A:AA:A7	21:81:00:50:76:28:E3:8C	21:81:00:50:76:2A:AA:A7
Range 7	20:81:00:50:76:2A:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A:AA:A8	21:81:00:50:76:2C:71:C3
Range 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
Range 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:FF:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:FF:FB

Table 7. QLogic WWN address pool

Predefined range	WWNN starting address	WWNN ending address	WWPN ending address	WWPN ending address
Fabric A				
Range 1	20:80:00:E0:8B:00:00:00	20:80:00:E0:8B:01:C7:1B	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:01:C7:1B
Range 2	20:80:00:E0:8B:01:C7:1C	20:80:00:E0:8B:03:8E:37	21:80:00:E0:8B:01:C7:1C	21:80:00:E0:8B:03:8E:37

Table 7. QLogic WWN address pool (continued)

Predefined range	WWNN starting address	WWNN ending address	WWPN ending address	WWPN ending address
Range 3	20:80:00:E0:8B:03:8E:38	20:80:00:E0:8B:05:55:53	21:80:00:E0:8B:03:8E:38	21:80:00:E0:8B:05:55:53
Range 4	20:80:00:E0:8B:05:55:54	20:80:00:E0:8B:07:1C:6F	21:80:00:E0:8B:05:55:54	21:80:00:E0:8B:07:1C:6F
Range 5	20:80:00:E0:8B:07:1C:70	20:80:00:E0:8B:08:E3:8B	21:80:00:E0:8B:07:1C:70	21:80:00:E0:8B:08:E3:8B
Range 6	20:80:00:E0:8B:08:E3:8C	20:80:00:E0:8B:0A:AA:A7	21:80:00:E0:8B:08:E3:8C	21:80:00:E0:8B:0A:AA:A7
Range 7	20:80:00:E0:8B:0A:AA:A8	20:80:00:E0:8B:0C:71:C3	21:80:00:E0:8B:0A:AA:A8	21:80:00:E0:8B:0C:71:C3
Range 8	20:80:00:E0:8B:0C:71:C4	20:80:00:E0:8B:0E:38:DF	21:80:00:E0:8B:0C:71:C4	21:80:00:E0:8B:0E:38:DF
Range 9	20:80:00:E0:8B:0E:38:E0	20:80:00:E0:8B:0F:FF:FB	21:80:00:E0:8B:0E:38:E0	21:80:00:E0:8B:0F:FF:FB
Fabric B				
Range 1	20:81:00:E0:8B:20:00:00	20:81:00:E0:8B:21:C7:1B	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:21:C7:1B
Range 2	20:81:00:E0:8B:21:C7:1C	20:81:00:E0:8B:23:8E:37	21:81:00:E0:8B:21:C7:1C	21:81:00:E0:8B:23:8E:37
Range 3	20:81:00:E0:8B:23:8E:38	20:81:00:E0:8B:25:55:53	21:81:00:E0:8B:23:8E:38	21:81:00:E0:8B:25:55:53
Range 4	20:81:00:E0:8B:25:55:54	20:81:00:E0:8B:27:1C:6F	21:81:00:E0:8B:25:55:54	21:81:00:E0:8B:27:1C:6F
Range 5	20:81:00:E0:8B:27:1C:70	20:81:00:E0:8B:28:E3:8B	21:81:00:E0:8B:27:1C:70	21:81:00:E0:8B:28:E3:8B
Range 6	20:81:00:E0:8B:28:E3:8C	20:81:00:E0:8B:2A:AA:A7	21:81:00:E0:8B:28:E3:8C	21:81:00:E0:8B:2A:AA:A7
Range 7	20:81:00:E0:8B:2A:AA:A8	20:81:00:E0:8B:2C:71:C3	21:81:00:E0:8B:2A:AA:A8	21:81:00:E0:8B:2C:71:C3
Range 8	20:81:00:E0:8B:2C:71:C4	20:81:00:E0:8B:2E:38:DF	21:81:00:E0:8B:2C:71:C4	21:81:00:E0:8B:2E:38:DF
Range 9	20:81:00:E0:8B:2E:38:E0	20:81:00:E0:8B:2F:FF:FB	21:81:00:E0:8B:2E:38:E0	21:81:00:E0:8B:2F:FF:FB

Working with server patterns

A *server pattern* represents pre-OS server configuration, including local storage, I/O adapter, SAN boot, and other baseboard-management-controller and UEFI firmware settings. Server patterns also integrate support for virtualizing I/O addresses so that you can virtualize server fabric connections or repurpose servers without disruption. A server pattern is used as an overall pattern to quickly configure multiple servers at one time.

About this task

You can define multiple server patterns to represent different configurations that are used in your data center.

When defining a server pattern, select or create category patterns and address pools as needed to construct the desired configuration for a specific group of servers. A *category pattern* defines specific firmware settings that can be reused by multiple server patterns. You can use address pools to define address ranges to use to assign addresses to individual servers when deploying server patterns. There are IP address pools, Ethernet Address (MAC) pools, and Fibre Channel Address (WWN) pools.

When a server pattern is deployed to multiple servers, multiple server profiles are generated automatically (one profile for each server). Each profile inherits settings from the parent server pattern, so you can control a common configuration from a single place.

You can create a server pattern from scratch, defining your desired configuration before your hardware arrives. Or, you can create a server pattern from an existing server and then use that pattern to provision your remaining servers. If you create a server pattern from an existing server, extended category patterns are learned and dynamically created from the current settings for the server. If you want to change the category settings, you can edit them directly from the server patterns.

Attention: When you create a new server pattern from scratch, you must define the boot settings for the servers. When you deploy the server pattern to servers, the existing boot order on the servers is overwritten with the default boot-order settings in the server pattern. If the servers do not start after you deploy a server pattern to those servers, the problem might be that the original boot settings were overwritten by the default boot order settings in the new server pattern. To restore the original boot settings on the servers, see Recovering boot settings after server pattern deployment.

Important: When you create server patterns, ensure that you create them for each type of server. For example, create a server pattern for all Flex System x240 compute nodes and another server pattern for all Flex System x440 compute nodes. Do not deploy a server pattern that was created for one server type to another server type.

Important: If the management node fails, you might lose your server patterns. Always back up the management software after you create or modify server patterns (see Backing up Lenovo XClarity Administrator).

Settings for network devices

Some Flex System network devices offer more configuration options in server patterns than others.

Although server patterns can be applied to any network device, some server-patterns functionality is limited to certain network adapters. Additionally, some advanced settings for Ethernet network adapters (such as adapter and port compatibility preferences) are not currently supported.

Server patterns can learn existing configuration data and settings for supported network adapters and can change configuration settings through pattern deployment.

Category patterns

The firmware settings are organized into categories that group together related settings. For each category, you can create a *category pattern* that contains common firmware settings and can be reused by multiple server patterns. Most of the firmware settings that you can configure directly on the baseboard management controller and UEFI can also be configured through category patterns. The firmware settings that are available depend on the server type, your Flex System environment, and the scope of the server pattern.

You can create category patterns separately from server patterns.

Category patterns can be predefined, learned from existing servers, or user-defined.

- **Extended category patterns**

  Extended category patterns are patterns for some I/O adapter ports, advanced Unified Extensible Firmware Interface (UEFI), and baseboard management-controller (BMC) settings that are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended category patterns; however, you can edit the patterns after they are created.

  The following Extended UEFI patterns are predefined by XClarity Administrator to optimize your servers for specific environments.
  - **ESXi Install Options**
  - **Efficiency – Favor Performance**
  - **Efficiency – Favor Power**
  - **Maximum Performance**
  - **Minimal Power**
- **User-defined category patterns**

  User-defined category patterns are patterns that you can create, including system information, management interfaces, devices and I/O ports, Fibre Channel boot targets, and I/O adapter ports. You can create the following category patterns:

  - **System information**. Settings include automatically generated system name, location, contacts.
  - **Management interface**. Settings include the automatically generated hostname, IP address, domain name space (DNS), interface speed, and port assignments for the management interface.Duplex settings are not supported by server patterns.
  - **Devices and I/O ports**. Settings include console redirection and COM ports. You can use server patterns to enable serial over LAN in the Console Redirection area. However, when serial over LAN is enabled, the only serial-port access mode setting that is supported by server patterns is **Dedicated**; the **Shared** and **Pre-Boot** IPMI settings for serial-port access mode are not available in server patterns.

    Important: If you create a server pattern from an existing server, and that server has the serial-port access mode setting **Shared** or **Pre-Boot**, the device and I/O ports pattern that is learned from the server has the serial-port access mode setting **Dedicated**.
  - **Fibre Channel boot targets**. Settings include specific primary and secondary Fibre Channel WWN boot targets.
  - **Ports**. Settings include I/O adapters and ports for configuring fabric interconnects.

Creating a server pattern

When you create a server pattern, you define the configuration characteristics for a specific type of server. You can create a server pattern from scratch using default settings or using settings from an existing server.

About this task

Before you create a server pattern, consider the following suggestions.

- The first time that you create a server pattern, consider creating it from an existing server. When you create a server pattern from an existing server, Lenovo XClarity Administrator learns and creates extended category patterns for some I/O adapter ports, UEFI, and baseboard management controller settings. Then, those category patterns are available for use in any server pattern that you create later. For more information about category patterns, see Defining firmware settings.
- Identify groups of servers that have the same hardware options and that you want to configure the same way. You can use a server pattern to apply the same configuration settings to multiple servers, thereby controlling a common configuration from one place.

- Identify the aspects of configuration that you want to customize for the server pattern (for example, local storage, network adapters, boot settings, management controller settings, UEFI settings).
- You cannot manage local user accounts or configure the LDAP server using Configuration Patterns.

Important: If the management node fails, you might lose your server patterns. Always back up the management software after you create or modify server patterns (see Backing up Lenovo XClarity Administrator).

Procedure

To create a server pattern, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

Step 3. Click the **Create** icon ( ). The New Server Pattern Wizard is displayed.

Step 4. To create the server pattern, perform one of the following actions.

- Click **Create a new pattern from an existing server** to use settings from an existing server. Then, select the managed server on which the new pattern is to be based from the displayed list.

  When you create a server pattern from an existing server, XClarity Administrator learns the settings from the specified managed server (including the extended port, UEFI, and management-controller settings) and dynamically creates category patterns for those settings. If the server is brand new, Lenovo XClarity Administrator learns the manufacturing settings. If XClarity Administrator is managing the server, XClarity Administrator uses the customized settings. You can then customize the settings specifically for the servers to which this pattern is to be deployed.
- Click **Create a new pattern from scratch** to use default settings. Then, select the server type in the **Form Factor** field.

Note: The options that are presented on the remaining tabs might differ depending on the type of server for which you are creating a pattern.

Step 5. Enter the name of the pattern and a description.

Step 6. Optional: Customize the server-profile name by selecting the **Custom** toggle and then selecting one or more elements to include in the naming schema (such as custom text, server name, and incrementing number) and the order.

Step 7. Click **Next**

Step 8. Choose the local storage configuration to be applied when this pattern is deployed to a server, and click **Next**.

For information about local storage settings, see Defining local storage.

Step 9. Optional: **Optional:** Modify the I/O adapter addressing, and define additional I/O adapters to match the hardware that you expect to configure with this pattern, and click **Next**.

For information about I/O adapter settings, see Defining I/O adapters.

Step 10. Define the boot order to be applied when this pattern is deployed to a server, and click **Next**.

For information about SAN boot targets settings, see Defining boot options.

Step 11. Select firmware settings from the list of existing category patterns.

You can create new category patterns by clicking the **Create** icon ( ).

For information about firmware settings, see Defining firmware settings.

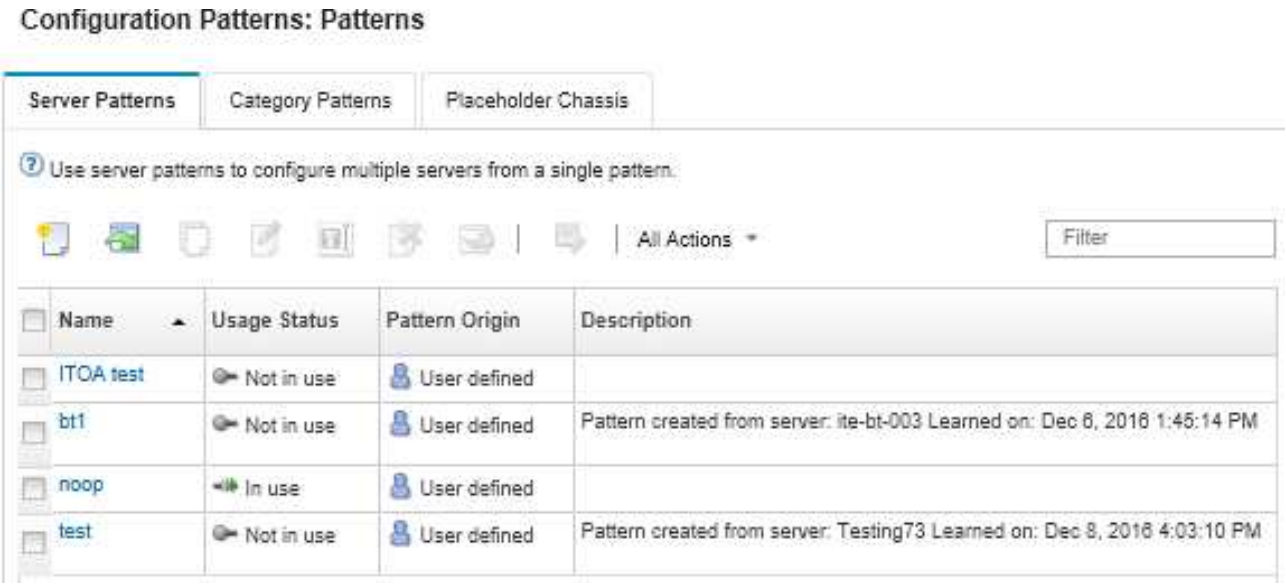
Step 12. Click **Save** to save the pattern, or click **Save and Deploy** to save and immediately deploy the pattern to one or more servers.

For information about deploying a server pattern, see Deploying a server pattern to a server.

After you finish

If you clicked **Save and Deploy**, the Deploy Server Pattern page is displayed. From this page, you can deploy the server pattern to specific servers.

If you clicked **Save**, the server pattern and all category patterns are saved to the Server Patterns page.



From this page, you can perform the following actions on selected server patterns:

- View details about the pattern by clicking the pattern name in the **Name** column.
- Deploy the pattern (see Deploying a server pattern to a server).
- Copy the pattern by clicking the **Copy** icon ( ).
- Edit the pattern (see Modifying a server pattern).
- Rename the pattern by clicking the **Rename** icon ( ).
- Delete the pattern by clicking the **Delete** icon ( ).
- Export and import server patterns (see Exporting and importing server and category patterns).

Defining local storage

You can define the local-storage configuration to be applied to target servers when this pattern is deployed.

About this task

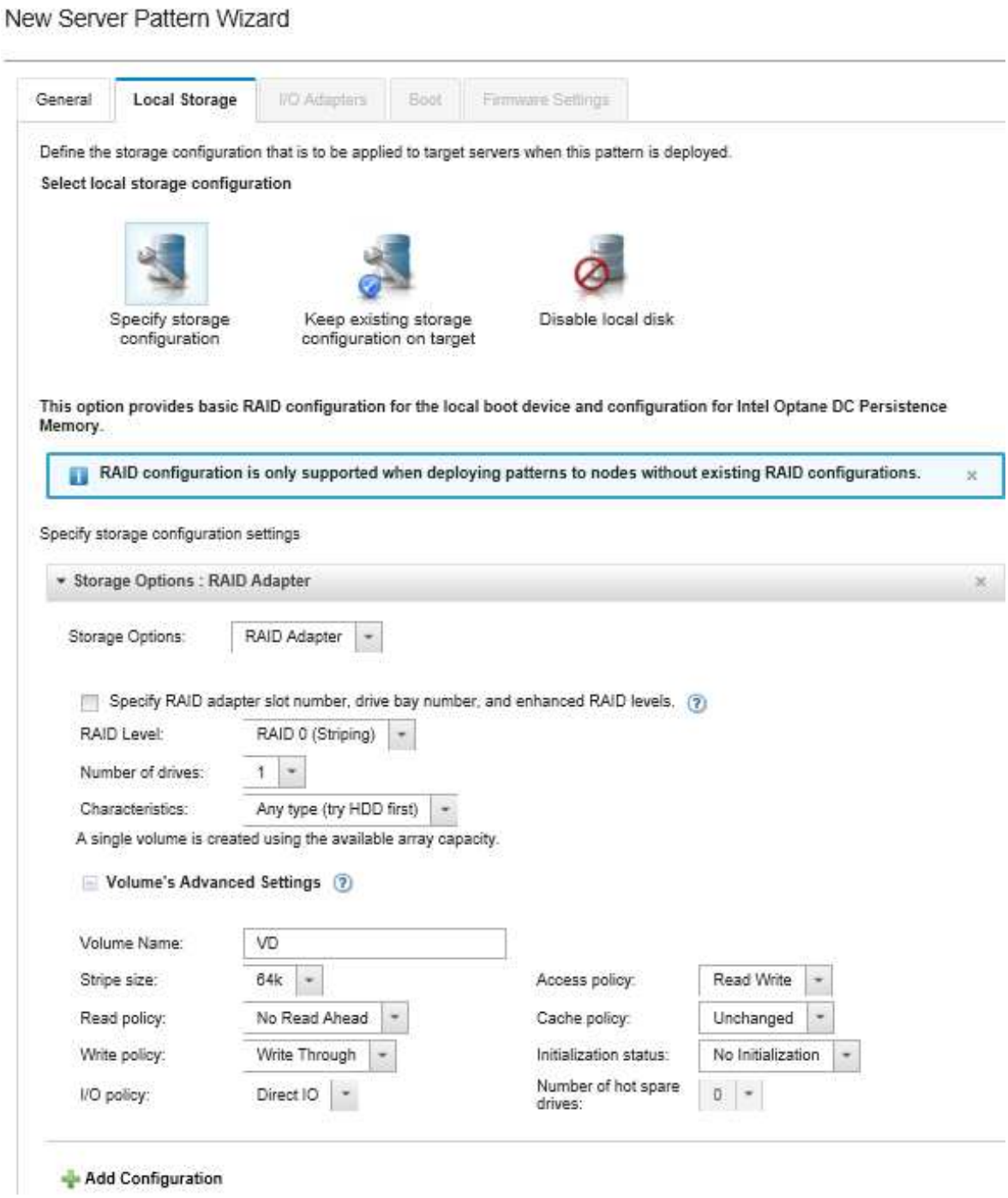
Notes:

- The onboard storage controllers in Flex System x220, Flex System x222, and ThinkSystem servers support software-based RAID. However, configuration of software RAID using Configuration Patterns is not supported.
- When configuring RAID using Configuration Patterns, if the server is powered off, the server boots to BIOS/UEFI Setup automatically before activating the server profile.

Procedure

To define the local-storage configuration, complete the following steps.

Step 1. From the New Server Pattern Wizard, click the **Local Storage** tab.



Step 2. To define local-storage settings, choose one of the following options.

- **Specify storage configuration**. (Devices without exiting RAID configurations only) Basic RAID settings are configured on the local boot device during deployment

  Specify the storage configuration based on the storage option. You can add additional storage options by clicking the **Add** (+) icon.

- **RAID Adapter**. Choose the RAID level, characteristics, and the number of drives that are installed in the server. RAID 0, 1, 5 are supported. In addition, you can choose advanced volume settings, such as stripe size, policies, and number of hot spare drives.

  ThinkSystem servers with XCC version 2.1 and later (ThinkSystem SR950 requires XCC version 1.4 or later), you can also specify the RAID adapter slot number and drive bay numbers to create a single volume using the available array capacity. In this case, RAID level 0, 1, 5, 6, 10, 50, 60, and 00 are supported. In addition, you can choose advanced volume settings, such as stripe size, policies, and hot spare drives.

  Note: On the target server, ensure that there are enough available drives of the specified type, and ensure that the RAID state of the drives is "Unconfigured Good," as reported in the **Drives** section on the servers Inventory Details page (see Viewing the details of a managed server).
- **Lenovo SD Media Adapter**. Choose the where to create the volume and the volume size. You can also choose advanced volume settings, such as media type and access policy.
- **ThinkSystem M.2 with Mirroring**. Choose the PCI slot, RAID level, volume name, and stripe size to create a single volume using the available array capacity.
  - You can define multiple ThinkSystem M.2 with Mirroring storage adapters, each in a different PCI slot.
  - For ThinkSystem Edge Servers, you must specify a specific PCI slot number. For other ThinkSystem servers that have only one M.2 RAID adapter installed, you can choose First Matched (the default value) or specify a specific PCI slot number.
- **Intel Optane DC Persistent Memory**. Choose the type of persistent memory, warning threshold for the percentage of remaining capacity, and percentage of total capacity to be used as memory. (The remaining memory is used as persistent storage).

  Attention:
  - To configure Intel Optane DC Persistent Memory DIMMs, security must be disabled and a namespace must not be created.
  - Enable Security is supported only when the security state is “Disabled” for all Intel Optane DC Persistent Memory DIMMs in the server.
  - Disable Security and Secure Erase are supported only when the security state is “Locked” and the passphrase is the same for all Intel Optane DC Persistent Memory DIMMs in the server.
  - The Intel Optane DC PMEM security state is not included in the XClarity Administrator inventory. You can manually check the security state in UEFi.

- **Keep existing storage configuration on target**. The existing storage configuration is not changed during deployment. Choose this option to use the storage configuration that is already in place on the target server.
- **Disable local disk**. (Flex System x240 Compute Node only) The on-board storage controller and storage option ROM (both UEFI and Legacy) are disabled during deployment. Disabling the local disk drive decreases the overall boot time when booting from SAN.

Defining I/O adapters

You can define I/O port settings and addressing mode to be applied to target servers when this pattern is deployed.

About this task

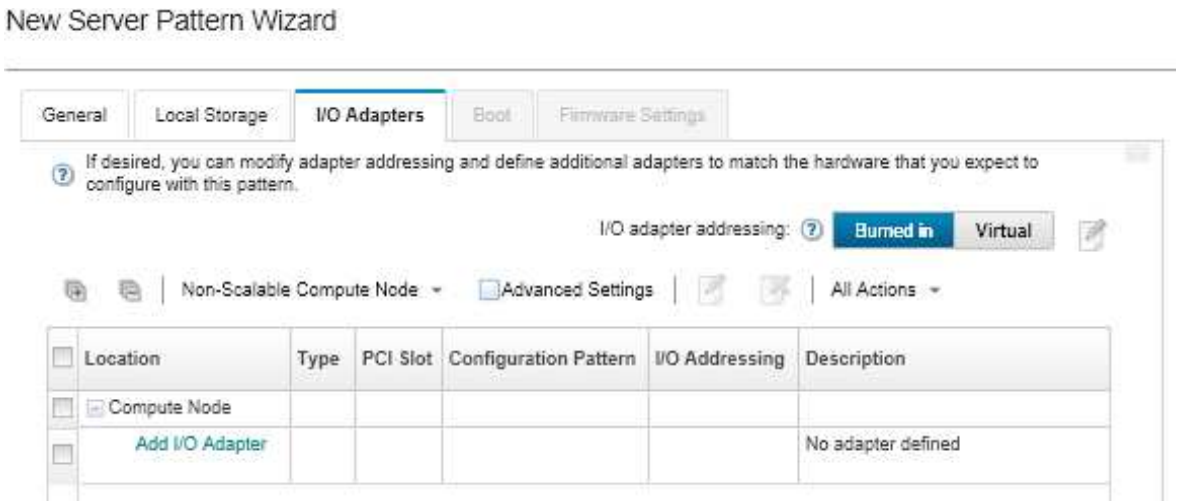
If you intend to virtualize or reassign your I/O adapter addresses, you can configure this pattern to use virtual I/O adapter addressing.

If you are creating a pattern from an existing server, some adapter information might be automatically learned. You can define additional I/O adapter patterns to match the hardware that you expect to have in the servers when this pattern is deployed. By defining I/O adapter patterns, you can configure adapter-port settings for your supported adapter. If using virtual I/O adapter addresses, you can also define SAN boot targets for Fibre Channel adapters that you add (see Defining boot options).

Procedure

To define I/O adapter settings, complete the following steps.

Step 1. From the New Server Pattern Wizard, click the **I/O Adapters** tab.



Note: You can display additional information about the I/O adapters by clicking **Advanced Settings**.

Step 2. If you are creating a server pattern for a server in a Flex System chassis, choose the type of I/O-adapter addressing mode:

- **Burned in**. Use existing World Wide Name (WWN) and Media Access Control (MAC) addresses that are provided with the adapter from manufacturing.
- **Virtual**. Use virtual I/O adapter addressing to simplify the management of LAN and SAN connections. Virtualizing I/O-addresses reassigns the burned-in hardware addresses with virtualized Fibre WWN and Ethernet MAC addresses. This can speed deployment by pre-configuring SAN zone membership and facilitate failover by eliminating the need to reconfigure SAN-zoning and LUN-masking assignments when replacing hardware.

  When virtual addressing is enabled, both Ethernet and Fibre Channel addresses are allocated by default regardless of defined adapters. You can choose the pool from which Ethernet and Fibre Channel addresses are allocated.

  You can also edit virtual-address settings by clicking the **Edit** icon ( ) next to the address modes.

  Restriction: Virtual addressing is supported for only servers in Flex System chassis. Rack and tower servers are not supported.

Step 3. If you are creating a server pattern for a server in a Flex System chassis, select one of the following scalability options. The rows in the table change based on what is selected.

- Non-scalable Flex system
- 2 node scalable Flex system
- 4 node scalable Flex system

Step 4. Choose the I/O adapters that you expect to be installed in the servers to which the pattern is to be deployed. To add an adapter:

a. Click the **Add I/O Adapter** link in the table to display the Add I/O Adapter 1 or LOM dialog.

b. Select the PCI slot for the adapter.

c. Select the adapter type from the table.

Note: By default, the table lists only I/O adapters that are currently installed in the managed servers. To list all supported I/O adapters, click **All Supported Adapters**.

d. Select the initial port pattern to be assigned to all ports in the port group when the pattern is deployed.

Port patterns are used to modify port settings that are learned from the server. These initial port patterns are assigned when the adapter is first added. After the adapter is added, you can assign different patterns to individual ports from the I/O Adapter page.

You can create a port pattern by clicking the **Create** icon ( ). You can create a port pattern based on an existing pattern by clicking the **Edit** icon ( ).

For more information about port patterns, see Defining port settings.

e. Click **Add** to add the port pattern to the table on the I/O Adapter page.

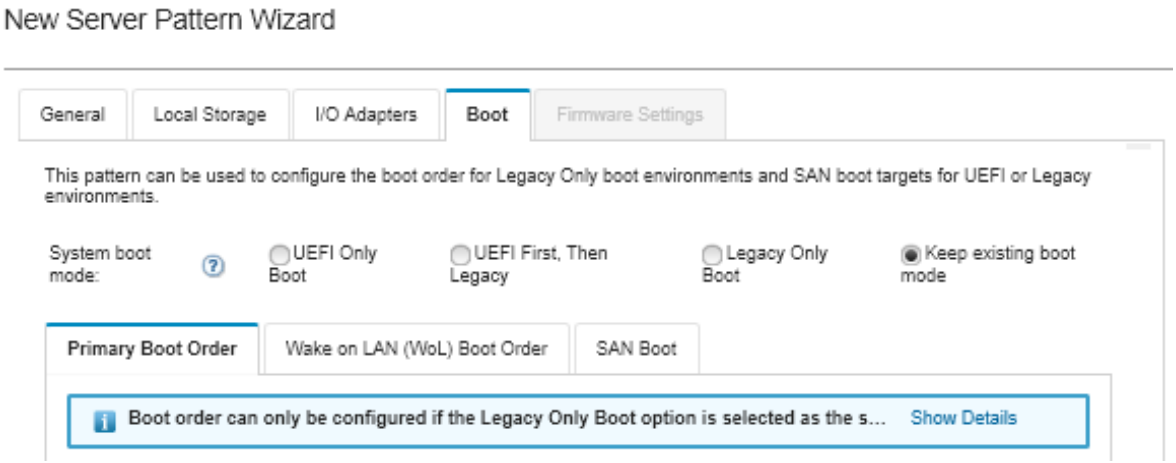
Defining boot options

You can define the boot order to be applied to the target servers when this pattern is deployed.

Procedure

Complete the following steps to create a boot-options pattern.

Step 1. From the New Server Pattern Wizard, click the **Boot** tab.



Step 2. Select one of the following system-boot modes:

- **UEFI Only Boot**. Select this option to configure a server that supports Unified Extensible Firmware Interface (UEFI). If you are booting UEFI-enabled operating systems, this option might shorten boot time by disabling legacy option ROMs.

  If the pattern is learned from a Thinksystem server, you can click the **Primary Boot Order** tab to specify the boot order. You can keep the boot order that is specified on the server to which the pattern is to be deployed or configure the boot order to specify the order in which boot options

are to be applied. However, boot priority of boot devices in a device group (boot option) is not supported.

- **UEFI First, Then Legacy**. Select this option to configure a server to attempt to boot using UEFI first. If there is an issue, the server attempts to boot in legacy mode.

  If the pattern is learned from a Thinksystem server, you can click the **Primary Boot Order** tab to specify the boot order. You can keep the boot order that is specified on the server to which the pattern is to be deployed or configure the boot order to specify the order in which boot options are to be applied. However, boot priority of boot devices in a device group (boot option) is not supported.

- **Legacy Only Boot**. Select this option if you are configuring a server to boot an operating system that requires legacy (BIOS) firmware. Select this option only if you are booting non-UEFI enabled operating systems.

  Tip: If you select the legacy-only boot mode (which makes boot time much faster), you cannot activate any Features on Demand (FoD) keys.

  If you choose this option, you can specify:

  – **Primary Boot Order**. Choose to keep the boot order specified on the server to which the pattern is to be deployed. You can also choose to configure the Legacy Only boot order to specify the order in which boot options are to be applied.

  – **Wake on LAN (WoL) Boot Order**. Choose to keep the current WoL boot order specified on the server to which the pattern is to be deployed. You can also choose to configure the Legacy Only boot order to specify the order in which WoL boot options are to be applied.

- **Keep existing boot mode**. Select this option to keep the existing settings on the target server. No changes to the boot order are made when the pattern is deployed.

Step 3. Select the **SAN Boot** tab to choose a boot target pattern and specify boot device targets.

Note: If you defined Fibre Channel adapters and enabled virtual addressing when you defined the I/O adapters, you can set SAN primary and secondary boot targets for the Fibre Channel adapters. You can specify multiple worldwide port name (WWPN) and logical unit number (LUN) identifiers for the storage targets.

Defining firmware settings

You can specify the baseboard management controller and UEFI firmware settings that are to be applied to target servers when this pattern is deployed.

About this task

The firmware settings are organized into categories that group together related settings. For each category, you can create a *category pattern* that contains common firmware settings and can be reused by multiple server patterns. Most of the firmware settings that you can configure directly on the baseboard management controller and UEFI can also be configured through category patterns. The firmware settings that are available depend on the server type, your Flex System environment, and the scope of the server pattern.

Category patterns can be predefined, user-defined, or learned from existing servers:

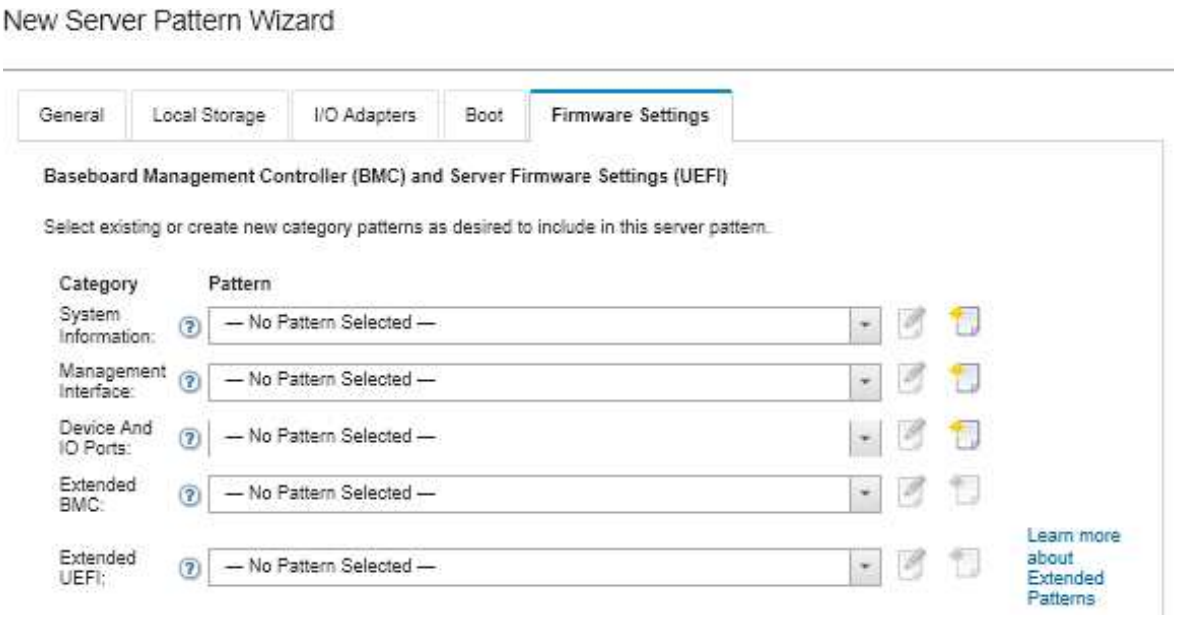
- *Extended category patterns* are patterns for some I/O adapter ports, advanced Unified Extensible Firmware Interface (UEFI), and baseboard management-controller (BMC) settings that are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended category patterns; however, you can edit the patterns after they are created.

- *User-defined category patterns* are patterns that you can create, including system information, management interfaces, devices and I/O ports, Fibre Channel boot targets, and I/O adapter ports.

Procedure

Complete the following steps to define firmware settings.

Step 1. From the New Server Pattern Wizard, click the **Firmware Settings** tab.



Step 2. Choose the category-pattern type that includes the settings that you want to define.

- **System information**. Use this category pattern to define automatic system-name generation, contact names, and locations. For more information about system-information patterns, see Defining system-information settings.
- **Management interfaces**. Use this category pattern to define automatic host-name generation, management IP-address assignments, domain name system (DNS) settings, and internet speed settings. For more information about management-interfaces patterns, see Defining management-interface settings).
- **Devices and I/O ports**. Use this category pattern to define console redirection and COM ports, PCIe speed, onboard devices, adapter option ROM, and option ROM execution order. For more information about device and I/O port patterns, see Defining devices and I/O ports settings.
- **Extended BMC**. Use this category pattern to define other baseboard management-controller settings. The extended management-controller patterns are automatically created when you create a server pattern from an existing server. You cannot manually create an extended management-controller pattern. For more information about management-interfaces patterns, see Defining extended management-controller settings.).
- **Extended UEFI**. Use this category pattern to define other Unified Extensible Firmware Interface (UEFI) settings. The extended UEFI patterns are automatically created when you create a server pattern from an existing server. You cannot manually create an extended UEFI pattern. For more information about management-interfaces patterns, see Defining extended UEFI settings).

Step 3. Create new category patterns by clicking the **Create** icon ( ) next to that category-pattern type.

You can also edit an existing category pattern by selecting a specific pattern from the drop-down list and clicking the **Edit** icon ( ) next to that category-pattern type. You can also copy an existing category pattern by editing the pattern and clicking **Save As** to save it with a new name.

Defining system-information settings

You can define system name, contact, and location information by creating a system information pattern.

Procedure

Complete the following steps to create a system-information pattern.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **System Information Patterns** vertical tab, and then click the **Create** icon ( ).

Tip: You can also create a new system-information pattern from the Firmware Settings page of the New Server Pattern wizard by clicking the **Create** icon next to the **System Information** selection.

Step 4. In the New System Information Pattern dialog, specify the following information.

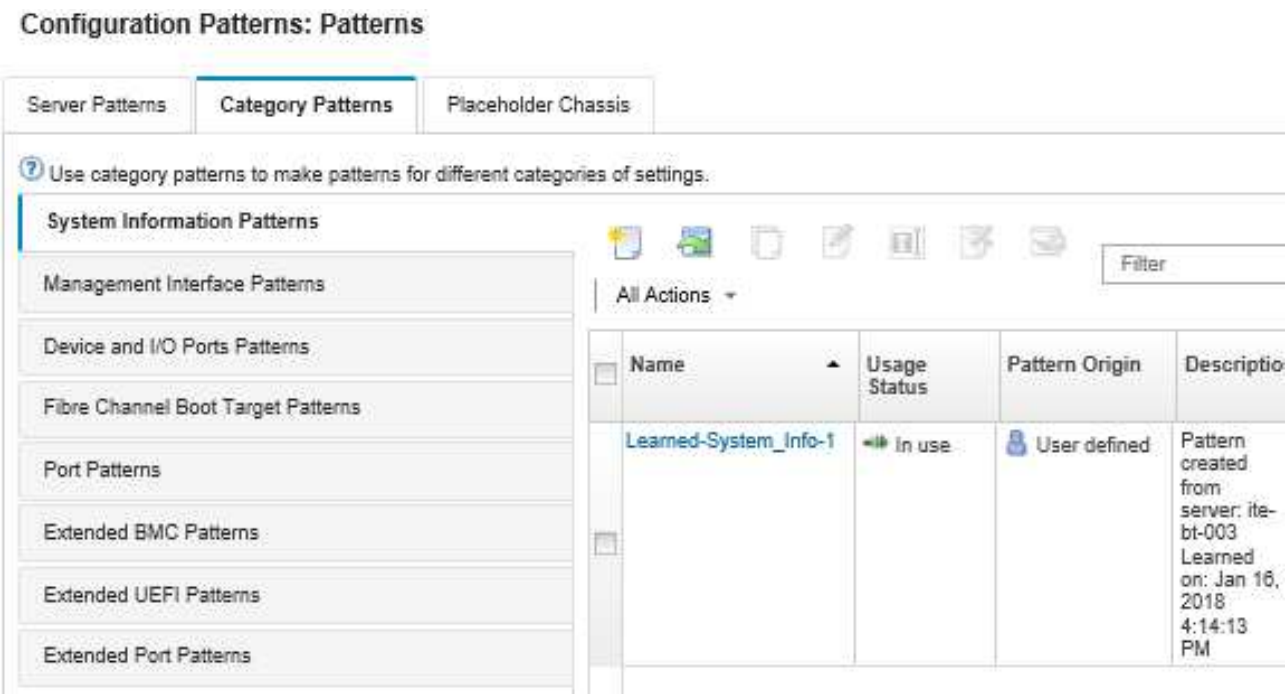
- Enter a name and description for the pattern.
- Choose whether to automatically generate system names. If you click **Custom**, you can specify how names are to be generated when the pattern is deployed. If you click **Disable**, the system name remains unchanged on each server when the pattern is deployed. For most devices, the name is limited to 256 English characters by the baseboard management controller. Automatically generated names are truncated to 256 characters.
- Specify the person to be contacted for this server and the location of the server.

  Note: If SNMP is enabled, you must specify a contact and system location.

Step 5. Click **Create**.

Results

The new pattern is listed on the **System Information Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining management-interface settings

You can define hostnames, IP address, domain name system (DNS), interface speed, and port assignments for the management interface by creating a management interface pattern.

Procedure

Complete the following steps to create a management-interface pattern.

Note: Duplex settings are not supported by server patterns.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Management Interface Patterns** vertical tab, and then click the **Create** icon ( ).

Tip: You can also create a new management-interface pattern from the Firmware settings page of the New Server Pattern wizard by clicking the **Create** icon ( ) next to the **Management Interface** selection.

Step 4. In the New Management Interface Pattern dialog, specify the following information.

- Enter a name and description for the pattern.

- Click the **Hostname** tab, and choose whether to automatically generate hostnames. If you click **Custom**, you can specify how names are to be generated when the pattern is deployed. If you click **Disable**, the hostname remains unchanged on each server when the pattern is deployed.

  Hostnames are limited to 63 English characters by the baseboard management controller. Automatically generated names are truncated to 63 characters.
- Click the **Management IP Addresses** tab, and configure IPv4 and IPv6 addresses settings.

  For **IPv4** addresses, you can choose one of the following options:
  - **Obtain dynamic IP address from DHCP server**.
  - **First by DHCP**. If it is not successful, obtain a static IP address from the address pool.
  - **Obtain a static IP address from the address pool.**

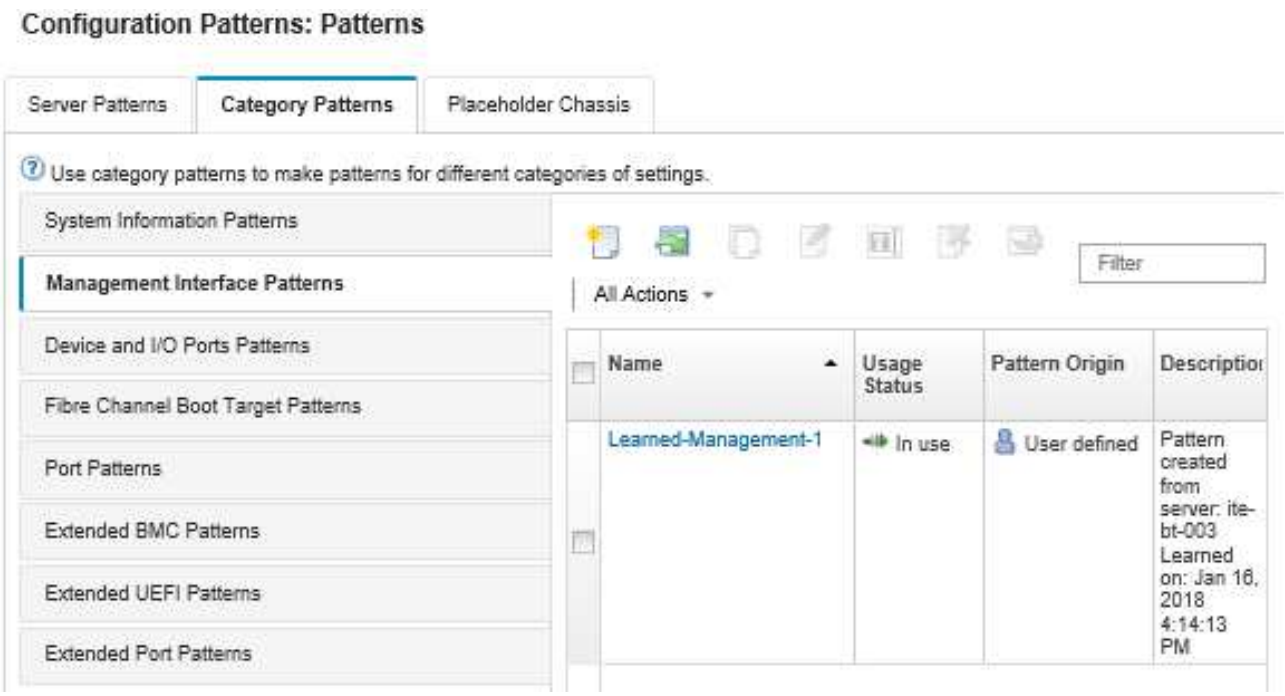
  For **IPv6** addresses, you can choose to:
  - **Use the stateless address auto configuration**.
  - **Obtain a dynamic IP address from a DHCP server**.
  - **Obtain a static IP address from the address pool**.

  In the **Domain Name System (DNS)** tab, choose to enable or disable the Dynamic Domain Name Service (DDNS). If you enable DDNS, you can choose one of the following options:
  - Obtain domain name from DHCP server.
  - Specify a domain name.
- Click the **Interface Settings** tab, and specify the maximum transmission unit (MTU). The default is 1500.
- Click the **Port Assignments** tab, and specify the numbers to use for the following ports:
  - HTTP
  - HTTPS
  - Telnet CLI
  - SSH CLI
  - SNMP agent
  - SNMP traps
  - Remote control console
  - CIM over HTTP
  - CIM over HTTPS

Step 5. Click **Create**.

Results

The new pattern is listed on the **Management Interface Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining devices and I/O ports settings

You can enable console redirection and enable and define the characteristics of the COM 1 port by creating a device and I/O ports pattern.

Procedure

To create a device and I/O ports pattern, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Devices and I/O Ports Patterns** vertical tab, and then click the **Create** icon ( ).

Tip: You can also create a devices and I/O ports pattern from the Firmware Settings page of the New Server Pattern wizard by clicking the **Create** icon ( ) next to the **Devices and I/O Ports** selection.

Step 4. In the New Devices and I/O Ports Pattern dialog, specify the following information.

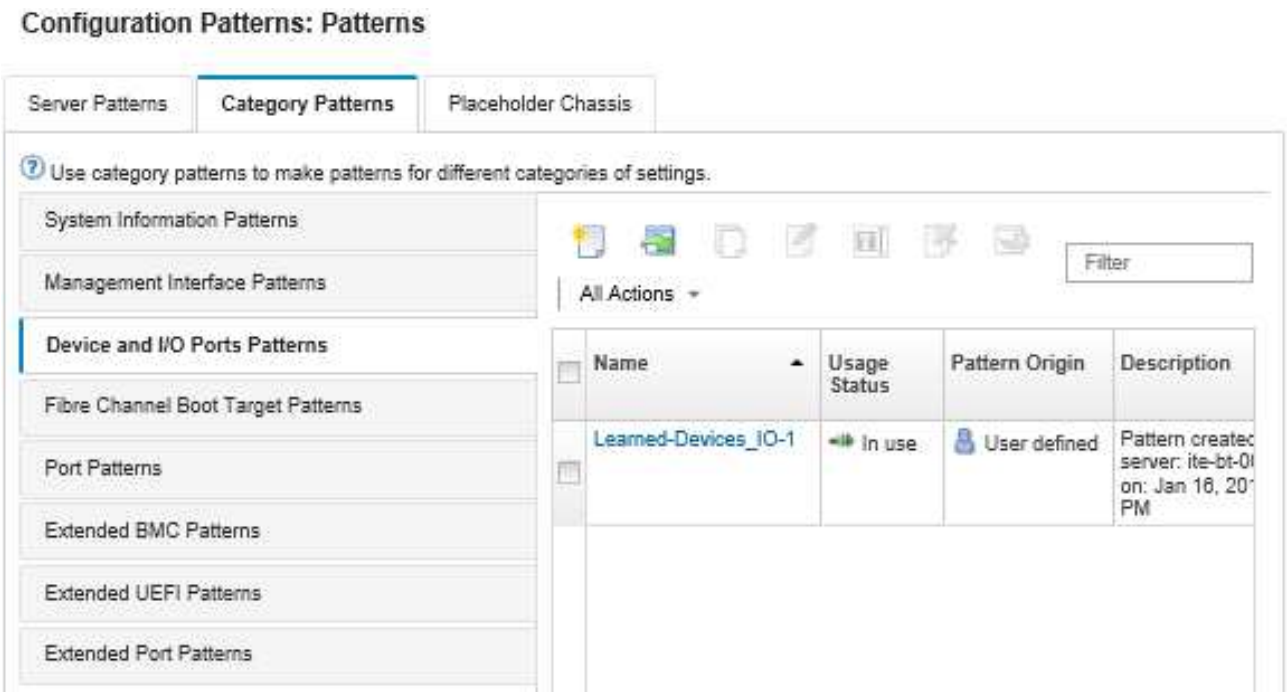
- Enter a name and description for the pattern.
- Choose to enable or disable console redirection. If you enable console redirection, you can choose to enable or disable the following:
  - **Serial over LAN**.

  - **Service processor redirection**. If you enable service processor redirection, you can choose to use COM port 1 or 2 for the Legacy optional serial data port. Note that if disabled, COM port 1 is always used.You can also choose one of the following CLI modes:
    - Disable
    - Enable with user-defined keystroke sequence
    - Enable with EMS compatible keystroke sequence
- Choose to enable or disable COM ports 1 and 2. If you choose to enable COM ports, specify the following settings:
  - Baud rate
  - Data bits
  - Parity
  - Stop bits
  - Text emulation
  - Active after boot
  - Flow control

Step 5. Click **Create**.

Results

The new pattern is listed on the **Devices and I/O Ports Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining Fibre Channel boot-target settings

You can configure the server to boot from a storage area network (SAN) device instead of from local disk drive by creating a Fibre Channel boot-target pattern.

Procedure

Complete the following steps to create a Fibre Channel boot-target pattern.

Restriction: Fibre Channel boot targets are supported for only Flex compute nodes. Standalone rack and tower servers are not supported.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Fibre Channel Boot Target Pattern** vertical tab, and then click the **Create** icon ( ).

Step 4. In the New Fibre Channel Boot Target Pattern dialog, specify the following information.

- Enter a name and description for the pattern.
- Specify one or more WWPN addresses and LUN identifiers to use as primary boot targets. In addition, you can optionally specify one or more WWPN addresses and LUN identifiers to use as secondary boot targets.

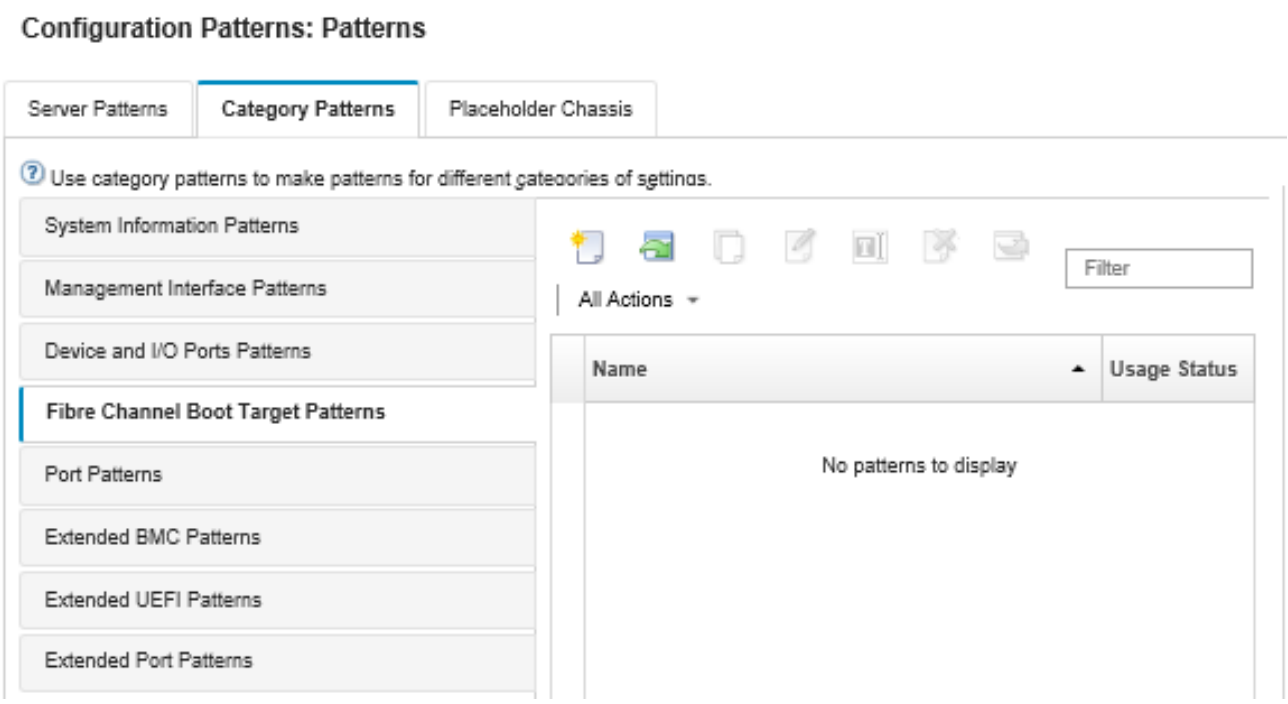
  For example, you can add the storage primary paths as primary targets, and the storage secondary paths as secondary targets. By using different target groups in different server patterns, you can balance the storage load during simultaneous boot requests from multiple hosts.

  Tip: If you specify `00:00:00:00:00:00:00:00` for the WWPN, XClarity Administrator attempts to boot from the first discovered target.

Step 5. Click **Create**.

Results

The new pattern is listed on the **Fibre Channel Boot Target Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining port settings

You can define typical port settings for a specific I/O adapter type by creating a port pattern.

About this task

You can use network settings in port patterns to configure switch internal ports. However, you cannot use port patterns to configure the switch global settings, such as VLAN IDs, global UFP mode, global CEE mode, and global FIPs. You must manually configure the global settings using the following rules that are compatible with the internal port settings that you intend to deploy before you deploy the port patterns. You also cannot use port patterns to configure the PVID tagging. See the documentation that came with your switch to determine the compatibility checks between the global settings and internal port settings and how to configure these settings for that switch.

- Ensure that **globalCEEState** is “On” when PFC is configured.
- Ensure that **globalCEEState** is “On” when vport is set to “FCoE” mode.
- Ensure that **globalCEEState** is “On” and **globalFIPsState** is “On” when FIPs are configured.
- Ensure that **globalUFPMode** is “Enable” when the switch internal port mode is set to “UFP” mode.
- Ensure that the VLAN ID is created before adding a port to a specific VLAN.

Procedure

Complete the following steps to create an I/O adapter port pattern.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Port Pattern** vertical tab, and then click the **Create** icon ( ).

Tip: You can also create a new port pattern from the Add I/O Adapter page by clicking the **Create** icon ( ) next to the **Initial port pattern** selection.

Step 4. In the New Port Pattern dialog, specify the following information.

- Enter a name and description for the pattern.
- Specify the following adapter and port compatibility settings. When assigning patterns to adapters and ports, pattern settings are filtered based on compatibility with the target adapter or port.
  - Target adapter type
  - Target port operational mode, including:
    - pNIC mode
    - vNIC virtual fabric mode
    - vNIC switch independent mode
    - vNIC unified fabric protocol mode

    These settings enable NIC virtualization. For more information, see NIC Virtualization in Flex System Fabric Solutions.
  - Target port protocols, including:
    - Ethernet only
    - Ethernet and FCoE
    - Ethernet and iSCSI
  - Port extended settings pattern, which is used to configure additional port settings that are learned from the server
- If you set the target port operational mode to **pNIC mode**, choose to apply corresponding settings to the Flex switch internal ports, where applicable. If selected, you can configure additional VLAN and advanced settings:
  - Specify the target port protocol.
  - If you set the target port protocol to **Ethernet and FCoE**, optionally select and specify the priority 2 ID.
- If you set the target port operational mode to **vNIC virtual fabric mode**, configure the physical function settings, including the type and VLAN tag for each function.
- If you set the target port operational mode to **vNIC switch independent mode**, specify the type, minimum bandwidth and VLAN tag for each enabled function. You can also choose to apply corresponding settings to the Flex switch internal ports, where applicable. If selected, you can configure additional switch internal port and advanced settings:
  - Specify the default LAN, which is used only by the operating system when the operating system sends untagged packets.
  - Specify a comma separated list of VLANs.
  - Choose to configure manual control and specify the triggers.
  - Choose to configure flow control type, including
    - Keep existing flow control
    - Priority-based flow control
    - Link-level flow control

For more information about these flow-control types, see the documentation that came with your Flex switch.

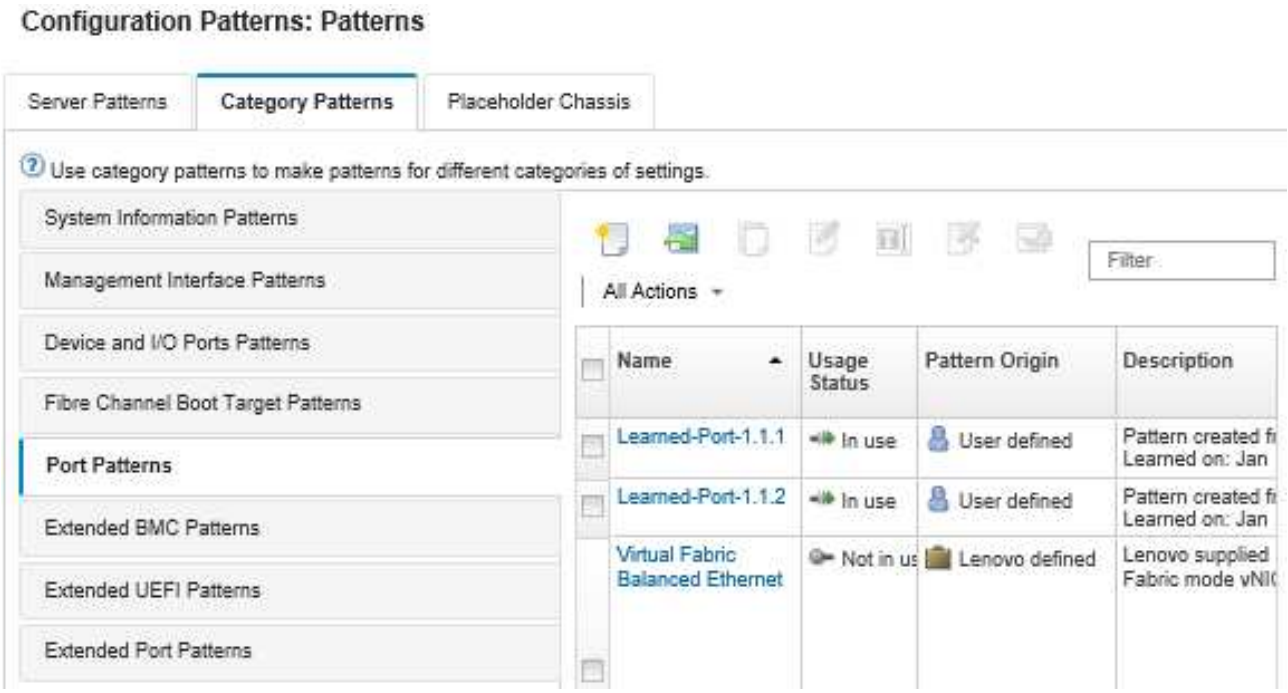
- If you set the target port operational mode to **vNIC unified fabric protocol mode**, choose to apply corresponding settings to the Flex switch internal ports, where applicable. If selected, you can configure additional UFP function and advanced settings:
  - Specify the QoS Mode (bandwidth or priority).
  - Choose to enable default VLAN ID tagging and specify the mode, minimum bandwidth and VLAN tag for each enabled function.
  - Choose to configure layer 2 failure and specify the number of triggers for each function.
  - For bandwidth QoS mode, specify the flow control type (priority based, link-level, or existing flow control).
  - For bandwidth QoS mode, choose to whether priority 4 is enabled when iSCSI is selected.

  Note: Ensure that global failover is “On” when defining failover triggers.

Step 5. Click **Create**.

Results

The new pattern is listed on the **Port Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Modifying current pattern settings by clicking the **Edit** icon ( ).
- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended management-controller settings

The extended baseboard management-controller settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server

pattern from an existing server. You cannot manually create extended management-controller patterns; however, you can copy and modify the patterns that have already been created.

Before you begin

Note: IMM thermal setting might conflict with the UEFI operating-mode setting. If they do conflict, the UEFI settings overwrites the IMM setting when the device is rebooted, and any thermal settings that you define in an extended baseboard management-controller pattern will be out of compliance. To resolve the non-compliance issue, either remove the setting from the extended baseboard management-controller pattern or select a setting that does not conflict with the current UEFI operating-mode setting.

Procedure

Complete the following steps to modify extended management-controller patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended BMC Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ( ).

Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

- To configure DNS settings, click **Network Settings Interface → DNS Configuration**. You can enable DNS, select the IP protocol, and specify up to three IPv4 or IPv6 addresses, and enable the discovery of XClarity Administrator IP addresses.

  Note: For Flex System devices, you can configure only the IP address to use to discover the XClarity Administrator server.

- To configure NTP settings, click **Network Settings Interface → Integrated Module NTP Setting**. You can specify the host name for up to 4 NTP servers and the frequency.

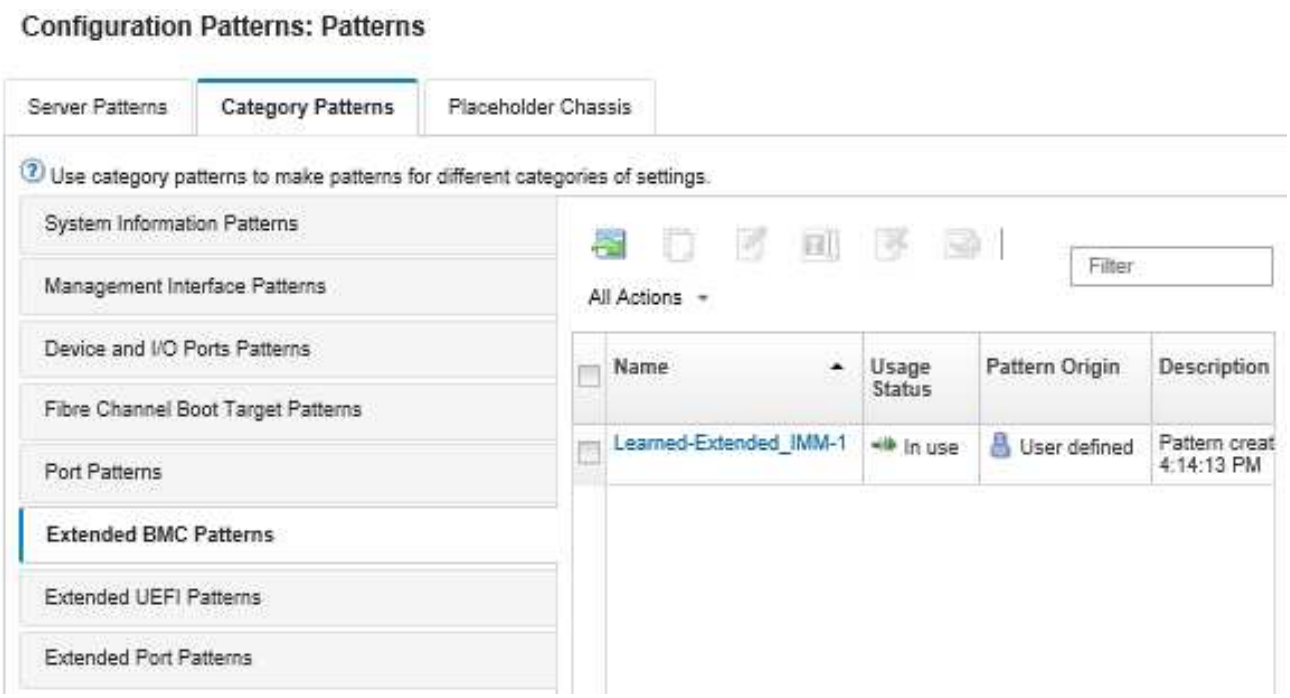
  Note: For Flex System devices, you cannot configure NTP settings.

- (Rack servers only) To data and time settings, click **General Settings → Integrated Module Clock Settings**. You can specify the time zone (UTC offset), enable or disable daylight savings time (DST), and choose whether to use UTC or the local time on the host.
- To change user account security settings, click **Account Security Configuration**.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended BMC Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended UEFI settings

The extended Unified Extensible Firmware Interface (UEFI) settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended UEFI patterns; however, you can copy and modify the patterns that have already been created.

About this task

The following Extended UEFI patterns are predefined by Lenovo XClarity Administrator to optimize your servers for specific environments.

- **ESXi Install Options**
- **Efficiency – Favor Performance**
- **Efficiency – Favor Power**
- **Maximum Performance**
- **Minimal Power**

Notes:

- Modification of UEFI security settings (including secure boot, trusted platform module (TPM), and physical presence policy configuration) are not supported using Extended UEFI Patterns.
- You can modify the UEFI administrator password for selected ThinkSystem and ThinkAgile servers from the Servers page by clicking **All Actions → Security → UEFI Administrator Password**. Lenovo XClarity Controller firmware level 20A is required.

Procedure

Complete the following steps to modify extended UEFI patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended UEFI Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ( ).

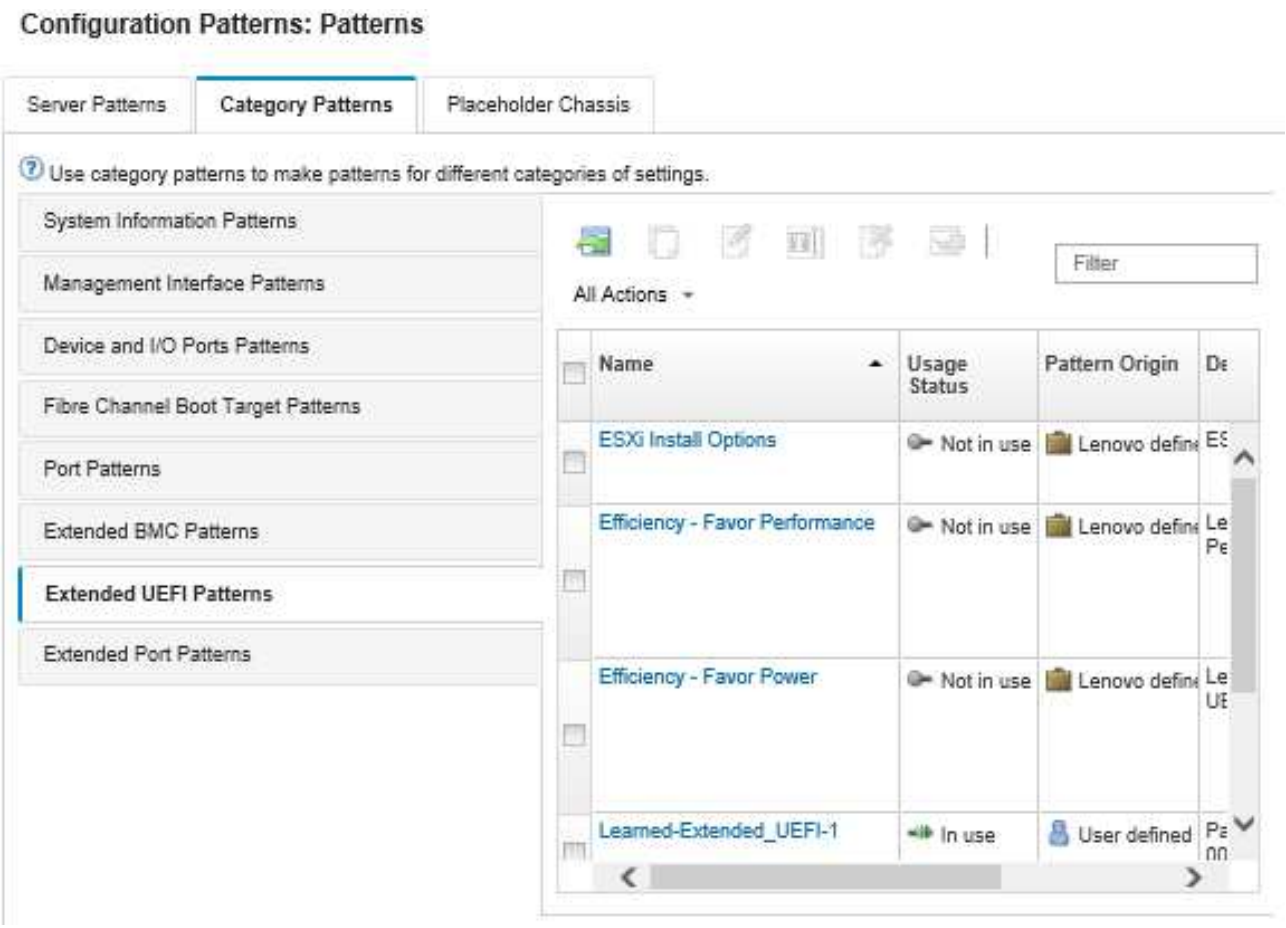
Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended UEFI Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).

- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended port settings

Extended port settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing server. You cannot manually create extended port patterns; however, you can copy and modify the patterns that have already been created.

About this task

XClarity Administrator provides the following predefined extended port pattern:

- **Virtual fabric balanced Ethernet**. Lenovo supplied port pattern for Virtual Fabric mode vNIC mode, Ethernet only

Some device-level settings on Mellanox and Broadcom I/O adapters must be set to the same value on all ports. If the settings are set to different values on different ports, the settings for one port will be used, and the settings for other ports will be out of compliance. To resolve the non-compliance issue, select the same value for those device level settings.

For Mellanox I/O adapters, the following settings must be set to the same value on all ports.
- Advanced power settings
- PCI Virtual Functions Advertised
- Slot power limiter
- Virtualization Mode

For Broadcom I/O adapters, the following settings must be set to the same value on all ports.
- Banner Message Timeout
- BW Limit
- BW Limit Valid
- BW Reservation
- BW Reservation Valid
- Enable PME Capability
- Maximum Number of PF MSI-X Vectors
- Multi-Function Mode
- Number of MSI-X Vectors per VF
- Number of VFs Per PF
- Option ROM
- SR-IOV
- Support RDMA

Procedure

Complete the following steps to modify extended port patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended Port Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ( ).

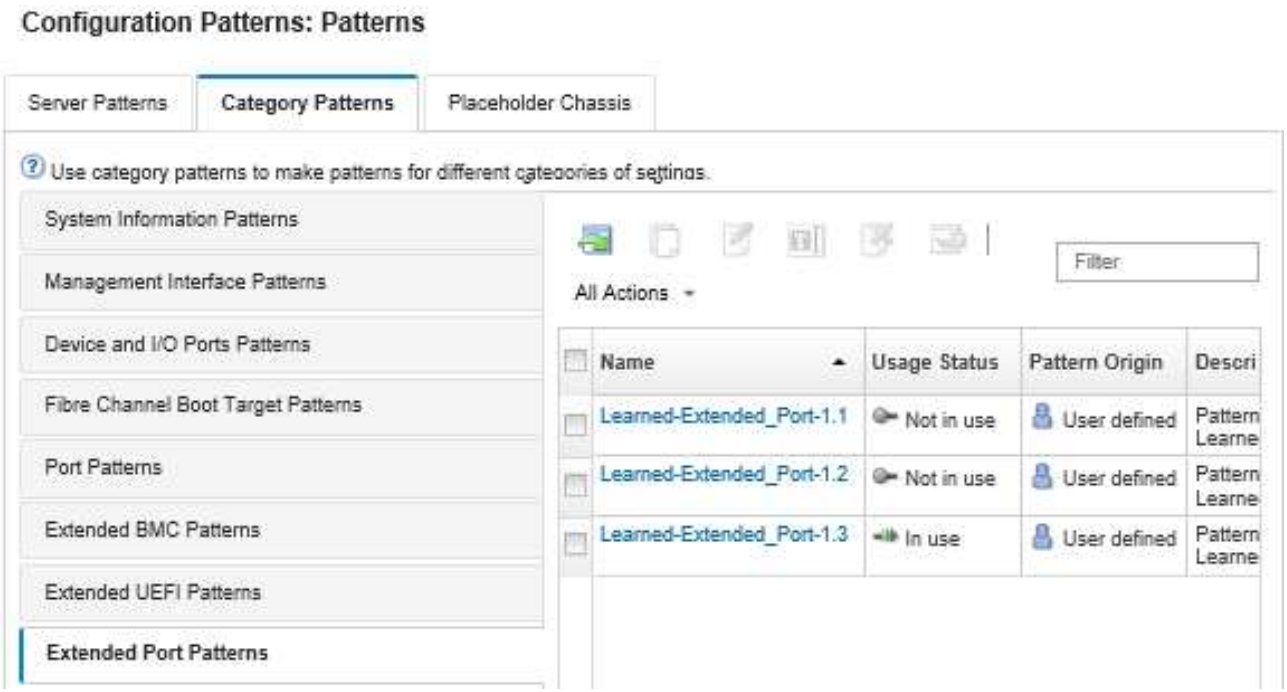
Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended Port Patterns** tab in the Configuration Patterns: Category Patterns page:



From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended SR635/SR655 BIOS settings

The extended SR635/SR655 BIOS settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing ThinkSystem SR635 or SR655 server. You cannot manually create extended SR635/SR655 BIOS patterns; however, you can copy and modify the patterns that have already been created.

Procedure

Complete the following steps to modify extended SR635/SR655 BIOS patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended SR635/SR655 BIOS Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ( ).

Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended SR635/SR655 BIOS Patterns** tab in the Configuration Patterns: Category Patterns page:

From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).
- Import or export patterns (see Exporting and importing server and category patterns).

Defining extended ThinkServer CPlus BIOS settings

The extended ThinkServer CPlus BIOS settings are learned and dynamically created from a specific managed server. Lenovo XClarity Administrator creates these patterns when you create a server pattern from an existing ThinkServer CPlus server. You cannot manually create extended ThinkServer CPlus BIOS patterns; however, you can copy and modify the patterns that have already been created.

Procedure

Complete the following steps to modify extended ThinkServer CPlus BIOS patterns.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Category Patterns** tab.

Step 3. Click the **Extended ThinkServer CPlus BIOS Patterns** vertical tab.

Step 4. Select the pattern to be modified, and click the **Edit** icon ( ).

Step 5. Modify the appropriate fields.

You can select the settings that you want to include in the category pattern by clicking **Include/ Exclude** settings.

Step 6. Click **Save** to the save changes to the current category pattern, or click **Save As** to save changes in a new category pattern.

Results

The modified category pattern is listed on the **Extended ThinkServer CPlus BIOS Patterns** tab in the Configuration Patterns: Category Patterns page:

From this page, you can also perform the following actions on a selected category pattern:

- Copy an existing pattern by clicking the **Copy** icon ( ).
- Delete a pattern by clicking the **Delete** icon ( ).
- Rename a pattern by clicking the **Rename** icon ( ).

- Import or export patterns (see Exporting and importing server and category patterns).

Deploying a server pattern to a server

You can deploy a server pattern to one or more managed servers. You can also deploy a server pattern to one or more empty bays in a chassis that is managed by Lenovo XClarity Administrator or in a placeholder chassis. Deploying a server pattern before the server is installed reserves management IP addresses, reserves virtual Ethernet or Fibre Channel addresses, and pushes the network setting to the relative switch internal ports.

Before you begin

Read the server-configuration considerations before you attempt to apply a server pattern to your managed devices (see Deploying a server pattern to a server).

Procedure

To deploy a server pattern to a managed server, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

Step 3. Select the server pattern to deploy, and click the **Deploy** icon ( ).

The Deploy Server Pattern dialog is displayed with the selected server pattern listed in the **Pattern to Deploy** list.

Step 4. Choose when to activate the configurations:

- **Full**. Immediately powers on or restarts the server to activate server, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) configurations.
- **Partial**. (default) Immediately activates management-controller configurations, but defers the activation of server and UEFI configurations until the next server restart. The server must be manually powered on or restarted before the profile is fully activated.

  Note: When deploying server patterns that included only IMM settings (including system information, management interface, and extended BMC category patterns), the server does not need to be restarted.
- **Deferred**. Generates a profile for the server, management controller, and UEFI configurations but does not activate the configuration settings on the server. You must manually activate the server profile by restarting the server before the profile is fully activated.

Note: The network settings on the relative switch internal ports are pushed to the switch immediately after the deployment, regardless of activation configuration.

Step 5. Choose one or more servers or empty chassis bays to which you want to deploy the server pattern.

Note: To display a list of empty chassis bays, select **Show Empty Bays**.

Step 6. Click **Deploy**. A dialog is displayed that lists the deployment status of each selected bay.

Step 7. Click **Deploy** again to start the deployment process.

Note: Deployment might take several minutes to complete. During deployment, a server profile is created and assigned to each selected server or chassis bay.

Step 8. Click **Close**.

After you finish

You can monitor the deployment progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar. You can also monitor the server-profile creation by clicking **Provisioning → Server Profiles**. After the deployment is complete, review the generated server profiles, and record the management IP address and any virtualized Ethernet or Fibre-Channel addresses.

If you deployed a server pattern to an existing server and selected:

- **Full** activation, a server profile is created for each server, the configuration is propagated to each server, and each server is rebooted to activate the configuration changes.
- **Partial** activation, a server profile is created for each server, and the configuration is propagated to each server. To fully activate the configuration changes, you must manually power on or restart each server (see Powering on and off a server).
- **Deferred** activation, a server profile is created for each server. You must manually activate the server profile on the server (see Activating a server profile).

If you deployed a server pattern to an empty bay in a managed chassis or placeholder chassis, after the compute nodes are physically installed in appropriate chassis bays and then discovered and managed by Lenovo XClarity Administrator, you must deploy and activate the server profile to the newly installed compute nodes (see Activating a server profile).

If one or more servers do not start after you deployed a new server pattern to those servers, the problem might be that the boot settings were overwritten with the default boot settings that are in the server pattern. For operating systems that are installed in UEFI mode, restoring the default settings might require additional configuration steps to restore the boot configuration. For examples for recovering boot settings on servers that are running on Windows or Linux, see Recovering boot settings after server pattern deployment.

Modifying a server pattern

You can make subsequent configuration changes to an existing server pattern. If the original server pattern is deployed to servers (if it is in use), you can redeploy the changed server pattern to all or a sub-set of those servers.

About this task

Note: If you choose not to redeploy the changed server pattern to a set of servers, those servers remain associated with the original unchanged server pattern.

By editing the server pattern, you can control a common configuration from a single place and retain the original set of virtual address assignments.

Procedure

Complete the following steps to modify a server pattern.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

Step 3. Select the server pattern to edit, and click the **Edit** icon (). The Edit Server Patterns Wizard is displayed.

Step 4. Enter the name of the pattern and a description.

Step 5. Choose the local storage configuration to be applied when this pattern is deployed to a server, and click **Next**.

For information about local storage settings, see Defining local storage.

Step 6. Optional: **Optional:** Modify the I/O adapter addressing, and define additional I/O adapters to match the hardware that you expect to configure with this pattern, and click **Next**.

For information about I/O adapter settings, see Defining I/O adapters.

Step 7. Define the boot order to be applied when this pattern is deployed to a server, and click **Next**.

For information about SAN boot targets settings, see Defining boot options.

Step 8. Select firmware settings from the list of existing category patterns.

You can create new category patterns by clicking the **Create** icon ( ).

For information about firmware settings, see Defining firmware settings.

Step 9. Click **Save** to save the changes to save configuration changes to the current server pattern, or click **Save As** to save the configuration changes to a new server pattern.

Step 10. Choose to save the changes to the current server pattern or to a new server pattern.

- Click **Save** to save the changes to the current server pattern. From the Save and Redeploy Pattern dialog, perform these steps:
  1. Choose when to activate the configurations.
     - **Full**. Immediately powers on or restarts the server to activate server, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) configurations.
     - **Partial**. (default) Immediately activates management-controller configurations, but defers the activation of server and UEFI configurations until the next server restart. The server must be manually powered on or restarted before the profile is fully activated.

       Note: When deploying server patterns that included only IMM settings (including system information, management interface, and extended BMC category patterns), the server does not need to be restarted.

     Note: The network settings on the relative switch internal ports are pushed to the switch immediately after the deployment, regardless of activation configuration.
  2. Select the target servers to which you want to redeploy the configuration changes. You can choose all of the servers to which the original server pattern was deployed or a subset of those server.
  3. Click **Redeploy**
- Click **Save As** to save changes to a new server pattern. To deploy the new pattern, see Deploying a server pattern to a server.

Exporting and importing server and category patterns

If you have multiple Lenovo XClarity Administrator instances, you can export server and category patterns from one XClarity Administrator instance and import them in another XClarity Administrator instance.

About this task

You can export only server and category patterns. Policies, address pools, and profiles cannot be exported. Exported patterns are dissociated with any reference address pools. To leverage the address pools in an imported pattern, edit the pattern and re-associate the pattern with the pools in XClarity Administrator in which they are imported.

Note: When you export a server patterns, the associated category patterns are also exported.

Procedure

- To export one or more patterns:
  1. From the XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.
  2. Click the **Server Patterns** or **Category Patterns** tab.
  3. Select one or more patterns to be exported.
  4. Click the **Export** icon ( ).
  5. Click **Export** to export the patterns.
  6. Save the pattern-data file to your local system.

     Note: If an exported pattern references address pools, these references are removed from the exported pattern to avoid conflicts when the pattern is imported into another XClarity Administrator instance. When the pattern is imported again, you can edit the imported pattern and assign the desired address pools.
- To import one or more patterns:
  1. From the XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.
  2. Click the **Import** icon ( ) to import the patterns. The Import Patterns dialog is displayed.
  3. Click **Select File**, and select a pattern-data file to be imported. Repeat for additional pattern-data files.
  4. Click **Import** to import the selected files.

     A summary report is displayed with a list of patterns that were imported, patterns that were renamed to naming conflicts, and patterns that were skipped because they already exist.

Working with server profiles

A *server profile* is an instance of a server pattern that is applied to a specific server. Server profiles are generated and assigned automatically when a server pattern is deployed to one or more servers. One server profile is created for each target server. Each server profile contains the specific configuration for a single server and contains information (such as assigned name, IP addresses, and MAC addresses) that is unique for that specific server.

About this task

The server profile is activated during the baseboard-management-controller startup process. You can choose to:
- Reboot the server when the pattern is deployed to activate the server profile immediately
- Defer activation until the next reboot.
- Defer activation until you manually activate the server profile.

Multiple server profiles can inherit from a single server pattern. After a server pattern is deployed to one or more servers, you can quickly deploy configuration changes to multiple servers by editing the parent server pattern and category patterns. The dependant server profiles are automatically updated and redeployed to their associated servers. By editing the server pattern, you can control a common configuration from a single place.

If you replace an existing server or if you install a pre-provisioned server in an empty bay in a chassis, you must activate the server profile for that new server to provision the configuration changes on the new server.

Note: You can deploy a server pattern to multiple servers; however, multiple patterns cannot be deployed to a single server.

You can change the server profile that is associated with a server in several ways, depending on the reason for the change.

- If you want to move or repurpose a server:
  1. Deactivate the current server profile on the current server (see Deactivating a server profile).
  2. Deploy the new server pattern to the new server (see Deploying a server pattern to a server).
- If a server failed and you want to use a spare server in its place:
  1. Deactivate the current server profile on the failed server (see Deactivating a server profile).
  2. Activate the same server profile on the spare server (see Activating a server profile).
  3. When the failed server is fixed, you can repeat these steps to switch the profile again.
- If a server failed and you want to replace the hardware:
  1. Deactivate the current server profile on the failed server (see Deactivating a server profile).
  2. Replace the failed server.
  3. Activate the same server profile on the new server (see Activating a server profile).

Important:

- When using address virtualization, a server retains its assigned virtual MAC or WWN address until it is powered down. When deactivating a profile that has address virtualization enabled, the **Power off the server** checkbox is selected by default. Ensure that the original server is powered off before you activate the inactive profile on a different server to avoid address conflicts.
- If you delete a profile that is not the most recently created, the virtual MAC and WWN addresses *are not* released from the address pool. For more information, see Deleting a server profile.
- The settings on a server can become out of compliance with its server profile if settings are changed without using Configuration Patterns or if an issue occurred during deployment, such a firmware issue or an invalid setting. You can determine the compliance status of each server from the Configuration Patterns: Server Profiles page.

Activating a server profile

You can activate a server profile on a replaced, reassigned, or newly installed and managed server.

About this task

If you replace an existing server or if you install a pre-provisioned server in an empty bay in a chassis, you must activate the server profile for that new server to provision the configuration changes on the new server.

Important:

- When using address virtualization, a server retains its assigned virtual MAC or WWN address until it is powered down. When deactivating a profile that has address virtualization enabled, the **Power off the server** checkbox is selected by default. Ensure that the original server is powered off before you activate the inactive profile on a different server to avoid address conflicts.
- If you delete a profile that is not the most recently created, the virtual MAC and WWN addresses *are not* released from the address pool. For more information, see Deleting a server profile.
- The settings on a server can become out of compliance with its server profile if settings are changed without using Configuration Patterns or if an issue occurred during deployment, such a firmware issue or an invalid setting. You can determine the compliance status of each server from the Configuration Patterns: Server Profiles page.

Procedure

To activate a server profile, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Profiles**. The Configuration Patterns: Server Profiles page is displayed.

Step 2. Select the server profile to activate.

Tips: The current state of the server profiles is listed in the **Profile Status** column. You can activate server profile that is in the Inactive or Pending activate state.

Step 3. Click the **Activate server profile** icon ( ).

Step 4. Click **Activate**.

If the profile is in the pending, active, or active failed state, you can choose when to activate the deployment:

- **Full**. Immediately powers on or restarts the server to activate server, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) configurations.
- **Partial**. (default) Immediately activates management-controller configurations, but defers the activation of server and UEFI configurations until the next server restart. The server must be manually powered on or restarted before the profile is fully activated.

  Note: When deploying server patterns that included only IMM settings (including system information, management interface, and extended BMC category patterns), the server does not need to be restarted.

When the server profile is first activated, the profile status changes to “Active.” After compliance is verified, the status changes to “Compliance” or “Non-Compliant.”

Results

The state of the server profile on the Configuration Pattern: Server Profiles page changes to Active.

Deactivating a server profile

You can unassign a server profile from a server or chassis bay by deactivating the profile.

Procedure

To deactivate a server profile, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Profiles**. The Configuration Patterns: Server Profiles page is displayed.

Step 2. Select the server profile to deactivate.

Tip: The current state of the server profile is listed in the **Profile Status** column.

Step 3. Click the **Deactivate server profile** icon ( ).

Step 4. Choose one of the following deactivation options:

- **Reset IMM Identity Settings**. Resets the profile-configured identity settings (including the baseboard-management-controller hostname, device name, or management interface assigned static IP addresses). Only the settings that are configured through the associated server pattern are reset.

  Note: For servers with statically assigned IP addresses, this option enables DHCP mode. If there is not a DHCP server enabled on the network, the server must be manually reconfigured with a valid static IP address. Converged, NeXtScale, and System x rack and tower servers must then be remanaged using XClarity Administrator.
- **Power off the server**. Powers off the server. When the server is powered back on, virtual address assignments revert to the burned-in defaults.
- **Force deactivation**. Deactivates the server profile even if the server has been removed or is not reachable.
- **Reset switch internal port settings**. Resets the profile-configured switch internal port settings to default values, including disabling UFP mode and removing associated member vports from VLAN definitions. Only the settings that are configured through the associated server pattern are reset.

  This option is disabled by default.

  Choose this option to leave the switch ports in a state where the server profile can then be deployed to another server without settings that would conflict with the previous switch port configuration.

Step 5. Click **Deactivate**.

Results

The state of the server profile on the Configuration Pattern: Server Profiles page changes to Inactive.

Note: If XClarity Administrator cannot communication with the management controller (for example if the management controller is in an error state or is restarting), deactivation of the server profile fails and the

server profile is not deactivated. If this occurs, reattempt the deactivation, and select the force deactivation option to deactivate the profile. The previously assigned server is still configured with the profile assigned identity and address assignments. The server must be manually powered down and removed from the infrastructure to avoid address conflicts.

Deleting a server profile

You can delete only server profiles that have been deactivated.

Before you begin

Ensure that the server profiles to be deleted are deactivated (see Deactivating a server profile).

Procedure

To delete a server profile, complete the following steps

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Profiles**. The Configuration Patterns: Server Profiles page is displayed.

Step 2. Select the server profile that is in the Deactivated state.

Tip: The current state of the server profile is listed in the **Profile Status** column.

Step 3. Click the **Delete** icon ( ).

Note: When you delete the most recently created profile, any virtual MAC or WWN address is released from the address pool. If you delete a profile that is not the most recently created, the virtual MAC and WWN addresses *are not* released from the address pool.

Working with placeholder chassis

You can pre-provision servers that will be installed in a Flex System chassis at a later time by defining a *placeholder chassis* to act as a target for the server pattern until the physical hardware arrives.

About this task

When you deploy a server pattern to a placeholder chassis, Lenovo XClarity Administrator creates a server profile for all 14 server bays in the Flex System chassis and reserves the management IP addresses and virtual Ethernet or Fibre Channel addresses for the servers.

The placeholder chassis bundles all of the server profiles, so that when the hardware arrives, you can deploy the placeholder chassis to activate the server profiles on the physical servers instead of deploying all 14 server profiles individually. Each server must be rebooted to fully activate the server profile.

Creating a placeholder chassis

You can create a placeholder chassis that can be pre-provisioned before the hardware is installed. Provisioning compute nodes in the chassis reserves management IP addresses and virtual Ethernet or Fibre Channel addresses.

Procedure

Complete the following steps to create a placeholder chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Placeholder Chassis** tab.

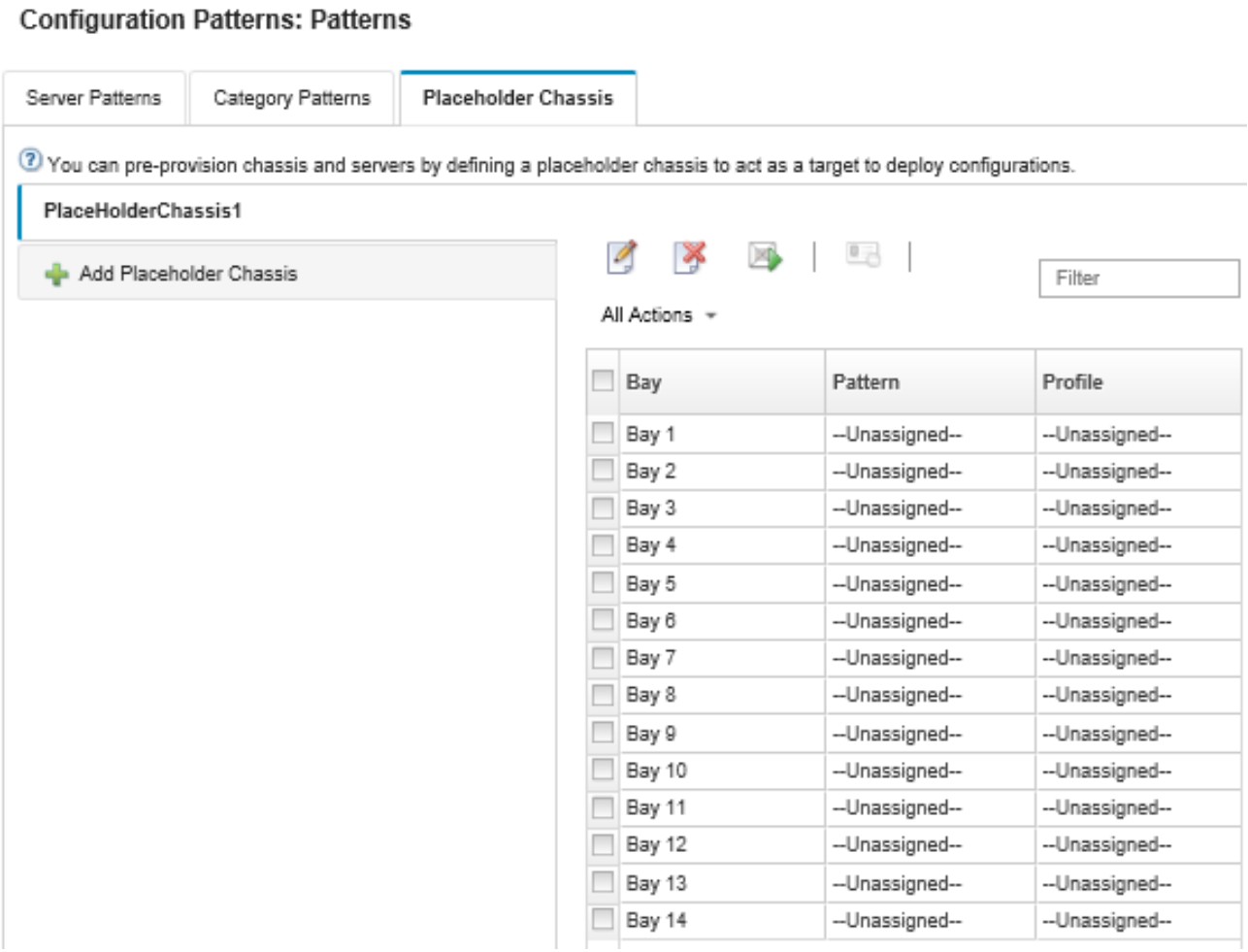
Step 3. Click the **Add Placeholder Chassis** vertical tab.

Step 4. Enter a name and description for the placeholder chassis.

Step 5. Click **Add**.

After you finish

A vertical tab is added for the new placeholder chassis on the Configuration Patterns: Placeholder Chassis page.



From this page, you can perform the following actions on a selected placeholder chassis:

- Deploy the placeholder chassis by clicking the **Deploy** icon ( ).
- Modify the placeholder chassis name and description by clicking the **Edit** icon ( ).
- Deploy a server pattern to the placeholder chassis (see Deploying a server pattern to a placeholder chassis).
- Deactivate the server profile from a placeholder chassis (see Deactivating a server profile).
- Delete the placeholder chassis by clicking the **Delete** icon ( ).

Deploying a server pattern to a placeholder chassis

You can deploy a server pattern to each bay in a placeholder chassis. Deploying a server pattern before the servers are installed in the Flex System chassis creates a server profile for each server bay in the chassis and reserves management IP addresses and virtual Ethernet or Fibre Channel addresses.

Procedure

Complete the following steps to deploy a server pattern to a placeholder chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

Step 3. Select the server pattern that you want to deploy to the placeholder chassis.

Step 4. Click the **Deploy** icon ( ). The Deploy Server Pattern dialog is displayed with a list of available chassis and placeholder chassis.

Step 5. Select **Deferred** from the **Activation** list.

Step 6. Click **Show Empty Bays**.

Step 7. Choose one or more placeholder chassis bays to which you want to deploy the server pattern.

Step 8. Click **Deploy**. A dialog is displayed that lists the deployment status of each selected bay.

Step 9. Click **Deploy** again to start the deployment process.

A server profile is created and assigned for each selected bay in the placeholder chassis.

Note: Deployment can take several minutes to complete

Step 10. Click **Close**.

After you finish

You can monitor the deployment progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar. You can also monitor the server-profile creation by clicking **Provisioning → Server Profiles**. After the deployment is complete, review the generated server profiles, and record the management IP address and any virtualized Ethernet or Fibre-Channel addresses.

After the Flex System chassis is physically installed in the rack and then discovered and managed by XClarity Administrator, you can deploy the placeholder chassis to provision all servers in the chassis (see Deploying a server pattern to a placeholder chassis).

Deploying a placeholder chassis

After you pre-configure a placeholder chassis by deploying a server pattern to that placeholder chassis, and then discover and manage the actual chassis, you can deploy the placeholder chassis to configure the actual compute nodes.

Procedure

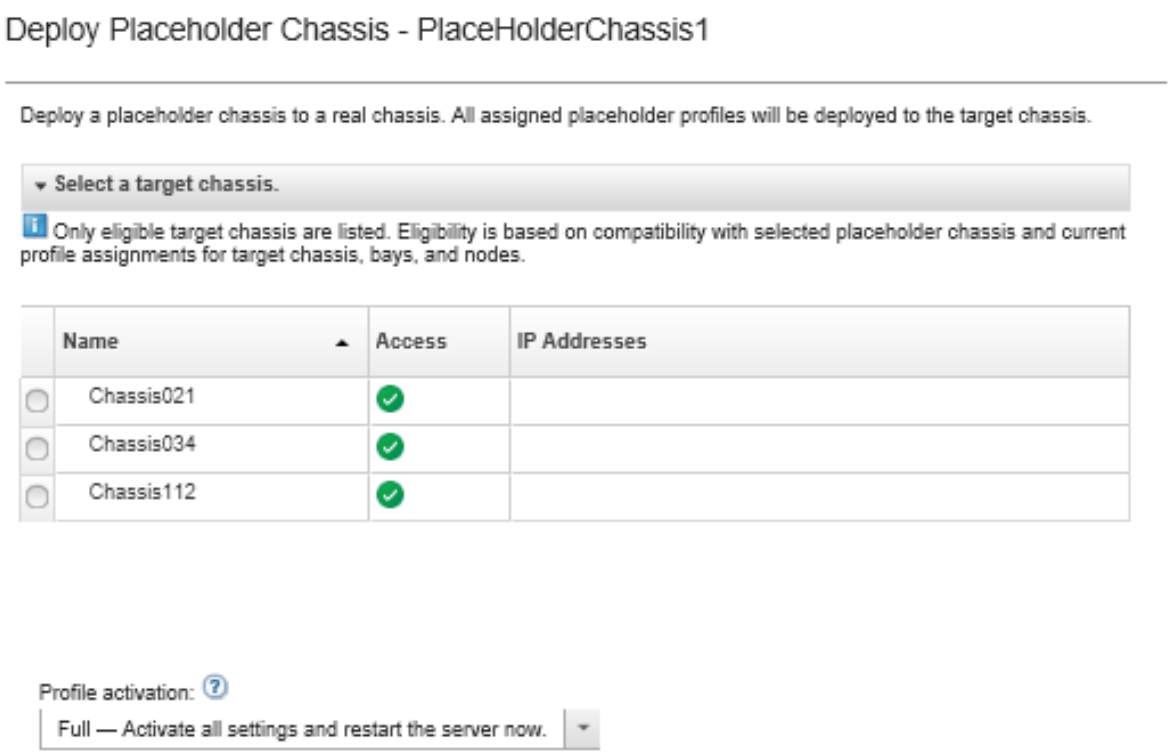
Complete the following steps to deploy a placeholder chassis.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server Configuration Patterns**. The Server Configuration Patterns page is displayed.

Step 2. Click the **Placeholder Chassis** tab.

Step 3. Select the vertical tab for the placeholder chassis that you want to deploy.

Step 4. Click the **Deploy placeholder chassis** icon ( ) to display the Deploy Placeholder Chassis dialog.



Step 5. Choose when to activate the configurations:

Note: The network settings on the relative switch internal ports are pushed to the switch immediately after the deployment, regardless of activation configuration.

- **Full**. Immediately powers on or restarts the server to activate server, baseboard management controller, and Unified Extensible Firmware Interface (UEFI) configurations.
- **Partial**. (default) Immediately activates management-controller configurations, but defers the activation of server and UEFI configurations until the next server restart. The server must be manually powered on or restarted before the profile is fully activated.

  Note: When deploying server patterns that included only IMM settings (including system information, management interface, and extended BMC category patterns), the server does not need to be restarted.

Step 6. Click **Activate**.

Resetting storage adapters to default values

You can reset the local storage adapters to their default manufacturing settings for one or more servers.

About this task

Attention: This action clears all data on the local storage adapters.

If the server is powered off and RAID link is supported, the server is booted to system setup to reset local HDD and SSD adapters.

Procedure

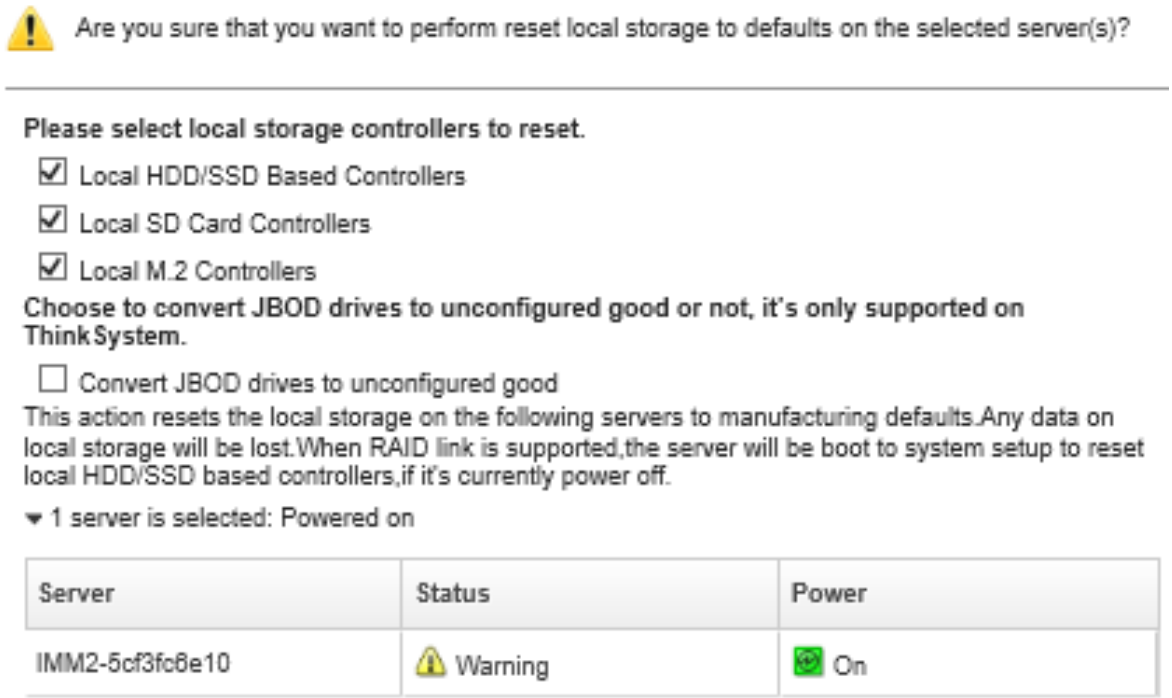
Complete these steps to clear the RAID configuration for one or more servers.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

You can sort the table columns to make it easier to find the server that you want to manage. In addition, you can select a server type from the **All Systems** drop down list and enter text (such as a name or IP address) in the **Filter** field to further filter the servers that are displayed.

Step 2. Select one or more servers

Step 3. Select **All Actions → Service → Reset Local Storage to Defaults**. A dialog is displayed that asks for additional information.



Step 4. Select the local storage adapters to reset.

Step 5. Optional: : (ThinkSystem servers only) Chose to convert JBOD drives to unconfigured good.

Step 6. Click **Reset Storage**.

Configuring memory

You can encrypt and decrypt persistent memory for Intel® Optane™ DC Persistent Memory DIMMs.

Procedure

Complete the following procedure to encrypt and decrypt persistent memory.

Step 1. From the XClarity Administrator menu, click **Hardware → Servers**. The Servers page is displayed with a tabular view of all managed servers (rack servers and compute nodes).

Step 2. Select one or more servers that you want to configure.

Step 3. Click **All Actions → Security → Intel Optane PMEM Operation** to display the Intel Optane PMEM Operation dialog.

Step 4. Select the security operation that you want to perform.

- **Enable security**. Data that is written to the persistent memory region is encrypted using the specified passphrase.

  Important: Record the encryption passphrase. The passphrase is required to authorize disabling security or erasing the encryption passphrase.

- **Disable security**. Data that is written to the persistent memory region is not encrypted.

  Data that is already stored in the persistent memory region remains encrypted and is still accessible.

  Note: This action is available only when security is enabled, and the passphrase set. You must authorize this operation using the current passphrase. You can disable security for multiple DIMMs in the device only if all DIMMs share the same passphrase.

- **Secure erase**. Erases the encryption passphrase that is used to encrypt the data that is stored in the persistent memory region to ensure that data is unrecoverable.

  Note: This action is available only when security is enabled, and the passphrase set. You must authorize this operation using the current passphrase.

- **Secure erase without passphrase**. Securely erases all the data that is stored in the persistent memory of the specified DIMMs in the device. After the secure erase, all data is unrecoverable.

  Note: This action is available only when security is disabled and passphrase is not required.

Step 5. If required, specify and confirm the passphrase.

Step 6. Click **OK**.

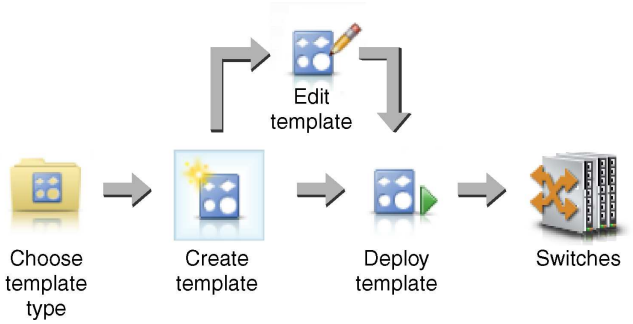
Chapter 12. Configuring switches using configuration templates

You can use templates to quickly provision multiple CNOS rack switches from a single set of defined configuration settings.

About this task

You can use switch-configuration templates in XClarity Administrator to configure global settings, port channels, virtual LANs, Virtual link aggregation groups, and spine-leaf topologies on managed switches. Currently, only rack switches running CNOS are supported.

The following figure illustrates the workflow for configuring managed rack switches.



1. **Choose a template type.**

   A *switch-configuration template* groups together related switch settings. You can create the following types of switch-configuration templates.
   - **Global**. Configures global settings, including system propriety, native VLAN tags, and L2 interfaces.
   - **Port channel**. Configures basic and advanced port-channel settings, and removes ports from and deletes a port channel.
   - **Spine-leaf**. Deploys a spine-leaf configuration to an existing topology.
   - **Virtual LAN (VLAN)**. Configures VLAN settings and properties, and deletes a V LAN.
   - **Virtual link aggregation group (VLAG)**. Configures basic, advanced, and peer VLAG settings, and creates and deletes a VLAG instance.
2. **Create a template.**

   You can create multiple switch-configuration templates to represent different configurations that are used in your data center. You use switch-configuration templates to control a common switch configuration from a single place.

   For more information about creating switch configuration templates, see Creating a switch-configuration template.
3. **Deploy the template to one or more switches.**

   You can deploy a server pattern to one or more individual rack switches running CNOS.

   For more information about deploying a switch configuration, see Deploying switch-configuration templates to a target switch.
4. **Edit a template.**

© Copyright Lenovo 2015, 2022

Editing a switch-configuration template does not automatically deploy the updated settings to all switches to which the initial template was deployed. You must manually redeploy changed templates. The history page keeps track of the settings for each deployment.

Setting default server-configuration preferences

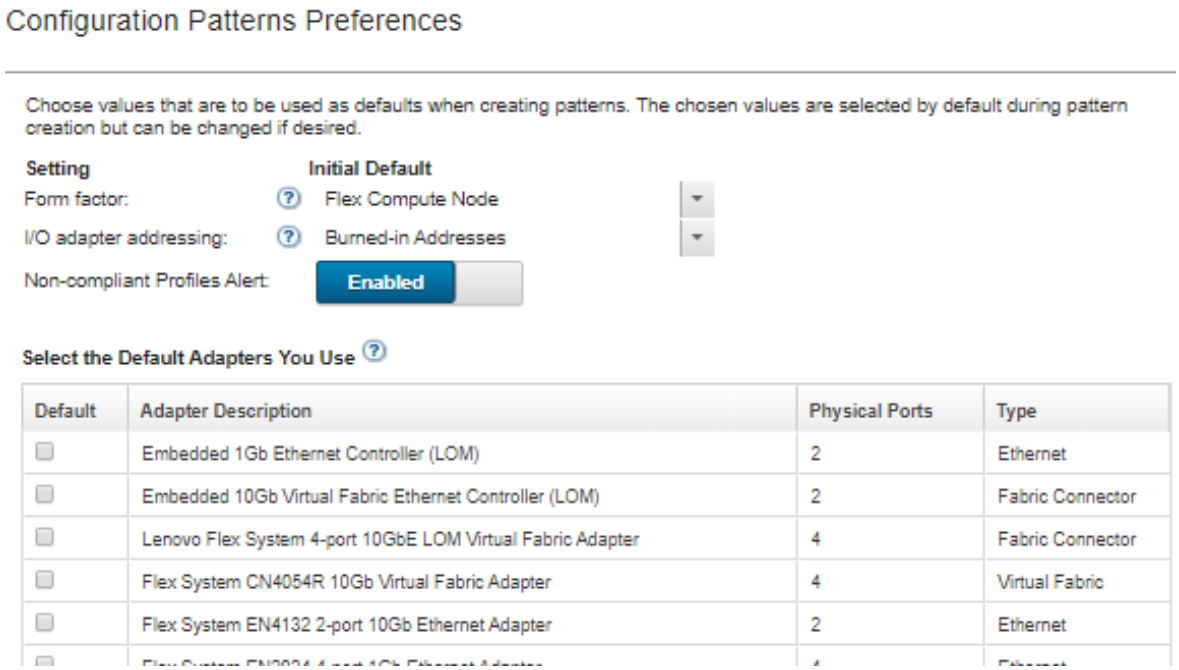
You can define values to be selected by default when creating server configuration patterns. The values can be changed during server pattern creation.

Procedure

To set default server-configuration settings, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning**, and then click the help icon ( ) after **Configuration Patterns** to display the Configuration Patterns: Getting Started page.

Step 2. Click **Set Configuration Pattern Preference** to display the Configuration Pattern Preference dialog.



Step 3. Select the default server form factor.

Step 4. Select the default I/O adapter addressing mode.

- **Burned in**. Use existing World Wide Name (WWN) and Media Access Control (MAC) addresses that are provided with the adapter from manufacturing.
- **Virtual**. Use virtual I/O adapter addressing to simplify the management of LAN and SAN connections. Virtualizing I/O-addresses reassigns the burned-in hardware addresses with virtualized Fibre WWN and Ethernet MAC addresses. This can speed deployment by pre-configuring SAN zone membership and facilitate failover by eliminating the need to reconfigure SAN-zoning and LUN-masking assignments when replacing hardware.

  When virtual addressing is enabled, both Ethernet and Fibre Channel addresses are allocated by default regardless of defined adapters. You can choose the pool from which Ethernet and Fibre Channel addresses are allocated.

  You can also edit virtual-address settings by clicking the **Edit** icon ( ) next to the address modes.

Restriction: Virtual addressing is supported for only servers in Flex System chassis. Rack and tower servers are not supported.

Step 5. Choose whether to enable or disable raising an alert when a server's configuration settings do not match the assigned server-configuration profile

Alerts are raised only for non-compliance with an active profile (in the ASSIGNED or ERROR_ ACTIVATING state).

When the server's configuration becomes compliant or if the server profile is unassigned, the non-compliant profile alert is deleted.

Step 6. Select one or more default I/O adapters that you want to use as preferred adapters in the selection lists.

Step 7. Click **Save**.

Creating a switch-configuration template

When you create a switch-configuration template, you define the settings for a specific type of configuration.

Before you begin

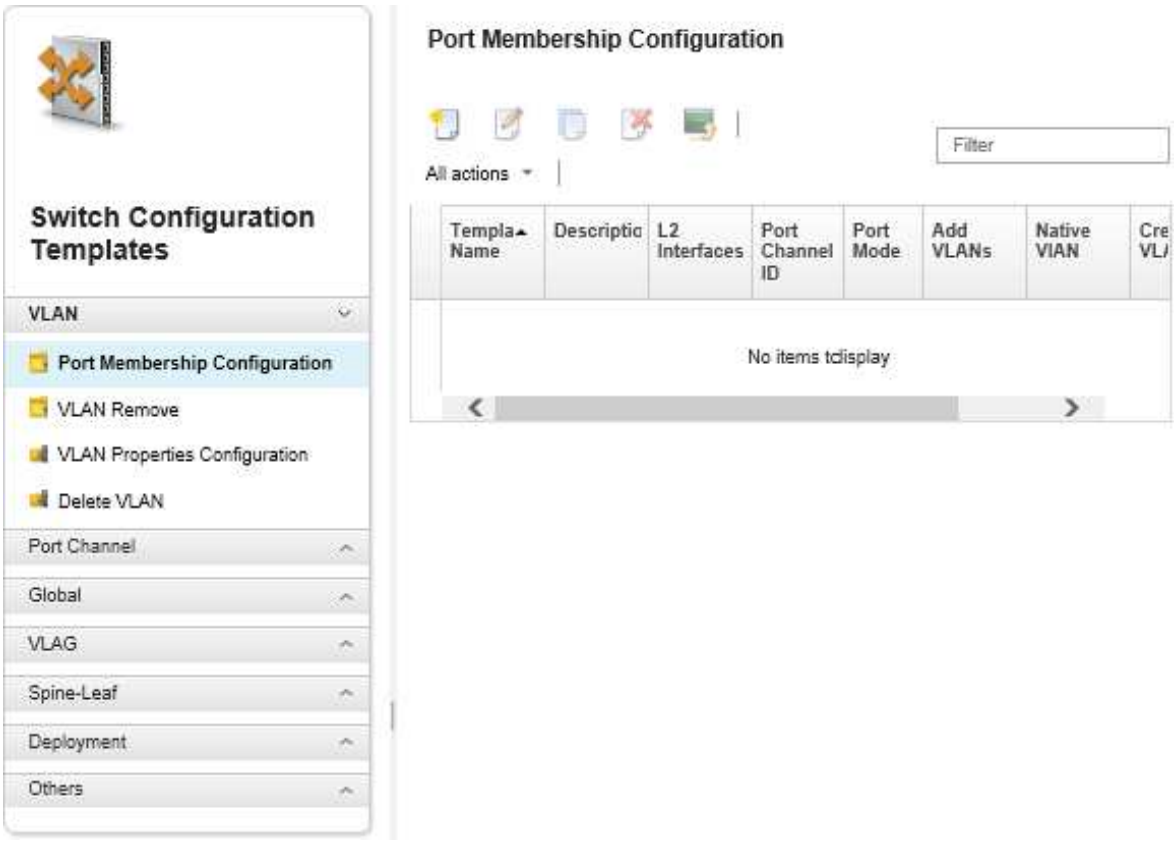
Before you create a switch-configuration template, consider the following suggestions:

- Identify groups of switches that have the same hardware options and that you want to configure the same way. You can use a switch-configuration template to apply the same configuration settings to multiple switches, thereby controlling a common configuration from one place.
- Identify the aspects of configuration that you want to customize (for example, global, port-channel, or VLAN settings).

Procedure

Complete the following steps to create a switch-configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.



Step 2. Select the type of template that you want to create from the left navigation.

Step 3. Click the **Create** icon ( ) to display the Create New Template dialog.

The fields that are listed on this dialog vary depending on the type of template.

Step 4. Click **Save** to save the template, or click **Save and Deploy** to save and immediately deploy the template to one or more managed rack switches

For information about deploying a template, see Deploying switch-configuration templates to a target switch .

After you finish

If you clicked **Save and Deploy**, the Deploy Switch Template page is displayed. From this page, you can deploy the switch-configuration template to specific switches.

If you clicked **Save**, the switch-configuration template is saved to the Switch Configuration Templates page. From this page, you can perform the following actions on selected server patterns:

- View details about the template by clicking the template name in the Name column.
- View an aggregated list of all templates, click **Others → All templates**.
- Deploy the template (see Deploying switch-configuration templates to a target switch).
- Copy and then modify a template by clicking the **Copy** icon ( ).
- Edit the template by clicking the **Edit** icon ( ).

Note: Changes to the template are *not automatically* redeployed to switches on which the original template was deployed.

- Rename the pattern by clicking the **Rename** icon ( ).
- Delete the pattern by clicking the **Delete** icon ( ).

Defining VLAN port-membership settings

You can add physical ports and port channels to one or more (for trunk) VLANs using the VLAN Port Membership Configuration template.

Procedure

Complete the following steps to create a Port Membership Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAN → Port Membership Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

Important: You must specify one or more physical L2 interfaces or port channel IDs.

- Enter a name and description for the template.
- Specify one or more valid physical L2 interfaces. You can specify a list of interfaces separated by a comma, a range of IDs separated by a dash, or a combination of both, for example:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Specify one or more valid port channel IDs (port aggregator interfaces). You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- Choose whether the port accepts tagged or untagged traffic. This can be one of the following values.
  - **access**. The port carries traffic for a single VLAN.
  - **trunk**. (default) The port carries traffic for all VLANs that are accessible by the switch.
- Specify one or more VLAN IDs to add to the port's VLAN membership list. You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Notes:

- If the port mode is set to “access,” only the first VLAN ID is used. For example, in the range `2-4,5,10-20`, only `2` is used.

  - CNOS reserves VLAN IDs 4000-4095 by default. Using reserved VLAN IDs (either by CNOS or another user) might cause the switch-configuration deployment to fail.
- Specify a native VLAN ID with which untagged traffic is tagged. This can be a number from 1-4096.

  Notes:
  - This field is valid only when the port mode is set to “trunk.”
  - If it is not specified, or if the ID is outside the end-state VLANs on a port, the port will effectively not allow untagged traffic.
- Select **Create VLANs** to create VLAN IDs that are currently missing on the target switch.

  If a port belongs in a VLAN that is not created, the port continues to be a member of that VLAN, but any traffic that is tagged with that VLAN ID and reaches the port is not allowed to pass.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining VLAN properties

You can configure advanced VLAN properties using the VLAN Properties Configuration template.

Procedure

Complete the following steps to create a VLAN Properties Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAN → VLAN Properties Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify a VLAN ID on which to apply the changes. This can be a number from 1-4095.

  Note: CNOS reserves VLAN IDs 4000-4095 by default. Using reserved VLAN IDs (either by CNOS or another user) might cause the switch-configuration deployment to fail.
- Specify a custom name for the VLAN.
- Choose whether the VLAN is active (enabled) or suspended (disabled).
- Choose whether IP multicast (IPMC) flood on the target VLAN is controlled (enabled) on IPv4 or IPv6 interfaces. This can be one of the following values.
  - **Disable**. IPv4 and IPv6 are disabled.
  - **Enable**. IPv4 and IPv6 are enabled.
  - **IPv4 Disable**.
  - **IPv4 Enable**
  - **IPv6 Disable**
  - **IPv6 Enable**

  This action is additive, meaning that “IPv4 Enable” deployed on top of “Disable” results in “IPv4 Enable,” but deploy on top of “IPv6 Enable” results in ""Enable.” The reverse is true for the disable options.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Removing VLAN settings

You can remove interfaces from VLANs using the VLAN Remove template.

Procedure

Complete the following steps to create a VLAN Remove template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAN → VLAN Remove** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

Important: You must specify one or more physical L2 interfaces or port channel IDs.

- Enter a name and description for the template.
- Specify one or more valid physical L2 interfaces. You can specify a list of interfaces separated by a comma, a range of IDs separated by a dash, or a combination of both, for example:
  - Ethernet1/10
  - Ethernet1/1,3,5,7
  - Ethernet1/1-10,21-30
  - Ethernet2/1-5,7,9,11-13
- Specify one or more valid port channel IDs (port aggregator interfaces). You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13
- Specify one or more VLAN IDs to remove from the port's VLAN membership list. You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13

Note: If the port mode is set to “access,” removing the VLAN causes the port to go in VLAN 1.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Deleting VLANs

You can remove VLAN configurations from the switch using the Delete VLAN template.

Procedure

Complete the following steps to create a Delete VLAN template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAN → Delete VLAN** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify one ore more VLAN IDs to remove from the port's VLAN membership list. You can specify a list of numbers separated by a comma, a range of numbers separated by a dash, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

  Note: You cannot delete reserved VLAN IDs.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining port-channel basic settings

You can create port aggregators and add ports to the aggregators using a port-channel Basic Configuration template.

If the port channel has ports in it, and some of those ports are part of the template, their properties (port priority, mode, and timeout) are updated with the template's settings when the template is deployed.

Procedure

Complete the following steps to create a port-channel Basic Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Port Channel → Basic Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify one or more valid physical L2 interfaces. You can specify a list of interfaces separated by a comma, a range of IDs separated by a dash, or a combination of both, for example:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Specify the port channel ID (port aggregator interface) to create or update. This can be a number from 1-4095.
- Specify the Link Aggregation Control Protocol (LACP) port mode. This can be one of the following values.

  - **Active**. (default) Enables LACP unconditionally
  - **Passive**. Enables LACP only when an LCAP device is detected.
  - **Static**. Disables LCAP.

  Note: Active and Passive can be mixed in the same aggregator, but Static cannot.
- Specify the LACP port priority. This can be a number from 1 - 65535.

  Note: The LACP port priority is used with the port number to form the LACP Port ID.
- Specify the LACP timeout mode before LCAP goes into individual mode. This can be one of the following values.
  - **Long**. (default) 90 seconds
  - **Short**. 3 seconds

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining port-channel advanced settings

You can configure advanced port-channel properties using the port-channel Advanced Configuration template.

Procedure

Complete the following steps to create a port-channel Advanced Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Port Channel → Advanced Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify a port channel ID (port aggregator interface) to update. This can be a number from 1-4095.
- Choose whether individual ports remain active when LACP fails. This can be one of the following values.
  - **Active**. (default) Enables LACP unconditionally.
  - **Suspend**. Disables LACP .
- Specify the minimum number of links that must be up for the port channel to be considered up. This can be a number from 1 – 32.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Deleting port channels

You can remove port channels from the switch using the Delete Port Channel template.

Procedure

Complete the following steps to create a Delete Port Channel template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Port Channel → Delete Port Channel** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify one ore more port channel IDs (port aggregator interfaces) to delete. You can specify a list of numbers separated by a comma, a range of numbers separated by a comma, or a combination of both. The values and ranges can be numbers from 1-4096, for example:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining general switch settings

You can configure general switch properties using the global Generic Configuration template.

Procedure

Complete the following steps to create a switch global Generic Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Global → Generic Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the LACP system priority that is used to generate the LACP system ID. This can be a number from 1 – 65535.
- Choose where to enable native VLAN tagging. This can be one of the following values.
  - **Ingress and Egress**
  - **Egress only**

  Note: This property is supported by CNOS 10.10.1 and later.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining global L2 interface settings

You can configure VLAN tagging properties on L2 Interfaces using the L2 Interface Configuration template.

Procedure

Complete the following steps to create an L2 Interface Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Global → L2 Interface Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify one or more valid physical L2 interfaces. You can specify a list of interfaces separated by a comma, a range of IDs separated by a dash, or a combination of both, for example:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Choose where to enable native VLAN tagging. This can be one of the following values.
  - **Ingress and Egress**
  - **Egress only**

  Note: This property is supported by CNOS 10.10.1 and later.
- Choose whether to enable or disable tunnelling (QinQ) support.

  Note: This property is supported by CNOS 10.10.1 and later.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining peer VLAG settings

You can configure a VLAG peers using the VLAG Peers Configuration template.

Procedure

Complete the following steps to create a VLAG Peers Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAG → Peers Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Choose whether to enable or disable the VLAG.
- For Peer 1 and Peer 2, complete the following fields. Fields for both peers must be populated.
  - Specify the IIPv4 or IPv6 address of the VLAG peer to use for health check.
  - Specify the ID of the port channel that is used between the two peers. This can be a number from 1 – 4095.
  - Specify the VRF that is used for health check (for example, management, default, or customVRF).

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining VLAG instance settings

You can create or update a VLAG instance using the VLAG Instance Configuration template. A VLAG instance is a device that is connected to both switches (usually through a port aggregation) to which the VLAG appears as a single device.

Procedure

Complete the following steps to create a VLAG Instance Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAG → Instance Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the VLAG ID. This can be a number from 1 – 64.
- Specify the ID of the port-channel that is connected to the Peer 1 and Peer 2. This can be a number from 1 – 4095.
- Choose whether to enable or disable the VLAG instance.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining VLAG advanced settings

You can configure advanced VLAG properties using the VLAG Advanced Configuration template.

Procedure

Complete the following steps to create a VLAG Advanced Configuration template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAG → Advanced Configuration** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the priority that is used to control which peer is primary. This can be a number from 1 – 65535.

  If not specified, the switch's default priority is used. For CNOS, the default is 0.
- Specify the grace period, in seconds, for the VLAG to come online after a simultaneous reboot. This can be a number from 240 – 3600.

  If not specified, the switch's default is used. For CNOS, the default is 300.
- Specify the tier ID that is used to differentiate VLAG setups in the same network. This can be a number from 1 – 512.

- Specify the vLAG startup delay interval, in seconds, that is used to delay bringing up ports after a peer reloads. This can be a number from 0 – 3600.

  If not specified, the switch's default is used. For CNOS, the default is 120.
- Specify the number of VLAG keep-alive attempts (unanswered hello messages) before the VLAG fails. This can be a number from 1 – 24.

  If not specified, the switch's default is used. For CNOS, the default is 3.
- Specify the interval, in seconds, between VLAG keep-alive attempts. This can be a number from 2 – 300.

  If not specified, the switch's default is used. For CNOS, the default is 5.
- Specify the interval, in seconds, between VLAG keep-alive retry attempts. This can be a number from 1 – 300.

  If not specified, the switch's default is used. For CNOS, the default is 30.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Deleting a VLAG instance

You can delete a VLAG instance using the VLAG Instance Delete template.

Procedure

Complete the following steps to create a VLAG Instance Delete template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **VLAG → Instance Delete** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the unique ID of the VLAG instance. This can be a number from 1 – 64.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Defining a spine-leaf topology

You can verify the physical topology and deploy a SpineLeaf (L3 fabric) setup on managed switches using the spine-leaf Topology Wizard template.

Procedure

Complete the following steps to create a spine-leaf Topology Wizard template.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Click **Spine-Leaf → Topology Wizard** in the left navigation, and then click the **Create** icon ( ).

Step 3. In the Create New Template dialog, specify the following information.

- Enter a name and description for the template.
- Specify the autonomous system (AS) number for the Border Gateway Protocol (BGP) protocol that is running on the switch. This can be a number from 1 – 4294967295.

  Note: This is supported by CNOS 10.9.3 and later.
- Choose whether to allow single links between switches.

  Typically, deployment fails if there are not at least two links between any spine and leaf switch.

Step 4. Click **Create** to save the template, or click **Create and Deploy** to save and immediately deploy the template to one or more managed rack switches.

For information about deploying a template, see Deploying switch-configuration templates to a target switch

Deploying switch-configuration templates to a target switch

You can define VLAN port settings by creating a VLAN port-configuration template.

About this task

There are three types of deployments:

- **Normal**. Deploys switch-configuration settings to one or more rack switches in a basic layered architecture.
- **VLAG**. Deploys switch-configuration settings to exactly two switches that support a virtual link aggregation group (VLAG) architecture. The switches must be of the same model and software version.
- **Spine-Leaf**. Deployment templates to one or more spine switches and leaf switches.

Procedure

To deploy a switch-configuration template to one or more managed switches, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Select one or more switch-configuration templates that you want to deploy.

Step 3. Click the **Deploy** icon ( ) to display the Deploy Template dialog.

Step 4. Select one or more switches to which you want to deploy the templates.

Only switches that are compatible with the selected templates are listed.

Step 5. Click **Deploy**. A dialog is displayed that lists the deployment status of each selected switch.

Step 6. Click **Deploy** again to start the deployment process.

Note: Deployment might take several minutes to complete.

After you finish

You can view the deployment history (see Viewing switch-configuration deployment history).

Viewing switch-configuration deployment history

You can view information about switch-configuration templates that have been deployed to managed switches, including the template name, template type, timestamp, and the switches to which they were deployed. Each deployment contains a snapshot of the template as it was when it was deployed.

Procedure

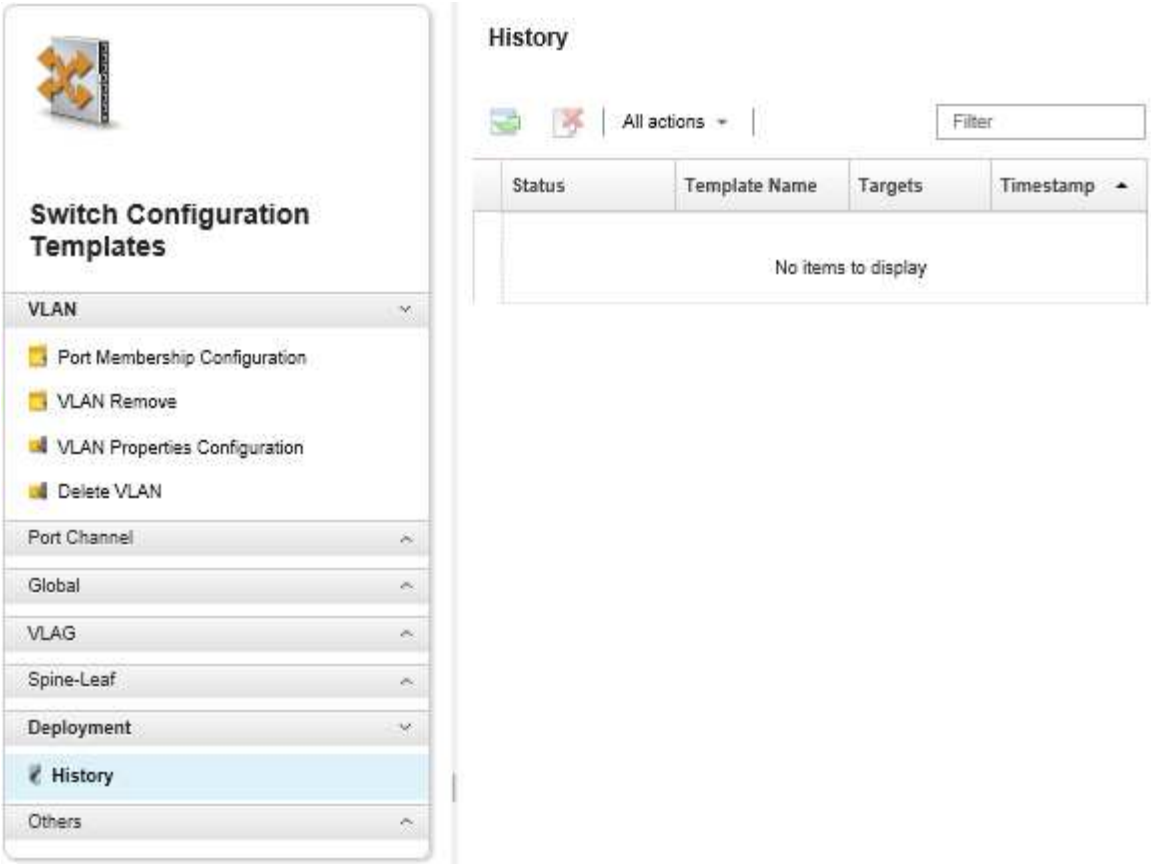
Complete the following steps to view switch-configuration deployment history.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Switch Configuration Templates**. The Switch Configuration Templates page is displayed.

Step 2. Expand **Deployment**, and click **History** in the left navigation to display a table of deployed templates.

The **Status** column indicates whether the configuration deployment was successful. It can be one of the following states:

- **Succeeded**. Configuration deployment to all target switches completed successfully.
- **Warning**. Configuration deployment to one or more target switches completed with warnings.
- **Failed**. Configuration deployment to one or more target switches failed.



After you finish

- View the information about each deployed template, including what was deployed and what succeeded or failed, by clicking the template name in the table.
- Clear the deployment history by selecting a deployment and clicking the **Delete** icon ( ).

Chapter 13. Updating firmware on managed devices

From the Lenovo XClarity Administrator web interface, you can download, install, and manage firmware updates for managed devices, including chassis, servers, storage systems, and switches. You can assign firmware-compliance policies to the managed devices to ensure that firmware on those devices remains compliant. You can also create and edit firmware-compliance policies when validated firmware levels do not match the suggested predefined policies.

Learn more:

- XClarity Administrator: Boosting Efficiency when Updating Firmware
- Lenovo ThinkSystem Firmware and Driver Update Best Practices
- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Firmware updates
- XClarity Administrator: Provisioning firmware security updates

Before you begin

Updating firmware and updating device drivers are separate processes in XClarity Administrator; there is no connection between these processes. XClarity Administrator does not maintain compliance between firmware and devices drivers on managed devices, even though it is recommended that you update device drivers at the same time as the firmware.

About this task

Note: An operating system is not required to update firmware. For bare metal servers, ensure that the server is powered off before updating firmware.

You can manage and apply firmware updates to the following managed devices.

- **Chassis**. CMM updates
- **ThinkAgile, ThinkSystem, System x, Converged, Flex System, and NeXtScale servers**. Baseboard management controller, UEFI, DSA, mezzanine, and adapter updates
- **RackSwitch and Flex System switches**
- **Lenovo Storage and ThinkSystem DM storage devices**
- **IBM TS4300 Tape Library device**

Firmware for the following devices cannot be updated through XClarity Administrator.

- **ThinkServer servers**. See the documentation that was provided with the server to find information about how to update the firmware.
- **Flex Power Systems compute nodes**. Several methods are available to update firmware for Flex Power Systems compute nodes. For more information, see IBM Flex System p260/p460 Compute Nodes online documentation. The process for other Flex Power Systems compute nodes is similar.
- **Flex switches that are in stacked mode or protected mode**. You *cannot* update firmware on stacked switches. Updating firmware is disabled for all switches that are stacked.
- **Flex switches**. If you are using the following switch, see the documentation that was provided with the switch to find information about how to update the firmware.
  - Cisco Nexus B22 Fabric Extender

Procedure

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

© Copyright Lenovo 2015, 2022

Step 1. **Manage the firmware-updates repository**

The *firmware-updates repository* contains a catalog of available updates and the update packages that can be applied to the managed devices.

The *catalog* contains information about firmware updates that are currently available for all devices that XClarity Administrator supports. The catalog organizes the firmware updates by device type. When you refresh the catalog, XClarity Administrator retrieves information about the latest available firmware updates from the Lenovo website (including the metadata .xml and readme .txt files) and stores the information in the firmware-updates repository. The payload file (.exe) is not downloaded. For more information about refreshing the catalog, see Refreshing the product catalog.

If new firmware updates are available, you must first download the update packages before you can update that firmware on the managed devices. Refreshing the catalog does not automatically download update packages. The **Product Catalog** table on the Firmware Updates Repository page identifies which update packages are downloaded and which are available for download.

You can download firmware updates in a few different ways:

- **Firmware-update repository packs**

  Firmware-update repository packs are collections of the latest firmware that is available at the same time as the XClarity Administrator release for all supported devices and a refreshed default firmware-compliance policy. These repository packs are imported and then applied from the Update Management Server page. When you apply a firmware-update repository pack, each update package in the pack is added to the firmware-updates repository, and a default firmware-compliance policy is automatically created for all manageable devices. You can copy this predefined policy, but you cannot change it.

  The following repository packs are available:

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all CMMs and Flex System switches.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all RackSwitch switches and Lenovo Storage devices.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all Converged HX Series, Flex System, NeXtScale, and System x servers.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all ThinkAgile and ThinkSystem servers.
  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all ThinkAgile and ThinkSystem V2 servers.

  You can determine whether firmware-update repository packs are stored in the repository from the **Download Status** column on Update Management Server page. This column contains the following values:

  - **Downloaded**. The firmware-update repository pack is stored in the repository.
  - **Not Downloaded**. The firmware-update repository pack is available but not stored in the repository.

- **UpdateXpress System Packs (UXSPs)**

  UXSPs contains the latest available firmware and device driver updates, organized by operating system. When you download UXSPs, XClarity Administrator downloads the UXSP, based on the version that is listed in the catalog, and stores the update packages in the firmware-updates repository. When you download a UXSP, each firmware update in the UXSP is added to the firmware-updates repository and listed on the **Individual Updates** tab, and a default firmware-compliance policy is automatically created for all manageable devices using the name *<uxsp-version>-<date>-<server-short-name>*`-UXSP` (for example, `v1.50-2017-11-22- SD530-UXSP`). You can copy this predefined policy, but you cannot change it.

  Note: When you download or import UXSPs from the Firmware Updates: Repository page, only firmware updates are downloaded and stored in the repository. Device driver updates are discarded. For information about downloading or importing Windows device driver updates using UXSPs, see Managing the OS device-drivers repository.

  You can determine whether UXSPs are stored in the firmware-updates repository from the **Download Status** column on the **Individual Updates** tab of the Firmware Updates: Repository page. This column contains the following values:

  – **Downloaded**. The entire update package or the individual firmware update is stored in the repository.
  – *x* **of** *y* **Downloaded**. Some but not all firmware updates in the update package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
  – **Not Downloaded**. The entire update package or the individual firmware update is available but not stored in the repository.

- **Individual firmware updates**

  You can download individual firmware-update packages, at one time. When you download firmware-update packages, XClarity Administrator downloads the update, based on the version that is listed in the catalog, and stores the update packages in the firmware-updates repository. You can then create firmware-compliance policies using those update packages for each of your managed devices.

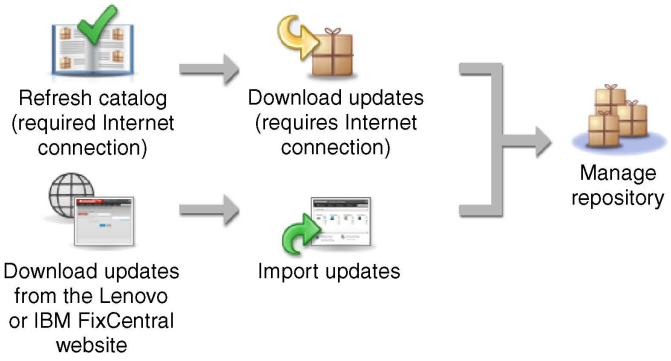
  Note: The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

  You can determine whether specific *firmware updates* are stored in the firmware-updates repository from the **Download Status** column on the **Individual Updates** tab on the Firmware Updates: Repository page. This column contains the following values:

  – **Downloaded**. The entire update package or the individual firmware update is stored in the repository.
  – *x* **of** *y* **Downloaded**. Some but not all firmware updates in the update package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
  – **Not Downloaded**. The entire update package or the individual firmware update is available but not stored in the repository.

XClarity Administrator must be connected to the Internet to refresh the catalog and download firmware-update. If it is not connected to the Internet, you can manually download the files to a

workstation that has network access to the XClarity Administrator host using a web browser and then import the files into the firmware-updates repository.



When you manually import firmware updates into XClarity Administrator, you must include the following required files: payload (image and MIB), metadata XML, change history, and readme. For example:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Attention:

- Only import these required files. Do not import other files that might be found on the firmware download websites.
- If you do not include the XML file in the update package, the update is not imported.
- If you do not include all required files that are associated with the update, the repository shows that the update is not downloaded, which means that it is partially imported. You can then import the missing files by selecting and importing them.
- The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

For more information about the firmware updates, see Managing the firmware-updates repository.

Step 2. **(Optional) Create and assigning firmware-compliance policies**

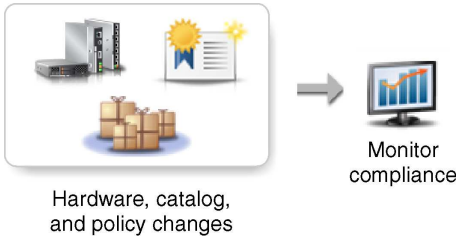
Firmware-compliance policies ensure that the firmware on certain managed devices is at the current or specific level by flagging the devices that need attention. Each firmware-compliance policy identifies which devices are monitored and which firmware level must be installed to keep the devices in compliance. You can set compliance at the device or firmware component level. XClarity Administrator then uses these policies to check the status of managed devices and to identify devices that are out of compliance.

When you create a firmware-compliance policy, you can choose to have XClarity Administrator flag a device when:

- The firmware on the device is down level
- The firmware on the device does not exactly match the compliance target version

XClarity Administrator comes with a predefined firmware-compliance policy named **Latest firmware in repository**. When new firmware is downloaded or imported into the repository, this policy is updated to include latest available versions of firmware in the repository.

After a firmware-compliance policy is assigned to a device, XClarity Administrator checks the compliance status of each device when the device inventory changes or firmware-updates repository changes. When the firmware on a device is not compliant with the assigned policy, XClarity Administrator identifies that device as not compliant on the Firmware Updates: Apply / Activate page, based on the rule that you specified in the firmware-compliance policy



For example, you can create a firmware-compliance policy that defines the baseline level for firmware that is installed in all ThinkSystem SR850 devices and then assign that firmware-compliance policy to all managed ThinkSystem SR850 devices. When the firmware-updates repository is refreshed and a new firmware update is added, those compute nodes might become out of compliance. When that happens, XClarity Administrator updates the Firmware Updates: Apply / Activate page to show that the devices are not compliant and generates an alert.

Note: You can choose to show or hide alerts for devices that do not meet the requirements of their assigned firmware-compliance policies (see Configuring global firmware-update settings). Alerts are hidden by default.

For more information about the firmware-compliance policies, see Creating and assigning firmware-compliance policies.

Step 3. **Applying and activating updates**

XClarity Administrator does not automatically apply firmware updates to managed devices. To update firmware, you must manually apply and active the update on selected devices. You can apply the firmware in one of the following ways:

- **Apply bundled firmware updates using compliance policies**

  You can apply firmware updates to *all* components in the selected devices according to the assigned firmware-compliance policy using a bundle image that contain the applicable firmware update packages.

  The bundled-update process first updates the baseboard management controller and UEFI out of band. When these updates are complete, the process creates a bundled image of remaining firmware in the compliance policy based on the machine type. Then, the process mounts the image to the selected device and restarts the device to boot the image. The image automatically runs to perform the remaining updates.

  Attention: Selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.

  Notes:

- Applying bundled firmware updates is supported only for ThinkSystem SR635 and SR655 servers.
- Applying bundled firmware updates is supported only for IPv4 address. IPv6 addresses are not supported.
- Ensure that each target device was booted to the OS at least once to retrieve the full inventory information.
- Baseboard management controller firmware v2.94 or later is required to use the bundled-update function.
- Only firmware updates from repository packs or individual firmware updates are used. UpdateXpress System Packs (UXSPs) are not supported.
- Only downloaded firmware updates are applied. Refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.
- Compliance check is supported only for the baseboard management controller and UEFI in ThinkSystem SR635 and SR655 servers; however, XClarity Administrator attempts to apply firmware updates to all available hardware components.
- Updates are applied according to the assigned firmware-compliance policy. You cannot choose to update a subset of components.
- XClarity Administrator v3.2 or later is required to apply firmware updates for Lenovo XClarity Provisioning Manager (LXPM), LXPM windows drivers, or LXPM Linux drivers to ThinkSystem SR635 and SR655 servers.
- The baseboard management controller and UEFI updates are skipped if the currently installed version is higher than the assigned compliance policy.
- Firmware-compliance policies must be created and assigned to the devices on which you intend to apply firmware updates. For more information, see Creating and assigning firmware-compliance policies.
- The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

- **Apply selected firmware updates with or without compliance policies**

  You can apply firmware updates on selected components and devices according to the assigned firmware-compliance policy using applicable firmware-update packages. You can also choose to apply firmware updates that are later than the currently installed firmware on selected components and devices without using compliance policies.

  You can choose to apply updates for all components in a specific device. You can also choose to update only a subset of components in the selected devices, such as the baseboard management controller or UEFI.

  To activate the firmware updates, the devices must be restarted. (Note that restarting a device is disruptive.) You can choose to restart the devices as part of the update process (called *immediate activation*), or wait until a maintenance window is available to restart the devices (called *delayed activation*). In this case, you must manually restart the device for the update to take effect.

  When you choose to update the firmware for a managed device, the following steps occur:

  1. XClarity Administrator sends the firmware updates (for example, for the management controller, UEFI, and DSA) to the device.

2. When the device is restarted, the firmware updates are activated on the device.
3. For servers, XClarity Administrator sends updates for optional devices, such as network adapter and hard drive updates. XClarity Administrator applies these updates, and the server is restarted
4. When you restart the device or choose immediate activation, the updates for the optional devices are activated.

Notes:

- When applying updates using compliance policies, a firmware-compliance policy must be created and assigned to each target devices. For more information, see Creating and assigning firmware-compliance policies.
- If you choose to install a firmware-update package that contains updates for multiple components, all components to which the update package applies are updated.
- Updates to CMMs and Flex switches are always activated immediately, even if you select delayed activation.

When you perform updates on a set of devices, XClarity Administrator performs the updates in the following order:

- Chassis CMM
- RackSwitch and Flex System switches
- Flex compute nodes, and rack and tower servers
- Lenovo Storage devices

Attention: Before you attempt to apply firmware updates on managed devices, ensure that you have completed the following actions:

- Read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).
- Initially, devices that are not supported for updates are hidden from the view. Devices that are not supported cannot be selected for updates.
- By default, all detected components are listed as available for applying updates; however, down-level firmware might prevent a component from appearing in inventory or reporting full-version information. To list all policy-based packages that are available for you to apply updates, click **All Actions → Global Settings**, and selecting **Enhanced Support for Down-Level Devices**. When this option is selected, “Other Available Software” is listed in the Installed Version column for undetected devices. For more information, see Configuring global firmware-update settings.

  Notes:

  - The global settings cannot be changed when updates to managed devices are in progress.
  - It takes a few minutes to generate the additional options. After a few moments, you might need to click the **Refresh** icon ( ) to refresh the table.
- Ensure that no jobs are currently running on the target server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.
- Ensure that the firmware-updates repository contains the firmware packages that you intend to deploy. If not, refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.

If you intend to install prerequisite firmware, ensure that the prerequisite firmware is downloaded in the repository as well.

In some cases, multiple versions might be needed to update firmware, and all versions would need to be downloaded to the repository. For example, to upgrade the IBM FC5022 SAN scalable switch from v7.4.0a to v8.2.0a, you must first install v8.0.1-pha, then v8.1.1, and then v8.2.0a. All three versions must be in repository to update the switch to v8.2.0a.

- Typically, devices must be restarted to activate the firmware update. If you choose to restart the device during the update process (*immediate activation*), ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

For more information about installing updates, see Applying and activating firmware updates.

Firmware-update considerations

Before you begin updating firmware for managed devices by using Lenovo XClarity Administrator, review the following important considerations.

General considerations

- **Minimum required levels of firmware.**

  Ensure that the firmware that is installed on each managed device is at the minimum required level before using XClarity Administrator to update firmware on those devices. For information about firmware requirements, see Supported firmware in the XClarity Administrator online documentation.

  Note: For information about I/O device support and known limitations, see the XClarity Administrator Support – Compatibility webpage.

- **Update all components to the level that is included in the firmware-updates repository.**

  Because firmware updates for Flex System components are tested and released together, it is recommended that you maintain the same firmware level on all components in a Flex System chassis. Therefore, it is important to update firmware on all components in the chassis in the same maintenance window. XClarity Administrator applies the selected updates in the correct sequence automatically.

- **LXPM Linux Drivers and LXPM Windows Drivers are not included when downloading UXSPs**

  Lenovo XClarity Provisioning Manager (LXPM) Linux and Windows drivers are not included in UpdateXpress System Packs (UXSPs). To apply these update packages to your devices, either download the latest firmware-update repository packs or manually download the individual packages and create a firmware compliance policy to include those packages.

- **Some firmware updates are codependent on a minimum level of device driver.**

  Before applying adapter and I/O firmware updates on a server, you might be required to update the device driver to a minimum level. In general, firmware updates are not dependent on specific levels of device drivers. Refer to the firmware update readme for such co-dependencies, and update the device drivers in your operating system before updating the firmware. XClarity Administrator does not update device drivers in your operating system.

- **Reboot XClarity Administrator before updating firmware**

  If previous attempts to update firmware fails, reboot XClarity Administrator before updating firmware. Rebooting the management sever ensures that the system reserved account that is used to update firmware is synchronized on the managed devices.

- **Firmware updates are disruptive and require workloads to be quiesced on devices.**

Performing firmware updates on managed devices is disruptive if you choose to immediately activate the update. You must quiesce the devices before updating firmware using immediate activation.

When updating firmware on servers, the servers are shut down and placed in a maintenance operating system to update device drivers for adapters, disk drives, and solid-state drives.

Flex switches in a given chassis are updated sequentially and are restarted during the firmware update process. Implementing redundant data paths lessens the disruption, but there might still be a brief interruption in network connectivity during the firmware update.

- **Do not use XClarity Administrator to update the firmware on the server on which XClarity Administrator is running.**

  If XClarity Administrator is running on a hypervisor host that runs on a server that it is managing, do not use XClarity Administrator to update firmware on that server. When firmware updates are applied with immediate activation, XClarity Administrator forces the target server to restart, which would restart the hypervisor host and XClarity Administrator as well. When applied with deferred activation, only some firmware is applied until the target system is restarted

CMM considerations

- **Virtually reseat CMMs before updating firmware .**

  If you are updating CMMs that are running firmware level stack release 1.3.2.1 2PET12K through 2PET12Q, that have been running for more than three weeks, and are in a dual-CMM configuration, you must virtually reseat both the primary and standby CMMs before updating firmware (see Virtually reseating a CMM.

Baseboard-management controller considerations

- **Minimum required BMC levels for Pending-Activation status**

  To see the pending-activation status, the following firmware version must be installed on the primary baseboard management controller in the server.
  - **IMM2**: TCOO46F, TCOO46E, or later (depending on the platform)
  - **XCC**: CDI328M, PSI316N, TEI334I, or later (depending on the platform)

- **Updates applied to the primary management controller and UEFI firmware partitions.**

  Baseboard management-controller (BMC) and UEFI updates can be applied to the primary and backup firmware partitions for the management controller and UEFI independently.

  You can also apply management controller and UEFI updates to only the primary firmware partitions on the server. By default, the management controller is configured to synchronize the backup management controller partition with the primary management controller partition after the primary management controller has been running satisfactorily and the new level is ready to promote to backup. However, the management controller is not configured to synchronize the UEFI backup partition by default. Therefore, consider one of the following options on the management controller:

  - Enable the automatic synchronization of the UEFI backup partition.

    This ensures that both the primary and backup partitions are running the same level of firmware (and that the backup UEFI firmware is compatible with the management controller firmware).
  - Disable the automatic synchronization of the management-controller backup partition.

    Although not recommended, this gives you complete control over the firmware levels for the management controller and the UEFI. However, you must manually update the management controller and UEFI firmware for both partitions.

  You use firmware-compliance policies to determine which updates are applied to each device. For more information about firmware-compliance policies, see Creating and assigning firmware-compliance policies.

Note: If the management controller and UEFI are configured to automatically synchronize the backup firmware from the primary, it is not necessary for XClarity Administrator to update the backup banks. In that case, you can clear the backup bank updates when applying updates to a server or remove the backup banks from the firmware-compliance policy.

- **Possibility of VMware vSphere ESXi system failure (host purple diagnostic screen) when a management controller is reset.**

  If you are running VMware vSphere ESXi on any server, ensure that the following minimum VMware ESXi levels are installed before updating the firmware on the server:

  – If you are running VMware vSphere ESXi 5.0, install a minimum level of 5.0u2 (update 2)

  – If you are running VMware vSphere ESXi 5.1, install a minimum level of 5.1u1 (update 1)

  If you do not install these minimum levels, a VMware vSphere ESXi system failure (host purple diagnostic screen) might occur whenever the management controller is reset, including when management-controller firmware is applied and activated.

  Note: This issue does not affect ESXi v5.5.

ThinkSystem device considerations

- **For ThinkSystem SE350 servers running XCC firmware version earlier than 20A, IPMI over KCS Access must be manually enabled in the baseboard management controller to ensure that the management controller can communicate with XClarity Administrator.**

  For ThinkSystem SE350 servers, IPMI over KCS is disabled by default. For ThinkSystem SE350 servers running XCC firmware version 20A or later, XClarity Administrator automatically enables IPMI over KCS during a firmware update and then disables it after the firmware update is complete. However, for ThinkSystem SE350 servers running XCC firmware version earlier than 20A, you must manually enable this option from the Lenovo XClarity Controller user interface by clicking **BMC Configuration → Security → IPMI over KCS Access**.

- For ThinkSystem SR635 and SR655 servers, the following limitations apply.

  – Only Immediate activation is supported. Delayed activation and Prioritized activation are not supported.

  – For XClarity Administrator v3.1.1 and later, you can use the bundled update function to update all components on ThinkSystem SR635 and SR655 servers, including baseboard management controller, UEFI, disk drives, and IO options.

    Attention: Selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.

    Notes:

    – Applying bundled firmware updates is supported only for ThinkSystem SR635 and SR655 servers.

    – Applying bundled firmware updates is supported only for IPv4 address. IPv6 addresses are not supported.

    – Ensure that each target device was booted to the OS at least once to retrieve the full inventory information.

    – Baseboard management controller firmware v2.94 or later is required to use the bundled-update function.

    – Only firmware updates from repository packs or individual firmware updates are used. UpdateXpress System Packs (UXSPs) are not supported.

- Only downloaded firmware updates are applied. Refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.
- Compliance check is supported only for the baseboard management controller and UEFI in ThinkSystem SR635 and SR655 servers; however, XClarity Administrator attempts to apply firmware updates to all available hardware components.
- Updates are applied according to the assigned firmware-compliance policy. You cannot choose to update a subset of components.
- XClarity Administrator v3.2 or later is required to apply firmware updates for Lenovo XClarity Provisioning Manager (LXPM), LXPM windows drivers, or LXPM Linux drivers to ThinkSystem SR635 and SR655 servers.
- The baseboard management controller and UEFI updates are skipped if the currently installed version is higher than the assigned compliance policy.
- Firmware-compliance policies must be created and assigned to the devices on which you intend to apply firmware updates. For more information, see Creating and assigning firmware-compliance policies.
- The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

  You can also use the traditional update function to apply firmware updates to only the baseboard management controller and UEFI.
- For XClarity Administrator v3.0:
  - Management data is not correctly updated when updating firmware from 20A to 20B or 20C. To work around this issue, either unmanage and then manage the device again, or restart XClarity Administrator.
  - Downgrading firmware updates is not supported.
- For XClarity Administrator v2.8 and later
  - You can update baseboard management controller and UEFI firmware using the traditional update process. Baseboard management controller firmware version AMBT10M or later is required, and UEFI firmware version CFE114L or later is required.
  - Firmware updates are not supported in the following situations.
    - If XClarity Administrator v2.7 manages ThinkSystem SR635 and SR655 servers running 20A firmware, and you upgrade to 20B firmware using the baseboard management controller before upgrading to XClarity Administrator v2.8.
    - If XClarity Administrator v2.7 manages ThinkSystem SR635 and SR655 servers running 20B firmware before upgrading to XClarity Administrator v2.8.
    - If XClarity Administrator v2.8 manages ThinkSystem SR635 and SR655 servers running 20A firmware, and you upgrade to 20B firmware using the baseboard management controller.

- **XClarity Administrator v2.1, v2.2, and v2.3 require a cumulative patch to manage ThinkSystem servers running BMC firmware TEI342s-2.40, CDI334v-2.50, or PSI322k-1.50.**

  For XClarity Administrator v2.1, v2.2, and v2.3, before updating BMC firmware on ThinkSystem servers to version TEI342s-2.40, CDI334v-2.50, or PSI322k-1.50, you must either apply the latest XClarity Administrator Virtual Appliance Cumulative Patch or update to XClarity Administrator v2.4. XClarity Administrator v2.0 or earlier does not require the cumulative patches.
- **Firmware updates is not supported on ThinkSystem servers using DHCPv6 or statically assigned IPv6 addresses**

When using IPv6 addressing on ThinkSystem servers, firmware updates is supported on only IPv6 Link-Local Address(LLA) and stateless addresses.

- **When updating firmware to version 20D, you must update both UEFI and XCC together.**

  UEFI and Lenovo XClarity Controller (XCC) must be updated together for version 20D. Updating XCC and not UEFI, and vice versa, will cause issues.

Flex System device considerations

- **Ensure that the Flex switches that are being updated are powered on,**
- **Select Immediate Activation when updating compute nodes that are at management-controller firmware levels earlier than Flex System 1.3.2.**

  When you apply the Flex System 1.3.2, 2nd Quarter lifecycle release to a compute node, you must choose *immediate activation* to update the compute node. Immediate activate forces the compute node to restart during the update process.

- **Flex switches must be configured with an IP address that is reachable from XClarity Administrator.**

  The target Flex switch must be assigned an IP address that can communicate with XClarity Administrator so that XClarity Administrator can download and apply the firmware update.

- **Update support on scalable complexes, such as x480 X6 and x880 X6 nodes.**

  Update support on scalable nodes such as the Flex System x480 X6 and x880 X6 compute nodes is limited to configurations where the complex is configured as a *single partition* that includes all compute nodes that are part of the multi-node complex. You cannot use XClarity Administrator to update a complex that consists of multiple partitions.

  If you assign a firmware-compliance policy to a partition that includes multiple servers in a scalable complex (such as Flex System x480 X6 and x880 X6 compute nodes), XClarity Administrator updates firmware on all management controllers and UEFIs for each server in the partition by default. However, if you select a subset of components within the partition, XClarity Administrator updates the firmware on only the selected components in the partition.

- **Before updating the CMM2 to v1.30 (1AON06C) or later, Flex switches must be running Level 3 version of Enhanced Configuration and Management (EHCM L3)**

  CMM2 and the Flex switches communicate using the EHCM protocol. This protocol is required for XClarity Administrator to update the Flex switches. When you update a CMM2 to v1.30 (1AON06C) or later, XClarity Administrator verifies that the Flex switches are running EHCM L3 and if not, cancels the CMM update with a warning that the Flex switches must be first updated to a version that supports EHCM-L3. You can override this verification by selecting **Attempt to update components already in compliance** when updating the CMM firmware.

  Attention: There is currently no firmware version for Flex System EN6131 Ethernet switches and IB6131 InfiniBand switches that support EHCM L3. This means that after you update the CMM2 to firmware v1.30 (1AON06C) or later, you can no longer use XClarity Administrator to update those switches. The work-around is to use the management controller web interface or command-line interface for the chassis to update the switch.

Flex System switch	Version	Release date
CN4093	7.8.4.0	June 2014
EN4023	6.0.0	April 2015
EN4093	7.8.4.0	June 2014
EN4093R	7.8.4.0	June 2014

Flex System switch	Version	Release date
EN6132	Not available	Not available
FC3171	9.1.3.02.00	June 2014
FC5022	7.4.0b1	March 2016
IB6132	Not available	Not available
SI4091	7.8.4.0	June 2014
SI4093	7.8.4.0	June 2014

Note: The EN2092 1-Gb Ethernet Scalable Switch does not require EHCM L3 and does not have this restriction.

Storage considerations

- **ThinkSystem DM storage devices considerations**

  To update firmware on ThinkSystem DM storage devices, the devices must be running v9.7 or later.

  Downgrading is supported for only minor versions. For example, you can downgrade 9.7P11 to 9.7P9; however you cannot downgrade 9.8 to 9.7.

  To download firmware for ThinkSystem DM series storage devices:

  – One or more ThinkSystem DM series storage devices must be managed by XClarity Administrator.
  – Each ThinkSystem DM series storage device must be entitled for hardware service and support.
  – You must specify the country where the ThinkSystem DM series storage devices are located on the Firmware Updates: Repository page. Only encrypted firmware can be downloaded for devices in the following countries: Armenia, Belarus, China, Cuba, Iran, Kazakhstan, Kyrgyzsta, North Korea, Russia, Sudan, Syrian.

- **Disk drives must be in the JBOD, Online, Ready, or Unconfigured (good) state.**

  To update firmware on disk drives, the RAID state must be JBOD, Online, Ready, or Unconfigured (good). Other states are not supported. To determine the RAID state for a disk drive, go to the Inventory page for the device, expand the **Drives** section, and check the **RAID State** column for that disk drive (see Viewing the details of a managed server).

- **Firmware version does not detect disk drives and solid state drives.**

  XClarity Administrator detects only the installed-firmware version and performs a compliance check for disk drives and solid-state drives (SSDs) that are attached to a MegaRAID or an NVME adapter. Other attached drives might have a level of firmware that is not supported or might not support firmware-version reporting. However, firmware updates are applied to those drives when selected.

- **NVMe firmware is applied even if it is not identified with a target component**

  On the Apply/Activate page, the NVMe firmware version is listed for solid state drives (SSDs). Because no target firmware update is identified for discovered NVMe devices, a warning message is displayed when you attempt to update the target system. However, the HDD/SSD update is applied even if it is not identified with a target component, so the NVMe firmware is still updated.

- **Applying the ServeRAID M5115 PSoC3 update package from XClarity Administrator requires a minimum installed level of 68.**

  The ServeRAID M5115 PSoC3 (Programmable System-on-Chip) update from earlier than version 68 must be done in a controlled manner.

Tip: You can view the code version for the ServeRAID M5115 PSoC3 by logging in to the CMM web interface and selecting the **Firmware** tab for the target compute node. Then, select the expansion card for the ServeRAID M5115 adapter. The PSoc3 code version is the GENERIC firmware type.

For installed versions earlier than 68, you cannot update using XClarity Administrator. Instead you must perform the following steps from either the Chassis Management Module (CMM) web interface or the command-line interface (CLI):

- **Using the CMM web interface:**
  1. Log in to the Chassis Management Module (CMM) web interface.
  2. From the main menu, click **Service and Support → Advanced**.
  3. Click the **Service Reset** tab.
  4. Select the appropriate compute node by clicking its radio button.
  5. From the **Reset** pull down button, click **Virtual Reseat**.
  6. Click **OK** to confirm.
- **Using the CMM CLI**:
  - Log in to the CMM Secure Shell (SSH) interface.
  - Enter the following command to perform a virtual reseat:
    `'service -vr -T blade[x]`

    where *x* is the bay number of the compute node to be reseated.

After the system is powered back on, boot to the operating system and update the ServeRAID M5115 PSoC3 using the extracted embedded update package. Complete the following steps to extract the embedded package.

- **Using Microsoft Windows:**

  Open the update package (lnvgy_fw_psoc3_m5115-70_windows_32-64.exe), and select Extract to Hard Drive. Then, select the path where the embedded package is to be extracted.
- **Using Linux:**

  Run the following command:

  `lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x`

  where *x* is the location where the embedded package is to be extracted.

Managing the firmware-updates repository

The *firmware-updates repository* contains a catalog of available updates and the update packages that can be applied to the managed devices.

About this task

The *catalog* contains information about firmware updates that are currently available for all devices that XClarity Administrator supports. The catalog organizes the firmware updates by device type. When you refresh the catalog, XClarity Administrator retrieves information about the latest available firmware updates from the Lenovo website (including the metadata .xml and readme .txt files) and stores the information in the firmware-updates repository. The payload file (.exe) is not downloaded. For more information about refreshing the catalog, see Refreshing the product catalog.

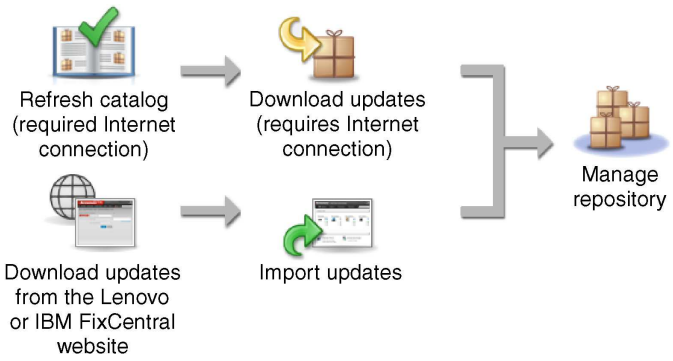
If new firmware updates are available, you must first download the update packages before you can update that firmware on the managed devices. Refreshing the catalog does not automatically download update

packages. The **Product Catalog** table on the Firmware Updates Repository page identifies which update packages are downloaded and which are available for download.

You can download firmware updates in a few different ways:

- **Individual firmware updates**. You can download individual firmware-update packages, at one time, based on the version that is listed in the catalog.
- **UpdateXpress System Packs (UXSPs)**. UXSPs contains the latest available firmware and device driver updates, organized by operating system. When you download UXSPs from the Firmware Updates: Repository page, only firmware updates are downloaded and stored in the repository. Device driver updates are excluded.
- **Firmware-update repository packs**. Repository packs contains the latest available firmware updates for all supported devices and a refreshed default firmware-compliance policy. These repository packs are imported and then applied from the Update Management Server page.

XClarity Administrator must be connected to the Internet to refresh the catalog and download firmware-update. If it is not connected to the Internet, you can manually download the files to a workstation that has network access to the XClarity Administrator host using a web browser and then import the files into the firmware-updates repository.



When you manually import firmware updates into XClarity Administrator, you must include the following required files: payload (image and MIB), metadata XML, change history, and readme. For example:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Attention:

- Only import these required files. Do not import other files that might be found on the firmware download websites.
- If you do not include the XML file in the update package, the update is not imported.
- If you do not include all required files that are associated with the update, the repository shows that the update is not downloaded, which means that it is partially imported. You can then import the missing files by selecting and importing them.
- The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

After the firmware-updates are downloaded in the repository, information is provided about each update, including the release date, size, policy usage, and severity. The severity indicates the impact and the need to apply the update to help you to assess how your environment might be affected.

- **Initial Release**. This is the first release of the firmware.
- **Critical**. The firmware release contains urgent fixes for data corruption, security, or stability issue.
- **Suggested**. The firmware release contains significant fixes for problems that you are likely to encounter.
- **Non-Critical**. The firmware release contains minor fixes, performance enhancements, and textual changes.

Notes:

- The severity is relative to the previously released version of the update. For example, if the installed firmware is v1.01, and update v1.02 is Critical and update v1.03 is Recommended, this means that the update from 1.02 to 1.03 is recommended, but the update from v1.01 to v1.03 is critical because it is cumulative (v1.03 includes v1.02 critical issues).
- Special cases might arise where an update is only critical or recommended for a specific machine type or operating system. Refer to the Release Notes for additional information.

Procedure

To view firmware updates that are available in the product catalog, complete the following steps.

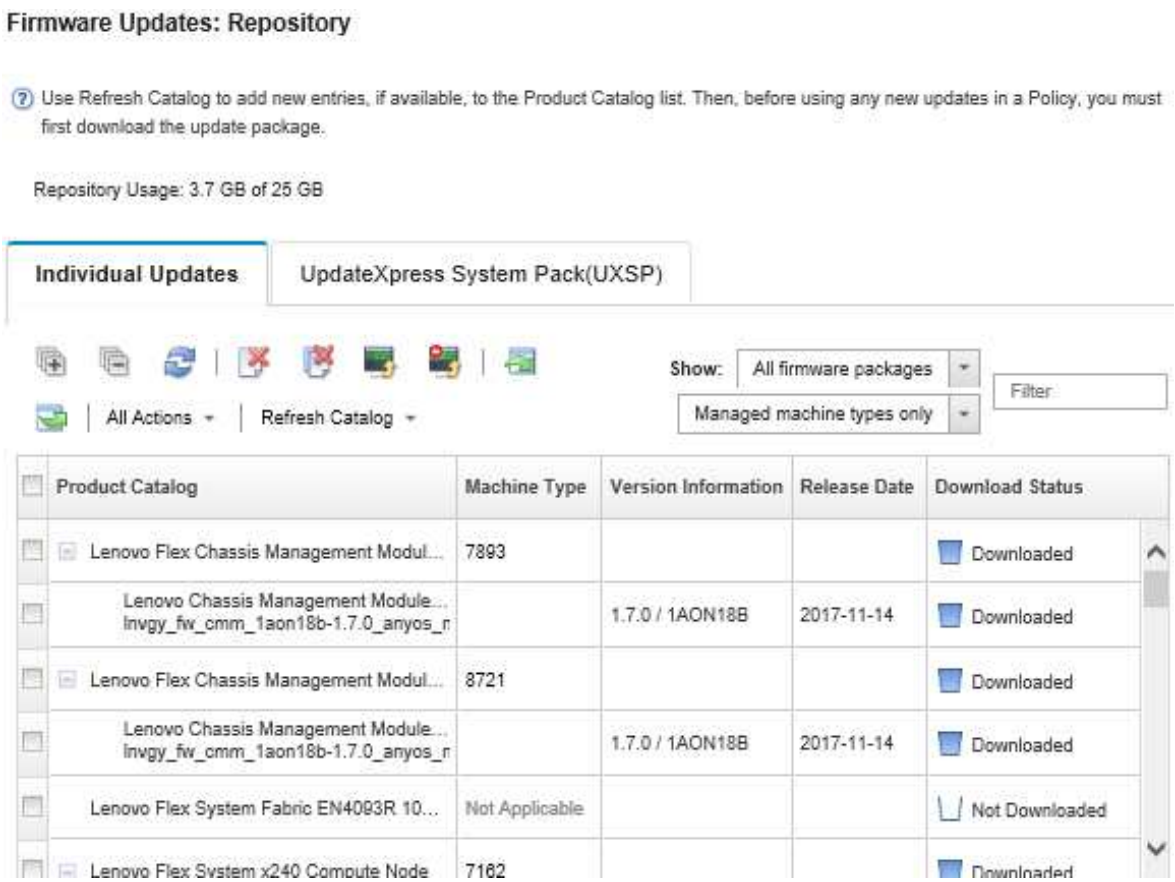
Step 1. From the XClarity Administrator menu bar, click **Provisioning → Repository**. The Firmware Updates Repository page is displayed with a list of available firmware-update packages, organized by device type.

Step 2. Click the **Individual Updates** tab to view information about available firmware update packages, or click the **UpdateXpress System Packs (UXSPs)** tab to view information about available UXSPs

Step 3. Expand a device and device components to list the update packages and firmware updates for that device.

You can sort the table columns and click the **Expand all** icon ( ) and **Collapse all** icon ( ) to make it easier to find specific firmware updates. In addition, you can filter the list of displayed devices and firmware updates by selecting an option in the **Show** menu to list only firmware updates of a specific age, firmware updates for all server types or only managed-server types or by entering text in the **Filter** field. Note that if you search for specific devices, only the devices are listed; firmware updates are not listed under the device name.

Note: For servers, specific update packages are available based on the type of server. For example, if you expand a server, such as the Flex System x240 Compute Node, update packages that are available specifically for that compute node are displayed.



Results

From this page, you can perform the following actions:

- Refresh this page with the current firmware-update information in the catalog by clicking the **Refresh** icon ( ).
- Retrieve the latest information about available updates by clicking **Refresh Catalog**.Retrieving this information might take several minutes to complete. For more information, see Refreshing the product catalog.
- Add the firmware updates to the repository by selecting one or more update packages or updates in the product catalog and then clicking the **Download** icon ( ). When the firmware updates are downloaded and added to the repository, the status changes to “Downloaded.”

  Note: The XClarity Administrator must be connected to the Internet to acquire updates through the XClarity Administrator user interface. If it is not connected to the Internet, you can import updates that you previously downloaded.

  For more information about downloading updates, see Downloading firmware updates.
- Import firmware updates that you manually downloaded to a workstation that has network access to XClarity Administrator by selecting one or more updates and then clicking the **Import** icon ( ).For more information about importing updates, see Downloading firmware updates.
- Stop firmware downloads that are currently in progress by selecting one or more updates and then clicking the **Cancel Downloads** icon ( ).Canceling downloads cancels *all* firmware downloads that are in progress. You can monitor the detailed progress of and stop a specific firmware download from the jobs log (see Monitoring jobs).

- Delete update packages or individual updates from the repository (see Deleting firmware updates).
- Export firmware updates that exist in the firmware-updates repository to a local system (see Exporting and importing firmware updates).

Using a remote repository for firmware updates

By default, Lenovo XClarity Administrator uses a local (internal) repository for storing firmware updates. You can free up disk space that is available to the XClarity Administrator local repository by using a mounted remote share over SSH File System (SSHFS) as a remote repository. You can then use firmware update files directly from the remote repository to maintain firmware compliance on your devices.

Before you begin

Only firmware updates can be stored on the remote share. Windows device drivers and XClarity Administrator updates can be stored only in the local updates repository.

Ensure that SFTP service on port 22 is open on the remote-share server. The baseboard management controllers must have access to this port.

The remote share is used as an SFTP server when it is used as a firmware repository. Ensure that you do not disable SFTP when updating the SSHD configuration.

About this task

When you change the location of the firmware updates repository, you can choose to copy all firmware update from the original repository to the new repository.

Firmware update files in the original repository *are not* automatically cleaned up after switching locations.

If XClarity Administrator has read-write permissions on the remote repository, the behavior is the same as using the local repository. However, if XClarity Administrator has read-only permissions, you cannot refresh the catalog, or download or import updates to the repository.

The same remote repository can be shared by multiple XClarity Administrator instances; however, if one XClarity Administrator instance changes the repository, the other XClarity Administrator instances are not notified automatically. You must refresh the repository to get the latest details. To refresh the repository, click **All Actions → Refresh Repository** from the Firmware Updates: Repository page.

Note: Take care when deleting firmware updates and UXSPs if the firmware-updates repository is located on a remote share that by multiple XClarity Administrator instances.

Procedure

To use a remote firmware-updates repository, complete the following steps.

Step 1. Add a remote share to XClarity Administrator (see Managing remote shares).

Step 2. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.

Step 3. Click **All Actions → Swap Repository Location** to display the Swap Repository Location dialog.

Step 4. Select the remote share that you just created from the **Repository Location** drop down list.

Step 5. Optionally select **Clean up current repository** to delete firmware-update files from the current repository location.

Step 6. Optionally select **Copy update packages from current repository the new repository** to copy firmware-update files to the new repository location before switching the repository location.

By default, firmware-update files that exist in the new location are not copied over (are skipped). You can optionally choose to overwrite any existing files or overwrite only existing file with a different size or modification date from the **Overwrite Rules** drop-down list.

Step 7. Click **OK**.

A job is created to copy firmware update packages to the new repository. You can monitor the job progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

Refreshing the product catalog

The product catalog contains information about all firmware updates that are available for all devices that Lenovo XClarity Administrator supports, including chassis, servers, and Flex switches.

Before you begin

An Internet connection is required to refresh the product catalog.

Refreshing the catalog might take several minutes to complete.

About this task

When you refresh the catalog, XClarity Administrator retrieves information about the latest available firmware updates from the Lenovo XClarity Support website and stores the information to the firmware-updates repository.

Refreshing the catalog only adds information about available firmware updates to the repository. It does not download the update packages. You must download the firmware updates to make the updates available for installation. For more information about downloading updates, see Downloading firmware updates.

Procedure

To refresh the product catalog, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.

Step 2. Click the **Individual Updates** tab to retrieve information about individual firmware-update packages, or click the **UpdateXpress System Pack (UXSP)** tab to retrieve information about UXSPs.

Step 3. Click **Refresh Catalog**, and then click one of the following options to obtain information about the latest available firmware updates.

- **Refresh Selected - Latest Only**. Retrieves information about the most current version of firmware updates that are available for only the selected devices.
- **Refresh All - Latest Only**. Retrieves information about the most current version of all firmware updates for all supported devices.
- **Refresh Selected**. Retrieves information about all versions of firmware updates that are available for only the selected devices.
- **Refresh All**. Retrieves information about all versions of all firmware updates that are available for all supported devices.

Tip: You can refresh the product catalog and download the latest firmware in one step by clicking **All Actions → Refresh and download the latest for all managed devices** or **All Actions → Refresh and download the latest for selected devices**.

Downloading firmware updates

You can download or import firmware updates in the firmware-updates repository, depending on your access to the Internet. Firmware updates must be available in the firmware-updates repository before you can update firmware on management devices.

Before you begin

Ensure that all ports and Internet address that Lenovo XClarity Administrator requires are available before you attempt to download firmware. For more information about ports, see Port availability and Firewalls and proxy servers in the XClarity Administrator online documentation.

If a device type is not listed in the firmware-updates repository, you must first manage a device of that type before downloading or importing individual firmware updates for that device type.

Important:

- For XClarity Administrator v1.1.1 and earlier, you must manually download and import the firmware updates for Lenovo hardware from Lenovo Data Center Support website.
- XClarity Administrator cannot download updates for RackSwitch switches and Lenovo DE, DX, and SS series storage devices from the Lenovo website to the firmware-updates repository; instead, you must manually download and import these updates from the Lenovo website to a workstation that has network access to the XClarity Administrator host, or download and apply the *firmware-update repository packs*, which contain all available firmware updates.
- Internet Explorer and Microsoft Edge web browsers have an upload limit of 4 GB. If the file that you are importing is greater than 4 GB, consider using another web browser (such as Chrome or Firefox).
- To download firmware for ThinkSystem DM series storage devices:
  - One or more ThinkSystem DM series storage devices must be managed by XClarity Administrator.
  - Each ThinkSystem DM series storage device must be entitled for hardware service and support.
  - You must specify the country where the ThinkSystem DM series storage devices are located on the Firmware Updates: Repository page. Only encrypted firmware can be downloaded for devices in the following countries: Armenia, Belarus, China, Cuba, Iran, Kazakhstan, Kyrgyzsta, North Korea, Russia, Sudan, Syrian.

About this task

You can download firmware updates in a few different ways:

- **Firmware-update repository packs**

  Firmware-update repository packs are collections of the latest firmware that is available at the same time as the XClarity Administrator release for all supported devices and a refreshed default firmware-compliance policy. These repository packs are imported and then applied from the Update Management Server page. When you apply a firmware-update repository pack, each update package in the pack is added to the firmware-updates repository, and a default firmware-compliance policy is automatically created for all manageable devices. You can copy this predefined policy, but you cannot change it.

  The following repository packs are available:

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all CMMs and Flex System switches.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all RackSwitch switches and Lenovo Storage devices.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all Converged HX Series, Flex System, NeXtScale, and System x servers.

- **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all ThinkAgile and ThinkSystem servers.
- **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contains firmware updates for all ThinkAgile and ThinkSystem V2 servers.

You can determine whether firmware-update repository packs are stored in the repository from the **Download Status** column on Update Management Server page. This column contains the following values:

- **Downloaded**. The firmware-update repository pack is stored in the repository.
- **Not Downloaded**. The firmware-update repository pack is available but not stored in the repository.

- **UpdateXpress System Packs (UXSPs)**

  UXSPs contains the latest available firmware and device driver updates, organized by operating system. When you download UXSPs, XClarity Administrator downloads the UXSP, based on the version that is listed in the catalog, and stores the update packages in the firmware-updates repository. When you download a UXSP, each firmware update in the UXSP is added to the firmware-updates repository and listed on the **Individual Updates** tab, and a default firmware-compliance policy is automatically created for all manageable devices using the name <*uxsp-version*>-<*date*>-<*server-short-name*>-UXSP (for example, v1.50-2017-11-22- SD530-UXSP). You can copy this predefined policy, but you cannot change it.

  Note: When you download or import UXSPs from the Firmware Updates: Repository page, only firmware updates are downloaded and stored in the repository. Device driver updates are discarded. For information about downloading or importing Windows device driver updates using UXSPs, see Managing the OS device-drivers repository.

  You can determine whether UXSPs are stored in the firmware-updates repository from the **Download Status** column on the **Individual Updates** tab of the Firmware Updates: Repository page. This column contains the following values:

  - **Downloaded**. The entire update package or the individual firmware update is stored in the repository.
  - *x* **of** *y* **Downloaded**. Some but not all firmware updates in the update package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
  - **Not Downloaded**. The entire update package or the individual firmware update is available but not stored in the repository.

- **Individual firmware updates**

  You can download individual firmware-update packages, at one time. When you download firmware-update packages, XClarity Administrator downloads the update, based on the version that is listed in the catalog, and stores the update packages in the firmware-updates repository. You can then create firmware-compliance policies using those update packages for each of your managed devices.

  Note: The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

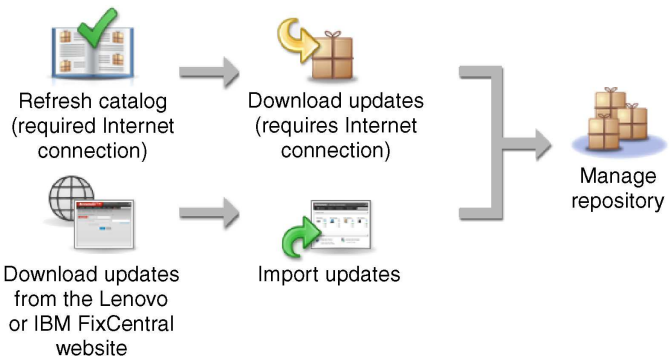
  You can determine whether specific *firmware updates* are stored in the firmware-updates repository from the **Download Status** column on the **Individual Updates** tab on the Firmware Updates: Repository page. This column contains the following values:

  - **Downloaded**. The entire update package or the individual firmware update is stored in the repository.

- *x* **of** *y* **Downloaded**. Some but not all firmware updates in the update package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
- **Not Downloaded**. The entire update package or the individual firmware update is available but not stored in the repository.

When you install XClarity Administrator or update to a new release, it is a best practice to download the latest repository pack to ensure you have the latest firmware updates. Then, you can schedule a recurring job to refresh the catalog to find individual updates that were posted on the web since the last repository pack and then electronically download those updates, one at a time.

XClarity Administrator must be connected to the Internet to refresh the catalog and download firmware-update. If it is not connected to the Internet, you can manually download the files to a workstation that has network access to the XClarity Administrator host using a web browser and then import the files into the firmware-updates repository.



When you manually import firmware updates into XClarity Administrator, you must include the following required files: payload (image and MIB), metadata XML, change history, and readme. For example:
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Note: The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers.

A message is displayed on the page when the repository is more than 50% full. Another message is displayed on the page when the repository is more than 85% full. To reduce the space used in the repository, you can remove unused images files and policies. You can remove unused firmware-compliance policies and associated firmware packages by clicking **Provisioning → Compliance policies**, selecting one or more policies to delete, and then clicking **Actions → Delete any policy and firmware packages**.

The following table summarizes the differences between acquiring firmware-update repository packs, UXSPs, and individual firmware-update packages.

Update package	UI page for downloading and importing files	Webpage to download files manually	Is the firmware updates repository refreshed?	Is the firmware-compliance policy refreshed automatically?
Firmware-update repository packs	Update Management Server page **Note:** You must import and then apply the repository pack.	XClarity Administrator download webpage	Yes	Yes
UpdateXpress System Packs	Firmware Updates: Repository page, **UpdateXpress System Packs (UXSPs)** tab	Lenovo XClarity Essentials UpdateXpress webpage	Yes	Yes
Firmware-updates	Firmware Updates: Repository page, **Individual Updates** tab	Lenovo Data Center Support website **Notes:** Use the Fix Central website for the following devices: • Flex System x220 Type 2585, 7906 • Flex System x222 Compute Nod Type 2589, 7916 • Flex System x240 Type 7863, 8737, 8738, 8956 • Flex System x280 / x480 / x880 X6 Type 4259, 7903 • Flex System x440 Type 2584, 7917	Yes	No

Procedure

To download one or more firmware updates, complete the following steps.

- To import one or more *firmware-update repository packs*:
  1. From the XClarity Administrator menu bar, click **Administration → Update Management Server** to display the Management Server Update page.
  2. Download the latest repository packs:
     - If XClarity Administrator is connected to the Internet:
       a. Retrieve information about the latest updates by clicking the **Refresh Catalog → Refresh All Managed – Latest only**). New management-server updates and firmware-update repository packs are listed in the table on the “Management Server Update” page.

          Refreshing the repository might take several minutes to complete.

          Note: Refreshing the repository does not automatically download payload files. Only the XML and readme files are downloaded.

       b. Select the firmware-update repository packs that you want to download.

          Tip: Ensure that the packages that you select have “Supplemental Pack” in the **Type** column.

c. Click the **Download Selected** icon (). When the download is complete, the **Download Status** for that software update changes to “Downloaded”.

– If XClarity Administrator is not connected to the Internet:

a. Download the firmware-update repository packs from the XClarity Administrator download webpage to a workstation that has a network connection to the XClarity Administrator host.

b. From the Management Server Update page, click the **Import** icon ().

c. Click **Select Files**, and browse to the location of the firmware-update repository packs on the workstation.

d. Select all package files, and then, click **Open**.

You must import the metadata file (.xml) as well as the image or payload file (.zip, .bin, .uxz, or .tgz), change history file (.chg), and readme file (.txt) for the update. Any files that are selected but are not specified in the .xml file are discarded. If you do not include the .xml file, the update is not imported.

e. Click **Import**.

When the import is complete, the firmware-update repository packs are listed in the table on the Management Server Update page, and the **Download Status** for each update is “Downloaded”.

3. Select the firmware-update repository packs that you want to install to the firmware-updates repository.

Note: Ensure that **Download Status** is “Downloaded” and that the **Type** is “Patch.”

4. Click the **Perform Update** icon () add the firmware-update packages to the repository.
5. Wait a few minutes for the update to complete and XClarity Administrator to be restarted.
6. Determine if the update is complete by refreshing the web browser.

When completed, the Management Server Update page is displayed, and the **Applied Status** column changes to “Applied.”

7. Clear the web browser cache.

- To download one or more *UXSPs*.

1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository** to display the Firmware Updates Repository page.
2. Click the **UpdateXpress System Packs (UXSPs)** tab.
3. Download the latest UXSPs:

– If XClarity Administrator is connected to the Internet:

To refresh the catalog and download the latest UXSPs for all managed devices, click **All Actions → Refresh and download the latest for all managed devices**.

To refresh the catalog and download the latest UXSPs for only selected devices:

a. Expand the device to display the list of available UXSPs.

b. Select one or more UXSPs that you want to download.

c. Click **All Actions → Refresh and download the latest for selected devices**.

When the download is complete, the **Download Status** for the selected UXSPs changes to “Downloaded.”

– If XClarity Administrator is not connected to the Internet:

a. Download the UXSPs from the Lenovo XClarity Essentials UpdateXpress webpage to a workstation that has a network connection to the XClarity Administrator host

b. From XClarity Administrator, click the **Import** icon ( ).

c. Click **Select Files**, and browse to the location of the UXSPs on the workstation.

d. Select all package files, and then, click **Open**.

You must import the metadata file (.xml) as well as the image or payload file (.zip, .bin, .uxz, or .tgz), change history file (.chg), and readme file (.txt) for the update. Any files that are selected but are not specified in the .xml file are discarded. If you do not include the .xml file, the update is not imported.

e. Click **Import**.

When the import is complete, the firmware-update repository packs are listed in the table on the Management Server Update page, and the Download Status for each update is ""“Downloaded.”

- To download one or more individual *firmware-update packages*.
  1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository** to display the Firmware Updates Repository page.
  2. If downloading firmware for ThinkSystem DM series storage devices, select the country where the storage devices are located.
  3. Click the **Individual Updates** tab.
  4. Download the latest individual firmware-updates:
     - If XClarity Administrator is connected to the Internet:

       To refresh the catalog and download the latest firmware for all managed devices, click **All Actions → Refresh and download the latest for all managed devices**.

       To refresh the catalog and download the latest firmware for only selected devices:

       a. Expand the device to display the list of available firmware updates.

       b. Select one or more firmware updates that you want to download.

       Tip: An update package can consist of multiple firmware updates. When you download a firmware update, you can choose to download the entire update package or only specific updates. You can also choose to download multiple packages at one time.

       c. Click **All Actions → Refresh and download the latest for selected devices**.

       When the download is complete, the **Download Status** for the selected firmware updates changes to “Downloaded”.

     - If XClarity Administrator is not connected to the Internet:

       a. Download the firmware-update packages from the Lenovo Data Center Support website to a workstation that has network connection to the XClarity Administrator host.

       For the following servers, download firmware updates for the SLES 11 operating system from the Fix Central website:

       - Flex System x220 Type 2585, 7906
       - Flex System x222 Compute Nod Type 2589, 7916
       - Flex System x240 Type 7863, 8737, 8738, 8956
       - Flex System x280 / x480 / x880 X6 Type 4259, 7903
       - Flex System x440 Type 2584, 7917

For all other servers, download firmware updates for the RHEL 6 operating system. from the Lenovo XClarity Support website.

b. From XClarity Administrator, click the **Import** icon ( ).

c. Click **Select Files**, and browse to the location of the firmware updates on the workstation.

d. Select all package files, and then click **Open**.

   You must import the metadata file (.xml) as well as the image or payload file (.zip, .bin, .uxz, or .tgz), change history file (.chg), and readme file (.txt) for the update. Any files that are selected but are not specified in the .xml file are discarded.

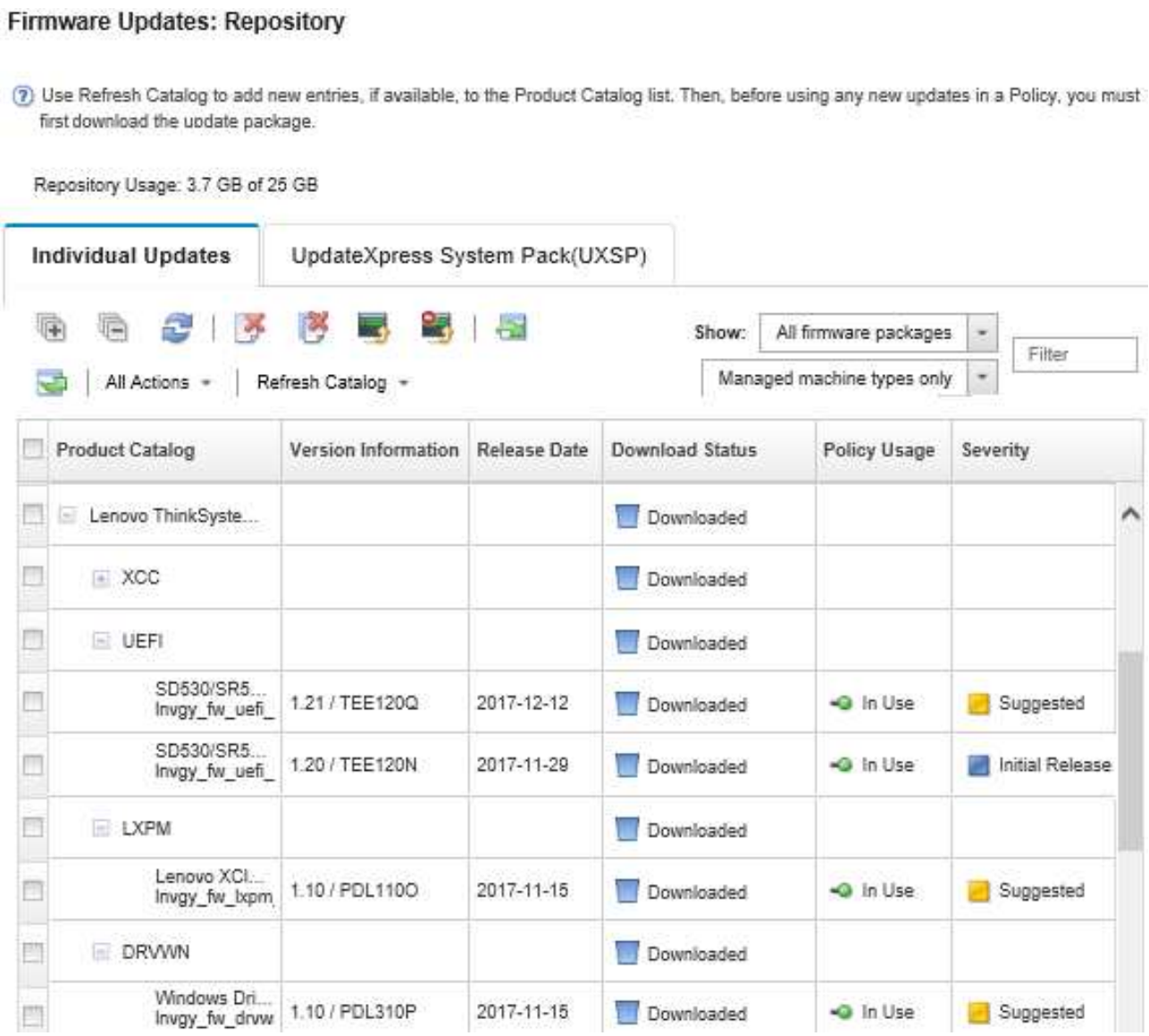
   Attention:

   - Only import these required files. Do not import other files that might be found on the firmware download websites.
   - If you do not include the XML file in the update package, the update is not imported.
   - If you do not include all required files that are associated with the update, the repository shows that the update is not downloaded, which means that it is partially imported. You can then import the missing files by selecting and importing them.
   - The core firmware updates (such as management controller, UEFI, and pDSA) are operating-system independent. Firmware-update packages for the RHEL 6 or SLES 11 operating systems are used to update compute nodes and rack servers. For more information about which firmware-update packages to use for your managed servers, see Downloading firmware updates.

e. Click **Import**.

Refreshing the catalog and downloading the firmware updates might take a several minutes. When the updates have been downloaded and stored in the repository, the row in the product catalog is highlighted, and the **Download Status** column is changed to “Downloaded.”

Note: The machine type for some switches might show up as a hexadecimal number.



After you finish

You can configure the maximum size of the updates repository (including firmware, OS device drivers, and management server updates) from the Firmware Repository page by clicking **All Actions → Global Settings**. The minimum size is 50 GB. The maximum size is dependent on the amount of disk space on the local system.

Exporting and importing firmware updates

You can export individual firmware updates and UpdateXpress System Packs (UXSPs) that exist in the repository to the local system.

About this task

Only firmware updates that exist in the repository are exported. Ensure that the download-status for the selected firmware updates is “Downloaded.”

All of the files that are associated with the firmware update are exported, including the update image or payload file (.zip, .bin, .uxz, or .tgz), metadata file (.xml), change history file (.chg), and readme file (.txt).

Attention: Do not change the name of the firmware update files.

Procedure

- To export firmware updates:
  1. Click the **Individual Updates** tab or **UpdateXpress System Packs (UXSPs)** tab.
  2. Select one or more firmware updates.
  3. Click the **Export** icon ( ).
- To import firmware updates:

  You can import files that you manually exported from Lenovo XClarity Administrator and files that you manually downloaded from the web. For more information, see Downloading firmware updates.

Deleting firmware updates

You can delete firmware updates and UpdateXpress System Packs (UXSPs) from the firmware-updates repository.

Before you begin

Ensure that all running or scheduled update jobs that use a firmware-compliance policy that contains the firmware updates to be deleted are completed or canceled (see Monitoring jobs).

Ensure that the update is not being used in a firmware-compliance policy before deleting the update. You cannot delete firmware-update packages that are currently used in one or more firmware-compliance policies.

Deleting a UXSP also deletes the firmware-compliance policy that was automatically created for that UXSP.

Note: Take care when deleting firmware updates and UXSPs if the firmware-updates repository is a remote share that is used by multiple XClarity Administrator instances.

Procedure

To delete one or more firmware updates from the repository, complete the following steps.

Step 1. Unassign all firmware-compliance policies that contain the firmware updates to be deleted from all managed devices.

   a. From the XClarity Administrator menu bar, click **Provisioning → Apply/Activate**. The Firmware Updates Apply/Activate page is displayed.

   b. Select “No assignment” or select another firmware-compliance policy in the **Assigned Policy** column for the managed devices that use the firmware-compliance policy.

Step 2. Delete all user-defined firmware-compliance policies that contain the firmware updates to be deleted, or edited the firmware-compliance policies to remove the firmware updates to be deleted.

   a. From the XClarity Administrator menu bar, click **Provisioning → Compliance Policies**. The Firmware Updates Compliance Policies page is displayed.

   b. Select the firmware-compliance policy, and then select the **Delete** icon ( ) to delete the policy, or click the **Edit** icon ( ) to remove the firmware updates from the policy.

Step 3. Delete the firmware updates.

- **Individual firmware updates**
  1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.
  2. Click the **Individual Updates** tab.
  3. Select one or more firmware updates to be deleted.
  4. Click the **Delete only images** icon (to delete only the image or payload file (.zip, .bin, .uxz, or .tgz). Information about the update, remains so that you can easily download the update again. Or click the **Delete full update packages** icon (to delete the full update packages, including the image or payload file, change history file (.chg), readme file (.txt), and metadata file (.xml).

  When you delete a firmware update, the payload files are removed; however, the XML file, which contains information about the update, remains so that you can easily download the update again, if needed, and the **Download Status** changes to "Not downloaded."
- **UXSPs**
  1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Repository**. The Firmware Updates Repository page is displayed.
  2. Click the **UpdateXpress System Pack (UXSP)** tab.
  3. Select one or more UXSPs to be deleted.
  4. Click the **Delete UXSP and associated policy** icon ( ) to delete the full UXSPs, including the image or payload file, change history file (.chg), readme file (.txt), and metadata file (.xml),and all associated firmware-compliance policies.

  If selected UXSPs are associated with policies that are in use (assigned to devices), the Delete UXSP, Policy, and Update Packages dialog is displayed. Choose whether to delete the assigned policies in addition to the UXSP and unassigned policies, and click **OK**.

Creating and assigning firmware-compliance policies

Firmware-compliance policies ensure that the firmware on certain managed devices is at the current or specific level by flagging the devices that need attention. Each firmware-compliance policy identifies which devices are monitored and which firmware level must be installed to keep the devices in compliance. You can set compliance at the device or firmware component level. XClarity Administrator then uses these policies to check the status of managed devices and to identify devices that are out of compliance.

Before you begin

When you create a firmware-compliance policy, you select the target update version to be applied to the devices that will be assigned to the policy. Ensure that firmware updates for the target version are in the updates repository before you create the policy (see Downloading firmware updates).

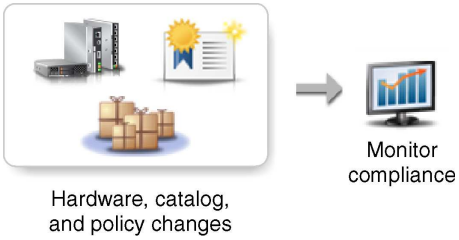
If a device type is not listed in the firmware-updates repository, you must first manage a device of that type and then download or import the complete set of firmware updates before creating compliance policies for devices of that type.

About this task

When you create a firmware-compliance policy, you can choose to have XClarity Administrator flag a device when:
- The firmware on the device is down level
- The firmware on the device does not exactly match the compliance target version

XClarity Administrator comes with a predefined firmware-compliance policy named **Latest firmware in repository**. When new firmware is downloaded or imported into the repository, this policy is updated to include latest available versions of firmware in the repository.

After a firmware-compliance policy is assigned to a device, XClarity Administrator checks the compliance status of each device when the device inventory changes or firmware-updates repository changes. When the firmware on a device is not compliant with the assigned policy, XClarity Administrator identifies that device as not compliant on the Firmware Updates: Apply / Activate page, based on the rule that you specified in the firmware-compliance policy



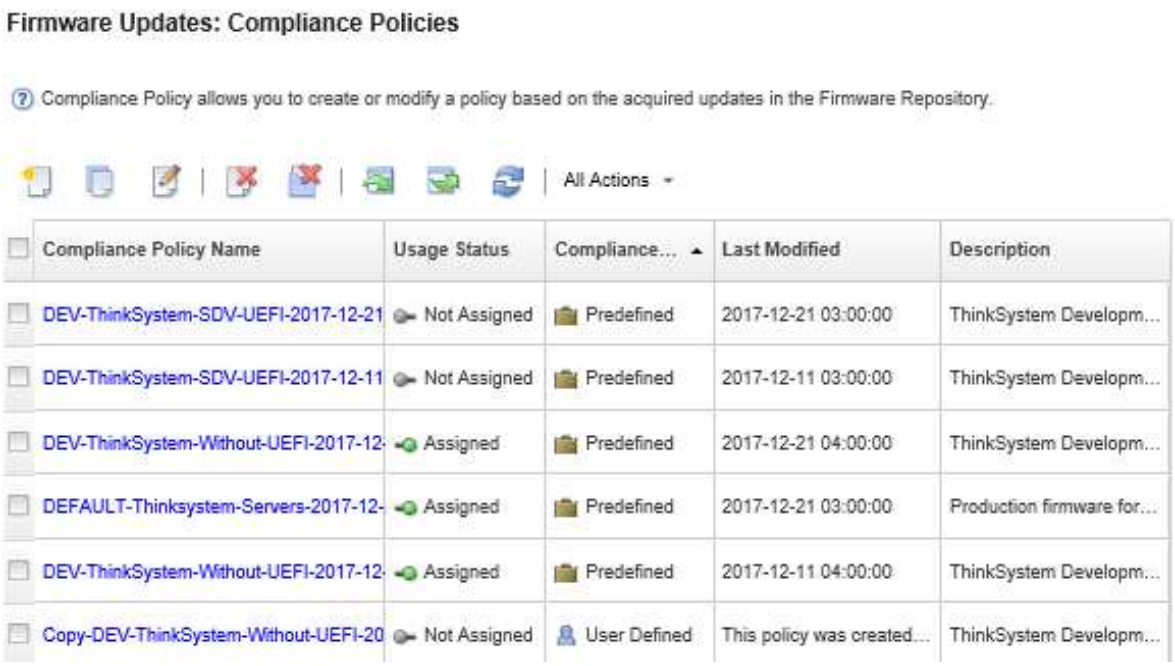
For example, you can create a firmware-compliance policy that defines the baseline level for firmware that is installed in all ThinkSystem SR850 devices and then assign that firmware-compliance policy to all managed ThinkSystem SR850 devices. When the firmware-updates repository is refreshed and a new firmware update is added, those compute nodes might become out of compliance. When that happens, XClarity Administrator updates the Firmware Updates: Apply / Activate page to show that the devices are not compliant and generates an alert.

Note: You can choose to show or hide alerts for devices that do not meet the requirements of their assigned firmware-compliance policies (see Configuring global firmware-update settings). Alerts are hidden by default.

Procedure

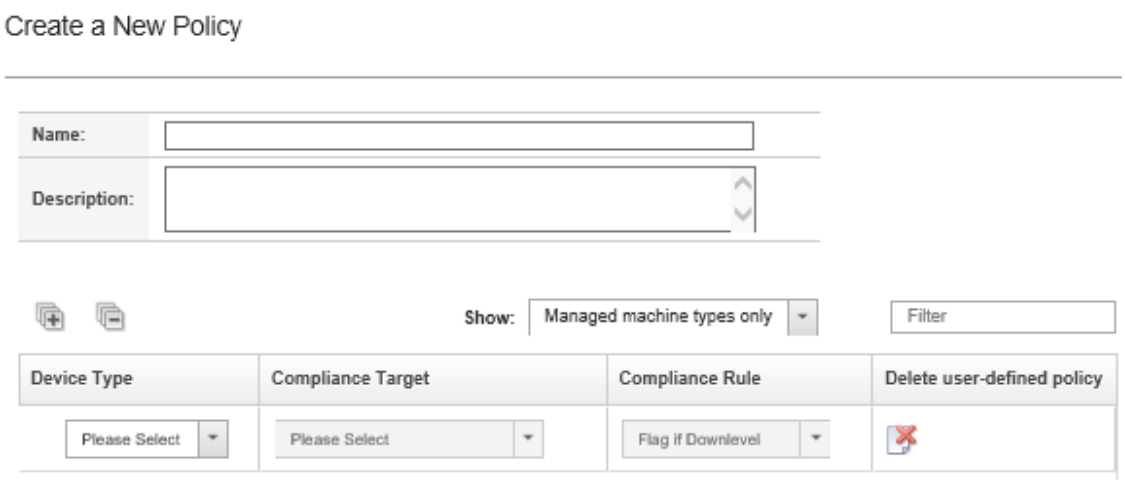
To create and assign a firmware-compliance policy, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Compliance Policies**. The Compliance Policy page is displayed with a list of all existing firmware-compliance policies.



Step 2. Create a firmware -compliance policy.

1. Click the **Create** icon ( ) to display the Create a New Policy dialog.



2. Fill in the name and description for the firmware-compliance policy.
3. Fill in the table based on the following criteria for each device.
   - **Device Type**. Choose a type of device or component for which this policy is to apply.

     Tip: If you choose a server, the compliance level is done at the UXSP level. However, you can also expand the server to specify specific firmware levels for each component, such as the baseboard management controller or UEFI.
   - **Compliance Target**. Specify the compliance target for the applicable devices and subcomponents.

     For servers, you can choose one of the following values.

     – **Default**. Changes the compliance target for each subcomponent to the default value (such as the latest set of firmware in the repository for that device).

– **Do not update**. Changes the compliance target for each subcomponent to “Do not update.”

For devices without subcomponents (such as CMMs, switches, or storage devices) or for subcomponents in a server, you can choose one of the following values.

– *<firmware_level>*. Specifies the baseline firmware level.

– **Do not update**. Specifies that the firmware is not to be updated. Note that firmware on the backup management controller is not updated by default.

Note: When you change default values for any subcomponent in a server, the compliance target for that server changes to **Custom**.

- **Compliance Rule**. Specify when a device is flagged as not compliant in the **Installed Version** column on the Firmware Updates: Apply/Activate.
  – **Flag if Downlevel**. If the firmware level that is installed on a device is earlier than the level that is specified in the firmware-compliance policy, the device is flagged as not compliant. For example, if you replace a network adapter in a compute node, and the firmware on that network adapter is earlier than the level identified in the firmware-compliance policy, the compute node is flagged as not compliance.
  – **Flag if Not Exact Match**. If the firmware level that is installed on a device is not an exact match with the firmware-compliance policy, the device is flagged as not compliant. For example, if you replace a network adapter in a compute node, and the firmware on that network adapter is different than the level identified in the firmware-compliance policy, then the compute node is flagged as not compliance.
  – **No Flag**. Devices that are out of compliance are not flagged.

4. **Optional:** Expand the system type to display each update in the package, and select the firmware level to be used as the compliance target, or select “Do not update” to prevent firmware from being updated on that device.
5. Click **Create**.

   The firmware-compliance policy is listed in the table on the Firmware Updates: Compliance Policy page. The table shows the usage status, origin of the policy (whether user-defined or predefined), and the last modification date.

Step 3. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed with a list of managed devices.

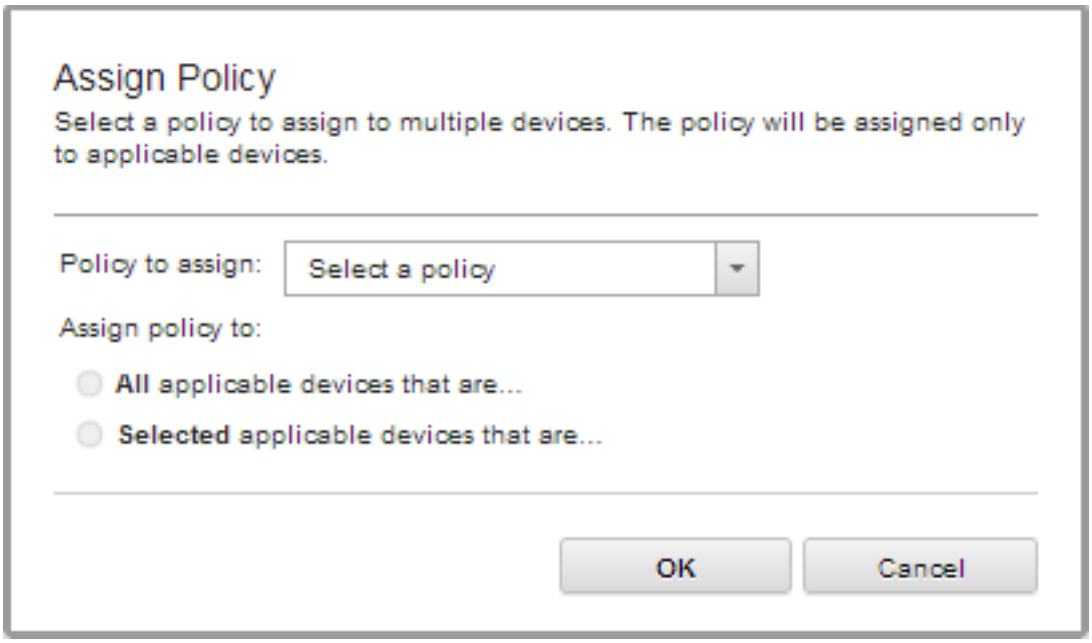
Step 4. Assign the firmware-compliance policy to devices.

- **To a single device**

  For each device, select a policy from the drop-down menu in the **Assigned Compliance Policy** column.

  You can select from a list of firmware-compliance policies that are applicable to each device. If a policy is not currently assigned to the device, the assigned policy is set to **No assignment**. If no policies are applicable to the device, the assigned policy is set to **No applicable policies**.

- **To multiple devices**
  1. **Optional:** Select one or more devices to which you want to assign a firmware-compliance policy.
  2. Click the **Assign policy** icon ( ) to display the Assign Policy dialog.



3. Select a firmware-compliance policy from the **Policy to assign** drop-down menu.

   You can select from a list of firmware-compliance policies that are applicable to all selected devices. If devices were not selected before opening the dialog, all policies are listed.

   To unassign a policy, select **No assignment**.

4. Select one of the following scopes for the policy assignment.
   - **All applicable devices that are…**
   - **Only selected applicable devices that are …**

5. Select one or more device criteria.
   - **Without an assigned policy**
   - **Non-compliant (overwrite current assigned policy)**
   - **Compliant (overwrite current assigned policy)**
   - **Not monitored (overwrite current assigned policy)**
   - **Other (overwrite current assigned policy)**. This applies to devices in other states, such as the Pending state, with missing data, or not supported for updates. Hover over the help icon ( ) to see a list of applicable devices.

   Note: Not monitored and **Other** criteria are listed only when there are devices in those states.

6. Click **OK**.

   The policy that is listed in the **Assigned Policy** column on the Firmware Updates: Repository page changes to the name of the selected firmware-compliance policy.

After you finish

After you create a firmware-compliance policy, you perform the following actions on a selected firmware-compliance policy:

- View policy details, including a list of assigned devices, by clicking on the policy name in the table.
- Create a duplicate of a selected policy by clicking the **Copy** icon ( ).

- Rename or modify a a selected policy by clicking the **Edit** icon ( ).You cannot edit a predefined firmware-compliance policy or a policy that is assigned to a managed device.

  If you modify an assigned policy in such a way that causes it to no longer apply to certain assigned devices, the policy is automatically unassigned from those devices.

  You cannot rename or modify the predefined **Latest Firmware** policy.

- Delete a selected firmware-compliance policy by clicking the **Delete policy** icon ( ) or delete the selected firmware-compliance policy and all associated firmware updates that are used only by that policy by clicking the **Delete any policy and firmware packages** icon ( ).You can choose to delete the policy even if it is assigned to a device.

  When you delete a policy that is assigned to a device, the policy is unassigned before it is deleted.

  You cannot delete the predefined **Latest Firmware** policy; however, you can disable the policy by clicking the **Global Settings** icon ( ), and then selecting **Disable Latest Firmware Policy**. When this option is selected, the Latest firmware policy is unassigned from managed devices, and the policy is no longer updated to include the latest available versions of firmware in the repository.

- Export a selected policy to a local system by selecting the policies and clicking the **Export** icon ( ). You can then import the policies to another XClarity Administrator instance by clicking the **Import** icon ( ).

After you create a firmware-compliance policy, you can assign the policy to a specific device (see Creating and assigning firmware-compliance policies) and apply and activate updates for that device (see Applying and activating firmware updates).

Identifying devices that are not compliant

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

Procedure

To determine whether the firmware on a device is compliant with its assigned firmware-compliance policy, click **Provisioning → Firmware Updates: Apply/Activate** from the Lenovo XClarity Administrator menu bar to display the Firmware Update: Compliance Policy page, and check the **Installed Versions** column for that device.

The **Installed Versions** column contains one of the following values:

- **Firmware version**. The firmware version that is installed on the device is compliant with the assigned policy.
- **Compliant**. The firmware that is installed on the device is compliant with the assigned policy.
- **Not Compliant**. The firmware that is installed on the device is not compliant with the assigned policy.
- **No Compliance Policy Set**. A firmware-compliance policy is not assigned to the device.

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

Configuring global firmware-update settings

Global settings serve as defaults settings when firmware updates are applied.

About this task

From the Global Settings page, you can configure the following settings:
- Enhanced support for down-level devices
- Alerts for devices that are not compliant with their assigned policies
- Automatic assignment of a firmware-compliance policy to a device that has no assigned policy
- Non-compliance status for devices with a firmware component that has no associated target in the firmware-compliance policy

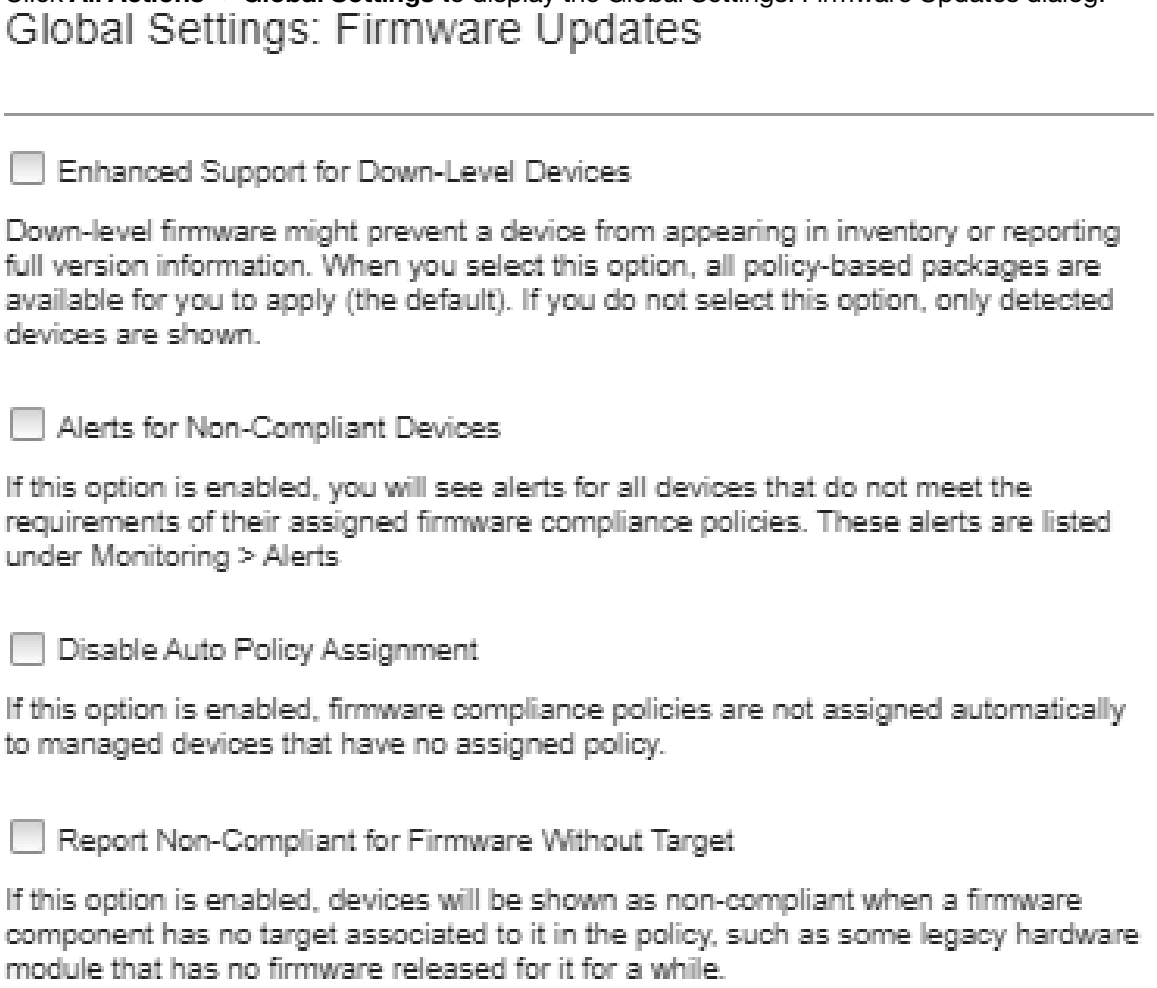
Procedure

To configure the global settings to be used for all servers, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.

Step 2. Click the **Update with Policy** or **Update without Policy** tab.

Step 3. Click **All Actions → Global Settings** to display the Global Settings: Firmware Updates dialog.



Step 4. Optionally select the following options.

- Select **Enhanced Support for Down-Level Devices** to display inventory and full-version information for all devices, even if the firmware is down-level or if the device is missing from the inventory.
- Select **Alerts for Non-Compliance Devices** to display alerts on the Alerts page for devices that do not meet the requirements of their assigned firmware-compliance policies. Alerts are hidden on the Alerts page by default. For more information, see Viewing active alerts.

- Select **Disable auto policy assignment** to disable automatic assignment of a firmware-compliance policy to a device that has no assigned policy. If this option is not selected, firmware compliance policies are assigned to devices without a policy when XClarity Administrator is restarted or when you manage a new device.
- Select **Report Non-Compliance for Firmware Without Target** to flag devices as non-compliant when a firmware component has no associated target in the firmware-compliance policy. If this option is not selected, devices without targets are flagged as compliant.

Step 5. Click **OK** to close the dialog.

Applying and activating firmware updates

Lenovo XClarity Administrator does not automatically apply firmware updates to managed devices. You can choose to apply firmware updates with or without compliance policies.

Before you begin

When using compliance policies, you can schedule updates on multiple devices at the same time. XClarity Administrator updates devices in the correct sequence automatically. The CMM is updated first, followed by switches, servers, and then storage devices.

Only downloaded firmware updates can be applied.

When you perform a firmware update, XClarity Administrator starts one or more jobs to perform the update.

While the firmware update is in progress, the target device is locked. You cannot initiate other management tasks on the target device until the update process is complete.

After a firmware update is applied to a device, one or more restarts might be required to fully activate the firmware update. You can choose whether to restart the device immediately, delay the activation, or prioritize activation. If you choose to restart immediately, XClarity Administrator minimized the number of restarts that are required. If you choose to delay activation, the updates are activated the next time the device is restarted. If you choose prioritized activation, the updates are immediately activated on the baseboard management controller, and all other firmware updates are activated the next time the device is restarted.

You can update selected firmware on a maximum of 50 devices at one time. If you choose to update selected firmware on more than 50 devices, the remaining devices are queued. A queued device is taken off the “selected-firmware update” queue when either the activation completes on an updated device or an updated device is placed in the Pending Maintenance Mode state (if a restart is required on that device). When a device in the Pending Maintenance Mode state is restarted, the device boots into Maintenance Mode and continues the update process, even if the maximum number of firmware updates is already in progress.

You can update bundled-firmware on a maximum of 10 devices at one time. If you choose to update bundled firmware on more than 10 devices, the remaining devices are queued. A queued device is taken off the “bundled-firmware update” queue when the activation completes on a device on which a bundled-firmware update was performed.

Attention: For Red Hat® Enterprise Linux (RHEL) v7 and later, restarting the operating system from a graphical mode suspends the server by default. Before you can perform the **Restart Normally** or **Restart Immediately** actions from XClarity Administrator, you must manually configure the operating system to change the behavior of the power button to power off. For instructions, see the Red Hat Data Migration and Administration Guide: Changing behavior when pressing the power button in graphical target mode.

Note: The XClarity Administrator automatically enables the LAN-over-USB interface.

Applying bundled firmware updates using compliance policies

After Lenovo XClarity Administrator identifies a managed device as not compliant, you can manually apply firmware updates to *all* components in selected ThinkSystem SR635 and SR655 servers that are not compliant with the assigned firmware-compliance policy using a bundled image that contain the applicable firmware update packages. The *bundled image* is created during the update process by collecting all firmware-update packages from the compliance policy.

Before you begin

- Read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).
- Initially, devices that are not supported for updates are hidden from the view. Devices that are not supported cannot be selected for updates.
- By default, all detected components are listed as available for applying updates; however, down-level firmware might prevent a component from appearing in inventory or reporting full-version information. To list all policy-based packages that are available for you to apply updates, click **All Actions → Global Settings**, and selecting **Enhanced Support for Down-Level Devices**. When this option is selected, "Other Available Software" is listed in the Installed Version column for undetected devices. For more information, see Configuring global firmware-update settings.

  Notes:

  – The global settings cannot be changed when updates to managed devices are in progress.

  – It takes a few minutes to generate the additional options. After a few moments, you might need to click the **Refresh** icon ( ) to refresh the table.
- Ensure that no jobs are currently running on the target server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.
- Applying bundled firmware updates is supported only for ThinkSystem SR635 and SR655 servers.
- Applying bundled firmware updates is supported only for IPv4 address. IPv6 addresses are not supported.
- Ensure that each target device was booted to the OS at least once to retrieve the full inventory information.
- Baseboard management controller firmware v2.94 or later is required to use the bundled-update function.
- Only firmware updates from repository packs or individual firmware updates are used. UpdateXpress System Packs (UXSPs) are not supported.
- Only downloaded firmware updates are applied. Refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.
- Compliance check is supported only for the baseboard management controller and UEFI in ThinkSystem SR635 and SR655 servers; however, XClarity Administrator attempts to apply firmware updates to all available hardware components.
- Updates are applied according to the assigned firmware-compliance policy. You cannot choose to update a subset of components.
- XClarity Administrator v3.2 or later is required to apply firmware updates for Lenovo XClarity Provisioning Manager (LXPM), LXPM windows drivers, or LXPM Linux drivers to ThinkSystem SR635 and SR655 servers.
- The baseboard management controller and UEFI updates are skipped if the currently installed version is higher than the assigned compliance policy.
- Firmware-compliance policies must be created and assigned to the devices on which you intend to apply firmware updates. For more information, see Creating and assigning firmware-compliance policies.

- The selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

Attention: Selected devices are powered off before starting the update process. Ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.

About this task

The bundled-update process first updates the baseboard management controller and UEFI out of band. When these updates are complete, the process creates a bundled image of remaining firmware in the compliance policy based on the machine type. Then, the process mounts the image to the selected device and restarts the device to boot the image. The image automatically runs to perform the remaining updates.

You can update bundled-firmware on a maximum of 10 devices at one time. If you choose to update bundled firmware on more than 10 devices, the remaining devices are queued. A queued device is taken off the "bundled-firmware update" queue when the activation completes on a device on which a bundled-firmware update was performed.

If an error occurs while updating a component in the device, the firmware-update process does not update the firmware for that specific component; however, the firmware-update process continues to update the other components in the device and continues to update all other devices in the current firmware-update job.

Procedure

To apply firmware updates in the form of a bundled image on managed devices, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.

Step 2. Click the **Update with Policy** tab.

Step 3. Select one or more devices and components to which firmware updates are to be applied.

You can sort the table columns to make it easier to find specific devices. In addition, you can filter the list of displayed devices by selecting an option in the **Show** menu to list only devices in a specific chassis, rack, or group, by entering text (such as a name or IP address) in the **Filter** field, or by clicking the following icons to list only devices with a specific status.

- **Hide compliant devices** icon ( )
- **Hide non-compliant devices status** icon ( )
- **Hide devices without an assigned compliance policy** icon ( )
- **Hide devices not being monitored** icon ( )
- **Hide devices with firmware pending activation** icon ( )
- **Hide devices with compliance errors** icon ( )
- **Hide devices not supported for updates** icon ( )
- **Hide devices undergoing firmware updates** icon ( )
- **Hide devices with nonstageable firmware** icon ( )

The **Groups** column indicates the groups of which each device is a member. You can hover over the **Groups** column to get a complete list of groups, by group type

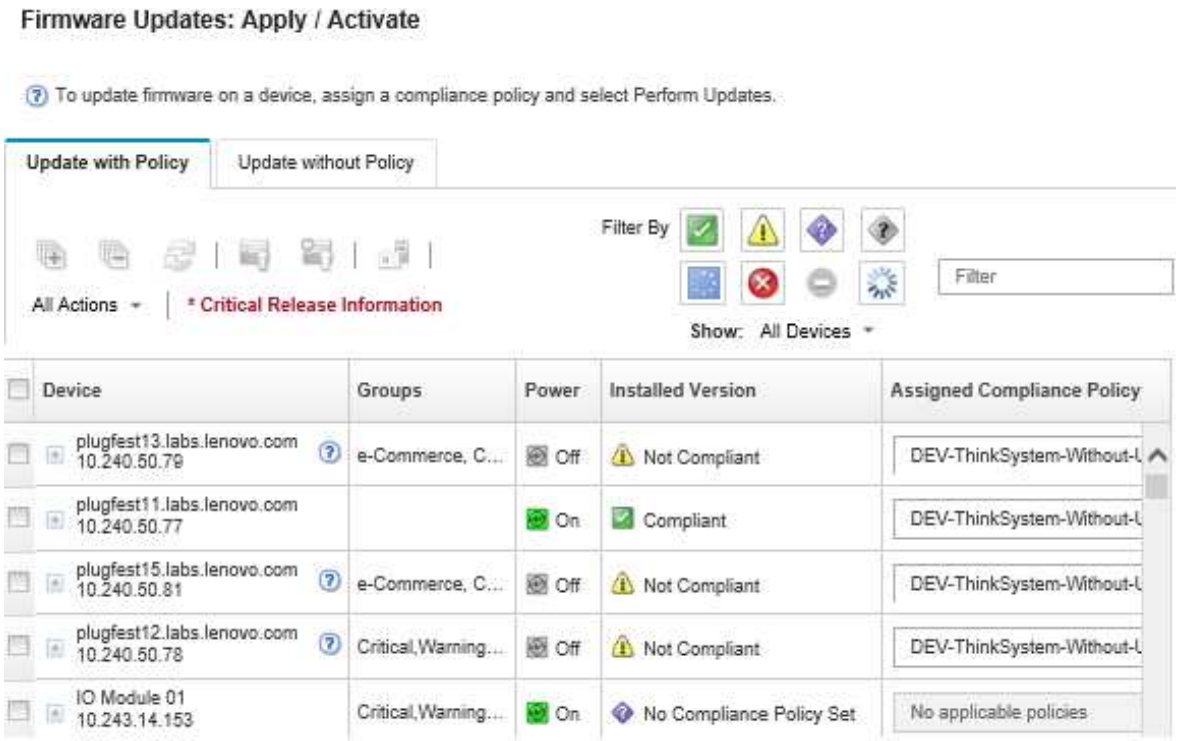
The **Installed Version** column indicates the installed firmware version, compliance status, or device status.

The compliance status can be one of the following:

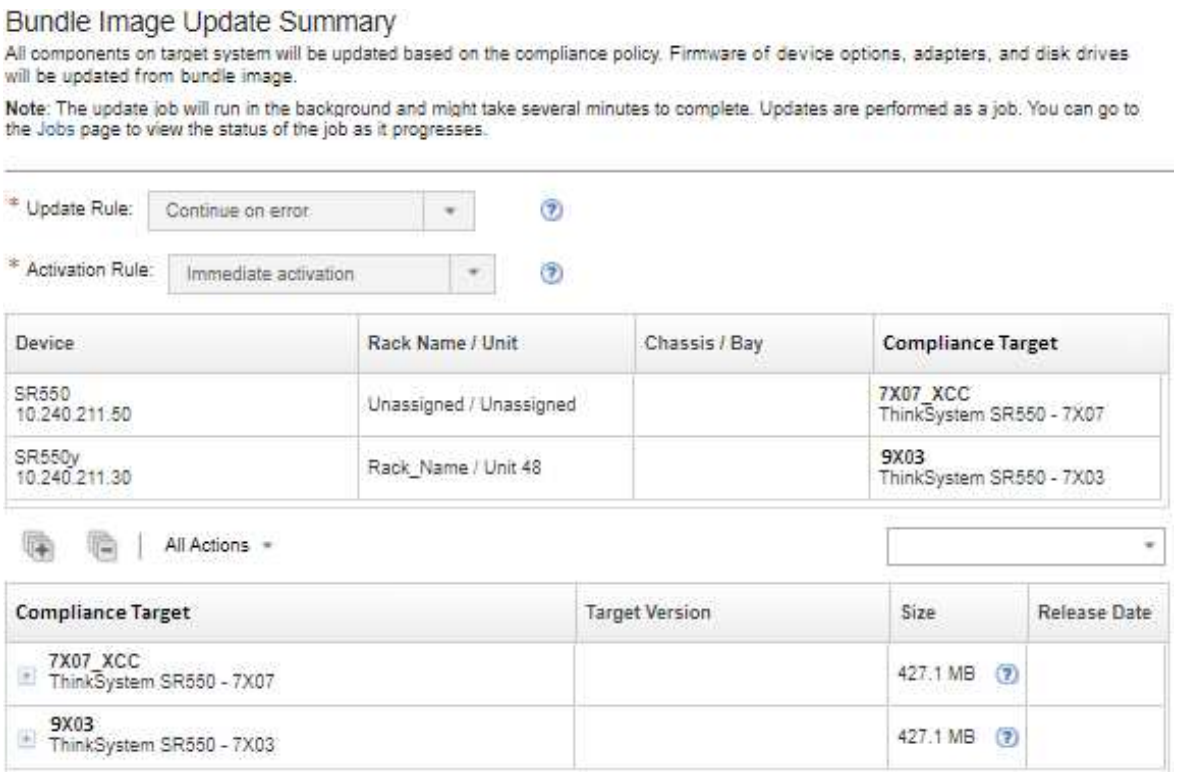
- **Compliant**
- **Compliance Error**
- **Not Compliant**
- **No Compliance Policy Set**
- **Not Monitored**

The device status can be one of the following:

- **Updates Not Supported**
- **Update in Progress**



Step 4. Click the **Perform Update from Bundle Image** icon ( ). The Bundle Image Update Summary dialog is displayed. This dialog lists the selected devices and the firmware updates that are included in the bundled image.



Step 5. Click **Perform Update from Bundle Image** to update immediately, or click **Schedule** to schedule this update to run at a later time.

After you finish

When applying a firmware update, if the server fails to enter maintenance mode, attempt to apply the update again.

If updates were not completed successfully, see Firmware update and repository issues in the XClarity Administrator online documentation for troubleshooting and corrective actions.

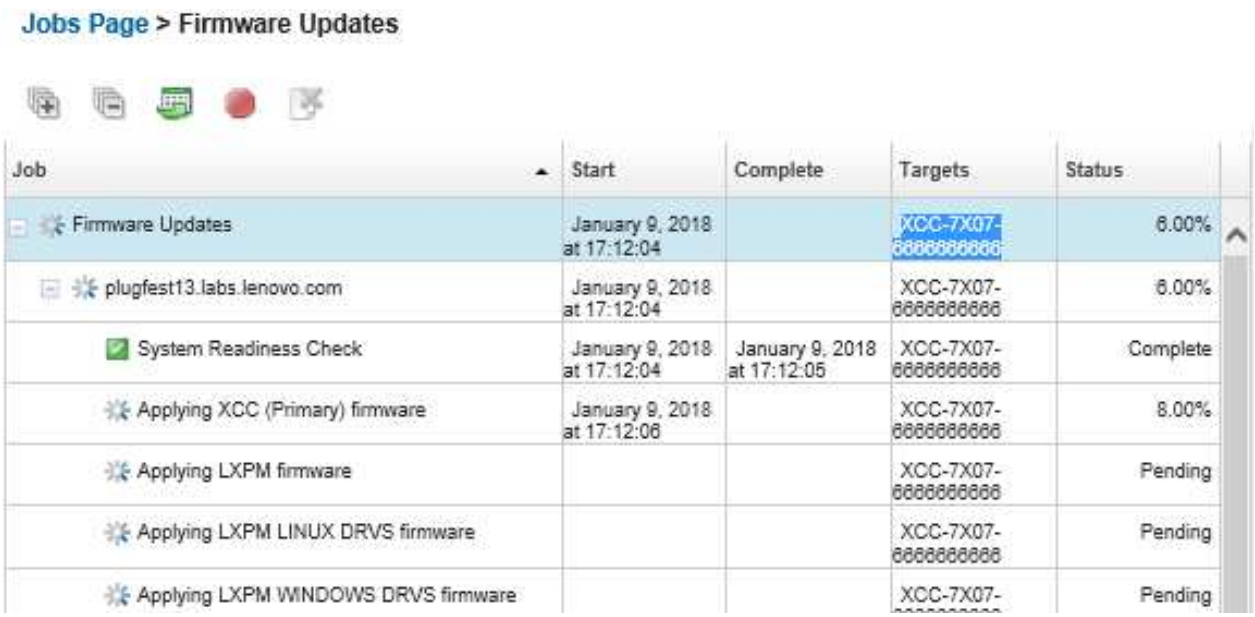
From the Firmware Updates: Apply/Activate page, you can perform the following actions.

- Export firmware and compliance information for each managed device by clicking **All Actions → Export View as CSV**.

  Note: The CSV file contains only filtered information in the current view. Information that is filtered out of the view and information in hidden columns are not included.
- Cancel an update that is being applied to a device by selecting the device and clicking the **Cancel Update** icon ( ).

  Note: You can cancel firmware updates that are in the queue to start. After the update process starts, the firmware update is cancelable only when the update process is performing a task other than applying the update, such as changing to maintenance mode or restarting the device.
- View the status of the firmware update directly from the Apply / Activate page in the **Status** column.
- Monitor the status of the update process from the jobs log. From the Lenovo XClarity Administrator menu, click **Monitoring → Jobs**.

  For more information about the jobs log, see Monitoring jobs .



When the firmware-update jobs are complete, you can verify that the devices are compliant by clicking **Provisioning → Firmware Updates: Apply/Activate** to go back to the Firmware Updates: Apply/Activate page, and then clicking the **Refresh** icon ( ). The current firmware version that is active on each device is listed in the **Installed Version** column.

Applying selected firmware updates using compliance policies

After Lenovo XClarity Administrator identifies a device as not compliant, you can manually apply and activate the firmware updates on these managed devices. You can choose to apply and activate all firmware updates that apply to a firmware-compliance policy or only specific firmware updates in a policy. Only downloaded firmware updates are applied.

Learn more:

- XClarity Administrator: Boosting Efficiency when Updating Firmware
- Lenovo ThinkSystem Firmware and Driver Update Best Practices
- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Firmware updates
- XClarity Administrator: Provisioning firmware security updates

Before you begin

- Read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).
- Initially, devices that are not supported for updates are hidden from the view. Devices that are not supported cannot be selected for updates.
- By default, all detected components are listed as available for applying updates; however, down-level firmware might prevent a component from appearing in inventory or reporting full-version information. To list all policy-based packages that are available for you to apply updates, click **All Actions → Global Settings**, and selecting **Enhanced Support for Down-Level Devices**. When this option is selected, “Other Available Software” is listed in the Installed Version column for undetected devices. For more information, see Configuring global firmware-update settings.

Notes:

  - The global settings cannot be changed when updates to managed devices are in progress.
  - It takes a few minutes to generate the additional options. After a few moments, you might need to click the **Refresh** icon ( ) to refresh the table.
- Ensure that no jobs are currently running on the target server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.
- Ensure that the firmware-updates repository contains the firmware packages that you intend to deploy. If not, refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.

  If you intend to install prerequisite firmware, ensure that the prerequisite firmware is downloaded in the repository as well.

  In some cases, multiple versions might be needed to update firmware, and all versions would need to be downloaded to the repository. For example, to upgrade the IBM FC5022 SAN scalable switch from v7.4.0a to v8.2.0a, you must first install v8.0.1-pha, then v8.1.1, and then v8.2.0a. All three versions must be in repository to update the switch to v8.2.0a.
- Typically, devices must be restarted to activate the firmware update. If you choose to restart the device during the update process (*immediate activation*), ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.
- For ThinkSystem SR635 and SR655 servers, you can use this traditional update function to apply only baseboard management controller and UEFI firmware updates. Management-controller firmware version AMBT10M or later is required, and UEFI firmware version CFE114L or later is required. To update all components (including the management controller, UEFI, disk drives, and IO options), use the bundle update function (see Applying bundled firmware updates using compliance policies).

About this task

- You can update selected firmware on a maximum of 50 devices at one time. If you choose to update selected firmware on more than 50 devices, the remaining devices are queued. A queued device is taken off the “selected-firmware update” queue when either the activation completes on an updated device or an updated device is placed in the Pending Maintenance Mode state (if a restart is required on that device). When a device in the Pending Maintenance Mode state is restarted, the device boots into Maintenance Mode and continues the update process, even if the maximum number of firmware updates is already in progress.
- You can apply and activate firmware that is later than the currently installed firmware.
- You can choose to apply all updates for a specific device. However, you can also choose to expand a device to specify updates for specific components, such as the baseboard management controller or UEFI.
- If you choose to install a firmware-update package that contains updates for multiple components, all components to which the update package applies are updated.

Procedure

To apply and activate updates on managed devices, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.

Step 2. Click the **Update with Policy** tab.

Step 3. Select one or more devices and devices to which firmware updates are to be applied.

You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed devices by selecting an option in the **Show** menu to list only devices in a specific chassis, rack, or group, by entering text (such as a name or IP address) in the **Filter** field, or by clicking the following icons to list only devices with a specific status.

- **Hide compliant devices** icon ( )
- **Hide non-compliant devices status** icon ( )
- **Hide devices without an assigned compliance policy** icon ( )
- **Hide devices not being monitored** icon ( )
- **Hide devices with firmware pending activation** icon ( )
- **Hide devices with compliance errors** icon ( )
- **Hide devices not supported for updates** icon ( )
- **Hide devices undergoing firmware updates** icon ( )
- **Hide devices with nonstageable firmware** icon ( )

The **Groups** column indicates the groups of which each device is a member. You can hover over the **Groups** column to get a complete list of groups, by group type

The **Installed Version** column indicates the installed firmware version, compliance status, or device status.

The compliance status can be one of the following:

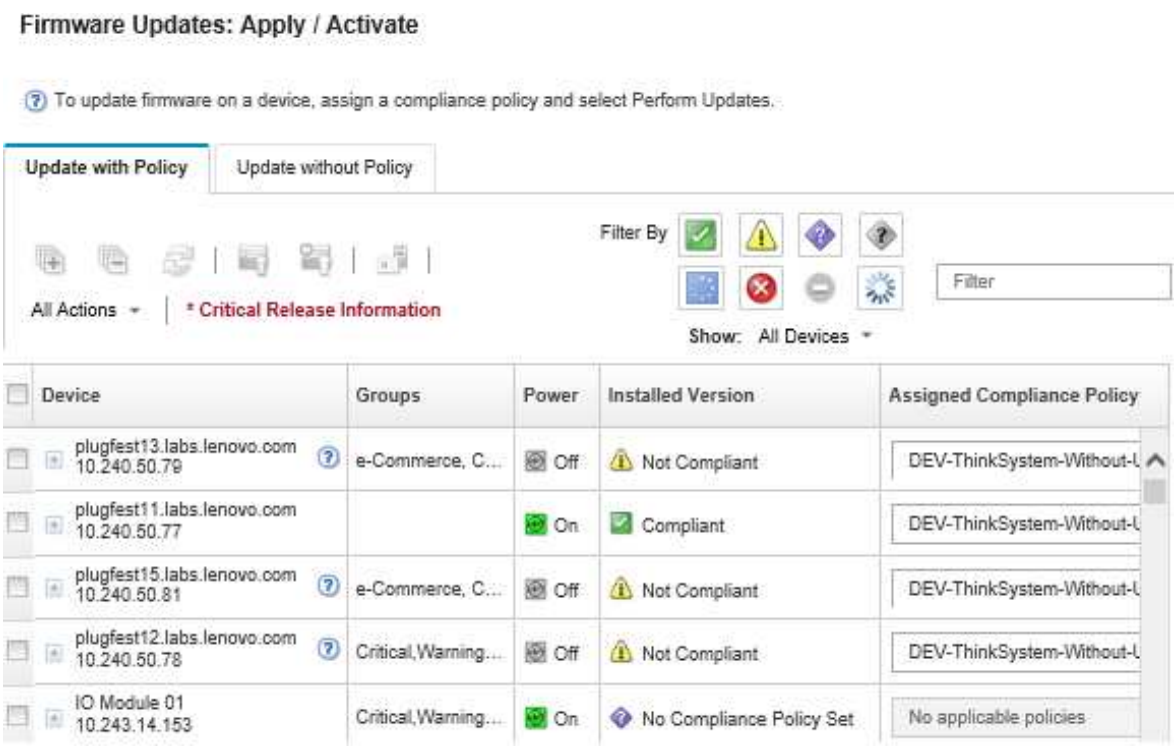
- **Compliant**
- **Compliance Error**
- **Not Compliant**
- **No Compliance Policy Set**
- **Not Monitored**

The device status can be one of the following:

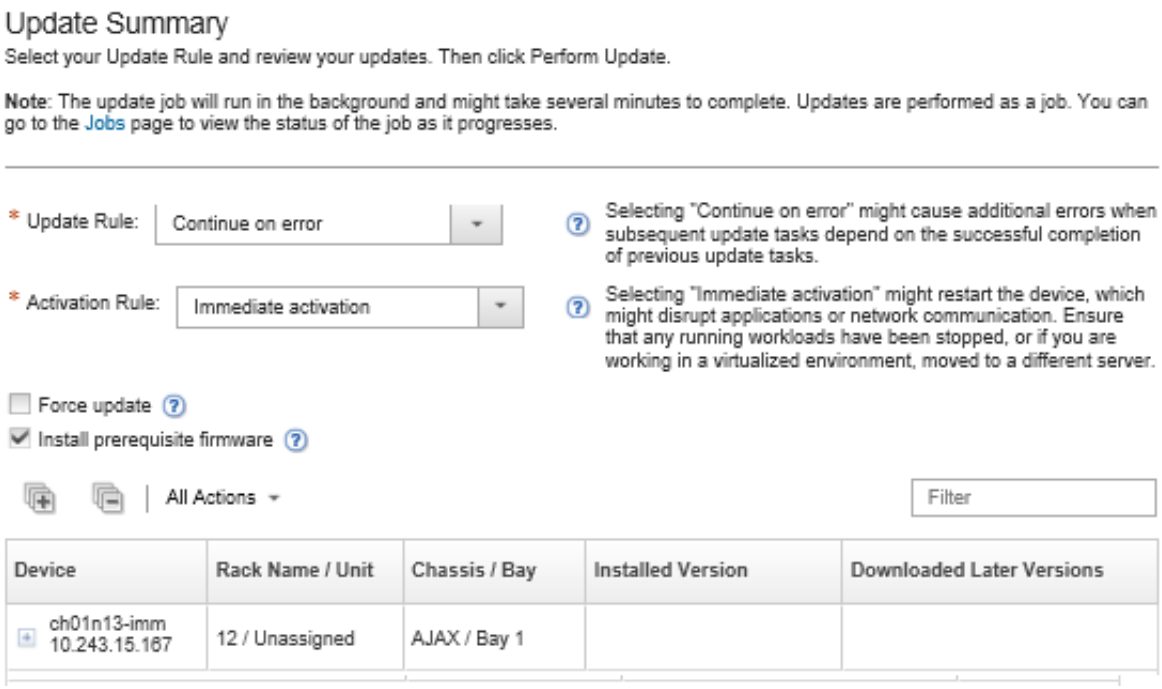
- **Updates Not Supported**
- **Update in Progress**

Notes: If the installed firmware version is pending activation, "(Pending Activation)" is appended to the installed firmware version or compliance status of each applicable device, for example "2.20 / A9E12EUS (Pending Activation)." To see the pending-activation status, the following firmware version must be installed on the primary baseboard management controller in the server.

- **IMM2**: TCOO46F, TCOO46E, or later (depending on the platform)
- **XCC**: CDI328M, PSI316N, TEI334I, or later (depending on the platform)



Step 4. Click the **Perform Updates** icon ( ). The Update Summary dialog is displayed.



Step 5. Select one of the following update rules

- **Stop all updates on error**. If an error occurs while updating any of the components (such as an adapter or management controller) in the target device, the firmware-update process stops for all selected devices in the current firmware-update job. In this case, none of the updates in the update package for the device are applied. The current firmware that is installed on all selected systems remains in effect.

- **Continue on error**. If an error occurs while updating any of the devices in the device, the firmware-update process does not update the firmware for that specific device; however, the firmware-update process continues to update the other devices in the device and continues to update all other devices in the current firmware-update job.
- **Continue to next system on error**. If an error occurs while updating any of the devices in the device, the firmware-update process stops all attempts to update the firmware for that specific device, so the current firmware that is installed on that device remains in effect. The firmware-update process continues to update all other devices in the current firmware-update job.

Step 6. Select one of the following activation rules:

- **Immediate activation**. During the update process, the device might be restarted automatically several times until the entire update process is complete. Ensure that you quiesce all applications on the device before you proceed.
- **Delayed activation**. Some but not all update operations are performed. Devices must be restarted to continue the update process. Additional restarts are then performed until the update operation completes.

  An event is raised when the status changes to **Pending Firmware Maintenance Mode** to notify you when the server needs to be restarted.

  If a device restarts for any reason, the delayed update process completes.

  This activation rule is supported for only servers and rack switches. CMMs and Flex switches are immediately activated, regardless of this setting.

  An event is raised when the status changes to **Pending Firmware Maintenance Mode** to notify you when the server needs to be restarted.

  The delayed update process completes when the device is restarted for any reason (including a manual restart). There is no time limit when the server must be restarted.

  XClarity Administrator can apply updates with delayed activation for up to 50 devices at one time. If you attempt to apply updates with delayed activation for more than 50 devices, the remaining devices are queued. A device comes off the queue when a device being updated is placed in the **Pending Firmware Maintenance Mode state.**

  Important:

  – If XClarity Administrator is restarted during the update job, the update job will stop with error.
  – If a server in the **Pending Firmware Maintenance Mode** state is restarted while XClarity Administrator is down or unreachable, the server boots to the BMU, but because XClarity Administrator cannot connect to the BMU and times out after 60 seconds, the system power status is restored by the baseboard management controller (powers off if it was off, restarts if it was powered on).
- **Prioritized activation**. Firmware updates on the baseboard management controller are activated immediately; all other firmware updates are firmware updates are activated the next time the device is restarted. Additional restarts are then performed until the update operation completes. This rule is supported only for servers.

  An event is raised when the status changes to Pending Firmware Maintenance Mode to notify you when the server needs to be restarted.

Note: When enabled, the Wake-on-LAN boot option can interfere with XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.

Step 7. Optional: **Optional:** Clear **Install prerequisite firmware** if you do not want to install prerequisite firmware. Prerequisite firmware is installed by default.

Note: When using **Delayed Activation** or **Prioritized Activation** for prerequisite firmware updates, you might need to restart the server to activate the prerequisite firmware. After the initial restart, the remaining firmware updates are installed using **Immediate Activation**.

Step 8. Optional: **Optional:** Select **Force update** to update firmware on the selected components even if the firmware level is up to date or to apply a firmware update that is earlier than the one currently installed on the selected components.

Note: You can apply earlier version of firmware to device options, adapters, and drives that support down-leveling. See your hardware documentation to determine if down-leveling is supported.

Step 9. Click **Perform Update** to update immediately, or click **Schedule** to schedule this update to run at a later time.

If needed, you can perform power actions on the managed devices. The power actions are useful when **Delayed Activation** is selected and you want the updates to continue when the device is waiting in the "Pending Maintenance" state. To perform a power action on a managed device from this page, click **All Actions → Power Actions**, and then click one of the following power actions.

- **Power on**
- **Power down OS and power off**
- **Power off**
- **Shut down OS and restart**
- **Restart**

After you finish

When applying a firmware update, if the server fails to enter maintenance mode, attempt to apply the update again.

If updates were not completed successfully, see Firmware update and repository issues in the XClarity Administrator online documentation for troubleshooting and corrective actions.

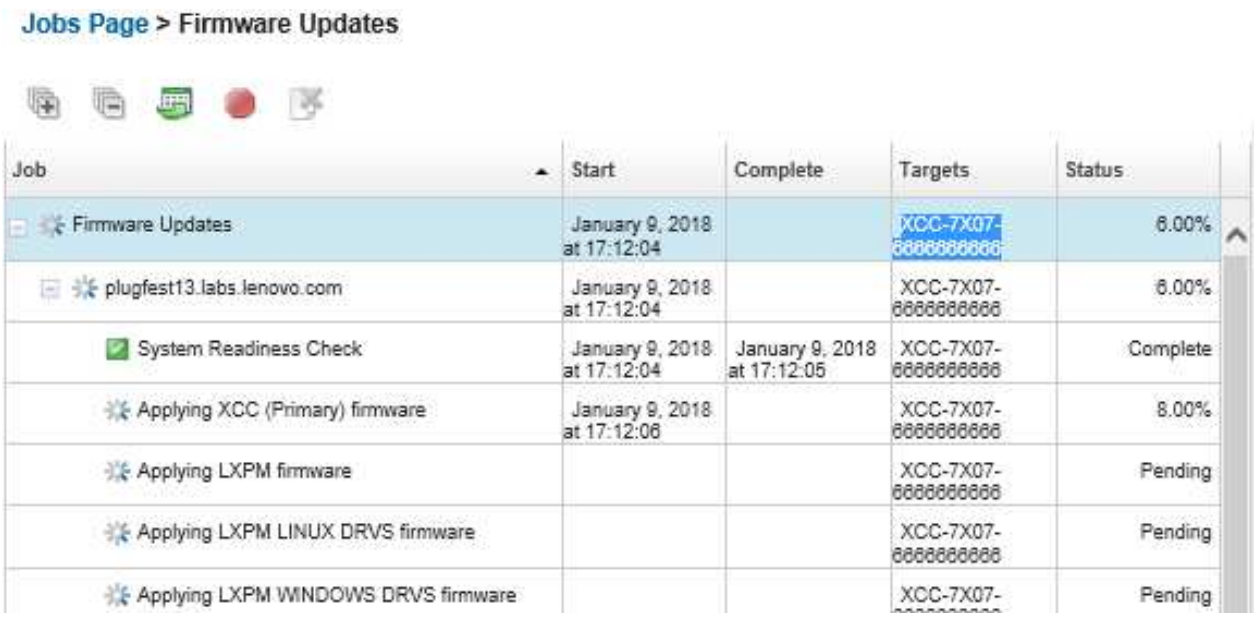
From the Firmware Updates: Apply/Activate page, you can perform the following actions:

- Export firmware and compliance information for each managed device by clicking **All Actions → Export View as CSV**.

  Note: The CSV file contains only filtered information in the current view. Information that is filtered out of the view and information in hidden columns are not included.
- Cancel an update that is being applied to a device by selecting the device and clicking the **Cancel Update** icon ( ).

  Note: You can cancel firmware updates that are in the queue to start. After the update process starts, the firmware update is cancelable only when the update process is performing a task other than applying the update, such as changing to maintenance mode or restarting the device.
- View the status of the firmware update directly from the Apply / Activate page in the **Status** column.
- Monitor the status of the update process from the jobs log. From the Lenovo XClarity Administrator menu, click **Monitoring → Jobs**.

  For more information about the jobs log, see Monitoring jobs .



When the firmware-update jobs are complete, you can verify that the devices are compliant by clicking **Provisioning → Firmware Updates: Apply/Activate** to go back to the Firmware Updates: Apply/Activate page, and then clicking the **Refresh** icon ( ). The current firmware version that is active on each device is listed in the **Installed Version** column.

Applying selected firmware updates without using compliance policies

You can quickly apply and activate firmware that is later than the currently installed firmware on a single managed device or group of devices without using compliance policies.

Learn more:

- XClarity Administrator: Boosting Efficiency when Updating Firmware
- Lenovo ThinkSystem Firmware and Driver Update Best Practices
- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Firmware updates
- XClarity Administrator: Provisioning firmware security updates

Before you begin

- Read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).
- Initially, devices that are not supported for updates are hidden from the view. Devices that are not supported cannot be selected for updates.
- By default, all detected components are listed as available for applying updates; however, down-level firmware might prevent a component from appearing in inventory or reporting full-version information. To list all policy-based packages that are available for you to apply updates, click **All Actions → Global Settings**, and selecting **Enhanced Support for Down-Level Devices**. When this option is selected, “Other Available Software” is listed in the Installed Version column for undetected devices. For more information, see Configuring global firmware-update settings.

  Notes:

  – The global settings cannot be changed when updates to managed devices are in progress.

  - It takes a few minutes to generate the additional options. After a few moments, you might need to click the **Refresh** icon ( ) to refresh the table.
- Ensure that no jobs are currently running on the target server. If jobs are running, the update job is queued until all other jobs have completed. To see a list of active jobs, click **Monitoring → Jobs**.
- Ensure that the firmware-updates repository contains the firmware packages that you intend to deploy. If not, refresh the product catalog, and download the appropriate firmware updates (see Refreshing the product catalog and Downloading firmware updates).

  Note: When XClarity Administrator is initially installed, the product catalog and the repository are empty.

  If you intend to install prerequisite firmware, ensure that the prerequisite firmware is downloaded in the repository as well.

  In some cases, multiple versions might be needed to update firmware, and all versions would need to be downloaded to the repository. For example, to upgrade the IBM FC5022 SAN scalable switch from v7.4.0a to v8.2.0a, you must first install v8.0.1-pha, then v8.1.1, and then v8.2.0a. All three versions must be in repository to update the switch to v8.2.0a.
- Typically, devices must be restarted to activate the firmware update. If you choose to restart the device during the update process (*immediate activation*), ensure that any running workloads have either been stopped or, if you are working in a virtualized environment, moved to a different server.

About this task

- You can update selected firmware on a maximum of 50 devices at one time. If you choose to update selected firmware on more than 50 devices, the remaining devices are queued. A queued device is taken off the “selected-firmware update” queue when either the activation completes on an updated device or an updated device is placed in the Pending Maintenance Mode state (if a restart is required on that device). When a device in the Pending Maintenance Mode state is restarted, the device boots into Maintenance Mode and continues the update process, even if the maximum number of firmware updates is already in progress.
- You can apply and activate firmware that is later than the currently installed firmware.
- You can choose to apply all updates for a specific device. However, you can also choose to expand a device to specify updates for specific components, such as the baseboard management controller or UEFI.
- If you choose to install a firmware-update package that contains updates for multiple components, all components to which the update package applies are updated.

Procedure

To apply and activate updates on a managed device, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.

Step 2. Click the **Update without Policy** tab.

Step 3. Select the firmware level in the **Downloaded later versions** column for each device that you want to update.

Step 4. Select one or more devices and devices that you want to update.

You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed devices by selecting an option in the **Show** menu to list only devices in a specific chassis, rack, or group, by entering text (such as a name or IP address) in the **Filter** field, or by clicking the following icons to list only devices with a specific status.

- **Hide components with some later versions** icon ( )

- **Hide components with no later versions** icon ( )
- **Hide devices not supported for updates** icon ( )
- **Hide devices undergoing firmware updates** icon ( )
- **Hide devices with nonstageable firmware** icon ( )

The **Groups** column indicates the groups of which each device is a member. You can hover over the **Groups** column to get a complete list of groups, by group type

The **Installed Version** column indicates the installed firmware version, compliance status, or device status.

The compliance status can be one of the following:

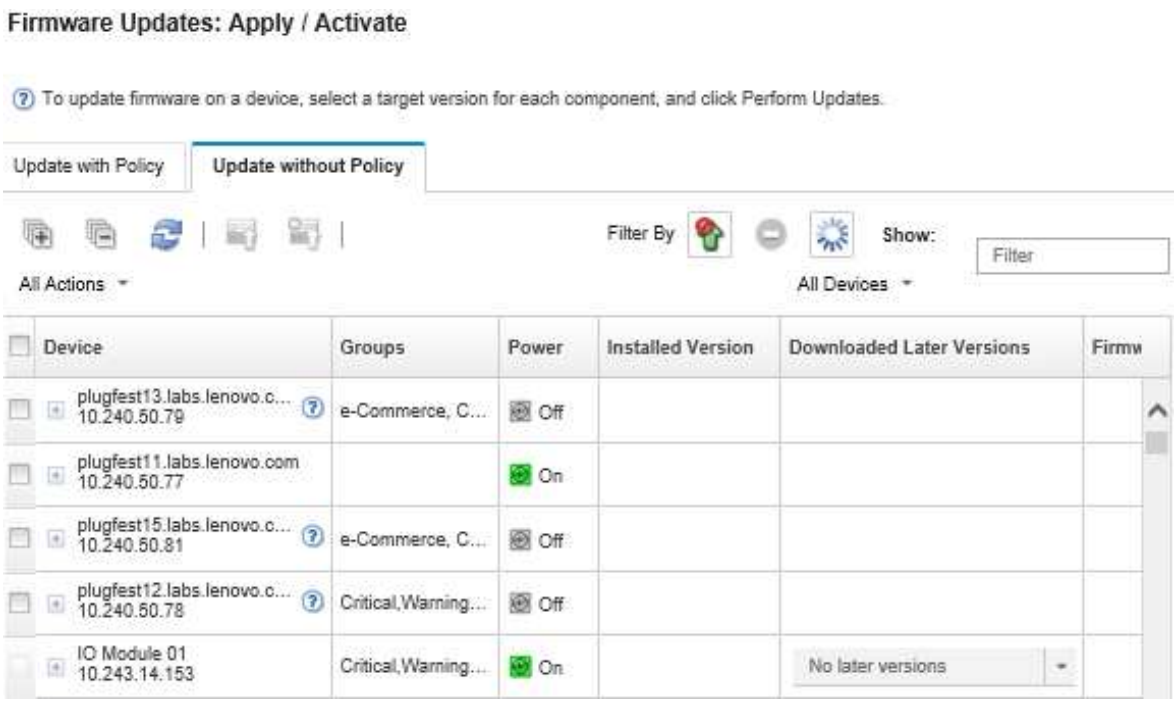
- **Compliant**
- **Compliance Error**
- **Not Compliant**
- **No Compliance Policy Set**
- **Not Monitored**

The device status can be one of the following:

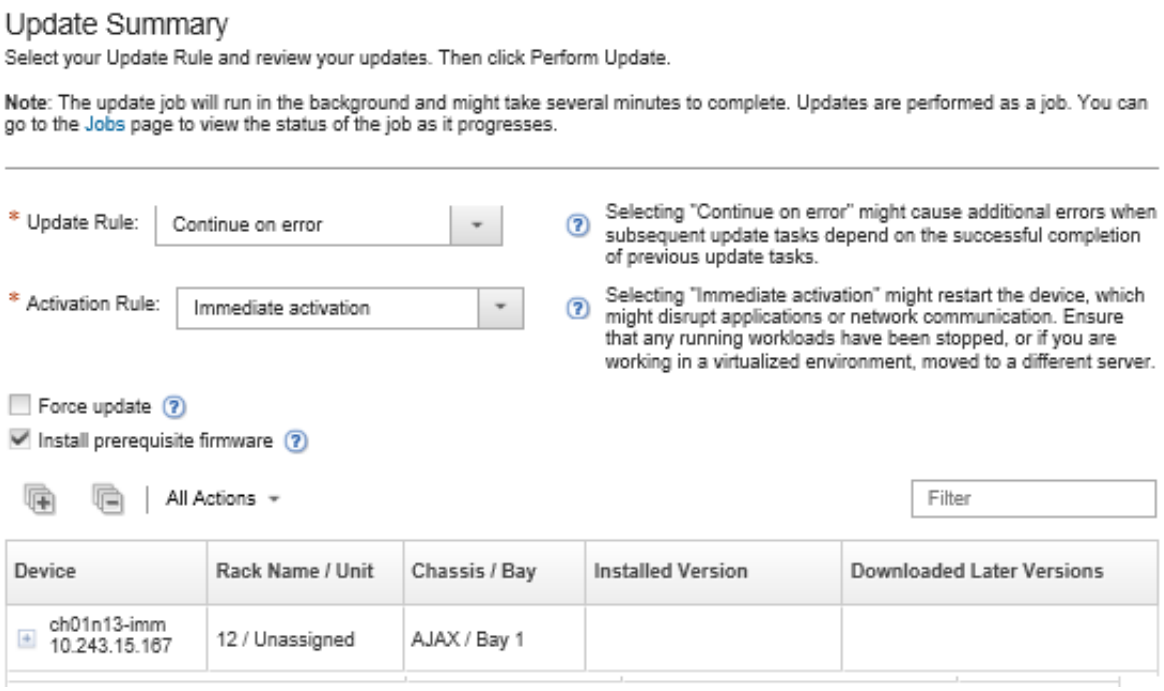
- **Updates Not Supported**
- **Update in Progress**

Notes: If the installed firmware version is pending activation, "(Pending Activation)" is appended to the installed firmware version or compliance status of each applicable device, for example "2.20 / A9E12EUS (Pending Activation)." To see the pending-activation status, the following firmware version must be installed on the primary baseboard management controller in the server.

- **IMM2**: TCOO46F, TCOO46E, or later (depending on the platform)
- **XCC**: CDI328M, PSI316N, TEI334I, or later (depending on the platform)



Step 5. Click the **Perform Updates** icon ( ). The Update Summary dialog is displayed.



Step 6. Select one of the following update rules

- **Stop all updates on error**. If an error occurs while updating any of the components (such as an adapter or management controller) in the target device, the firmware-update process stops for all selected devices in the current firmware-update job. In this case, none of the updates in the update package for the device are applied. The current firmware that is installed on all selected systems remains in effect.
- **Continue on error**. If an error occurs while updating any of the devices in the device, the firmware-update process does not update the firmware for that specific device; however, the

firmware-update process continues to update the other devices in the device and continues to update all other devices in the current firmware-update job.

- **Continue to next system on error**. If an error occurs while updating any of the devices in the device, the firmware-update process stops all attempts to update the firmware for that specific device, so the current firmware that is installed on that device remains in effect. The firmware-update process continues to update all other devices in the current firmware-update job.

Note: When enabled, the Wake-on-LAN boot option can interfere with XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.

Step 7. Select one of the following activation rules:

- **Immediate activation**. During the update process, the device might be restarted automatically several times until the entire update process is complete. Ensure that you quiesce all applications on the device before you proceed.
- **Delayed activation**. Some but not all update operations are performed. Devices must be restarted to continue the update process. Additional restarts are then performed until the update operation completes.

  An event is raised when the status changes to **Pending Firmware Maintenance Mode** to notify you when the server needs to be restarted.

  If a device restarts for any reason, the delayed update process completes.

  This activation rule is supported for only servers and rack switches. CMMs and Flex switches are immediately activated, regardless of this setting.

  An event is raised when the status changes to **Pending Firmware Maintenance Mode** to notify you when the server needs to be restarted.

  The delayed update process completes when the device is restarted for any reason (including a manual restart). There is no time limit when the server must be restarted.

  XClarity Administrator can apply updates with delayed activation for up to 50 devices at one time. If you attempt to apply updates with delayed activation for more than 50 devices, the remaining devices are queued. A device comes off the queue when a device being updated is placed in the **Pending Firmware Maintenance Mode state.**

  Important:

  – If XClarity Administrator is restarted during the update job, the update job will stop with error.

  – If a server in the **Pending Firmware Maintenance Mode** state is restarted while XClarity Administrator is down or unreachable, the server boots to the BMU, but because XClarity Administrator cannot connect to the BMU and times out after 60 seconds, the system power status is restored by the baseboard management controller (powers off if it was off, restarts if it was powered on).
- **Prioritized activation**. Firmware updates on the baseboard management controller are activated immediately; all other firmware updates are firmware updates are activated the next time the device is restarted. Additional restarts are then performed until the update operation completes. This rule is supported only for servers.

  An event is raised when the status changes to Pending Firmware Maintenance Mode to notify you when the server needs to be restarted.

Note: When enabled, the Wake-on-LAN boot option can interfere with XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues “Wake on Magic Packet” commands.

Step 8. Optional: **Optional:** Clear **Install prerequisite firmware** if you do not want to install prerequisite firmware. Prerequisite firmware is installed by default.

Note: When using **Delayed Activation** or **Prioritized Activation** for prerequisite firmware updates, you might need to restart the server to activate the prerequisite firmware. After the initial restart, the remaining firmware updates are installed using **Immediate Activation**.

Step 9. Optional: **Optional:** Select **Force update** to update firmware on the selected components even if the firmware level is up to date or to apply a firmware update that is earlier than the one currently installed on the selected components.

Note: You can apply earlier version of firmware to device options, adapters, and drives that support down-leveling. See your hardware documentation to determine if down-leveling is supported.

Step 10. Click **Perform Update** to update immediately, or click **Schedule** to schedule this update to run at a later time.

If needed, you can perform power actions on the managed devices. The power actions are useful when **Delayed Activation** is selected and you want the updates to continue when the device is waiting in the "Pending Maintenance" state. To perform a power action on a managed device from this page, click **All Actions → Power Actions**, and then click one of the following power actions.

- **Power on**
- **Power down OS and power off**
- **Power off**
- **Shut down OS and restart**
- **Restart**

After you finish

When applying a firmware update, if the server fails to enter maintenance mode, attempt to apply the update again.

If updates were not completed successfully, see Firmware update and repository issues in the XClarity Administrator online documentation for troubleshooting and corrective actions.

From the Firmware Updates: Apply/Activate page, you can perform the following actions:

- Export firmware and compliance information for each managed device by clicking **All Actions → Export View as CSV**.

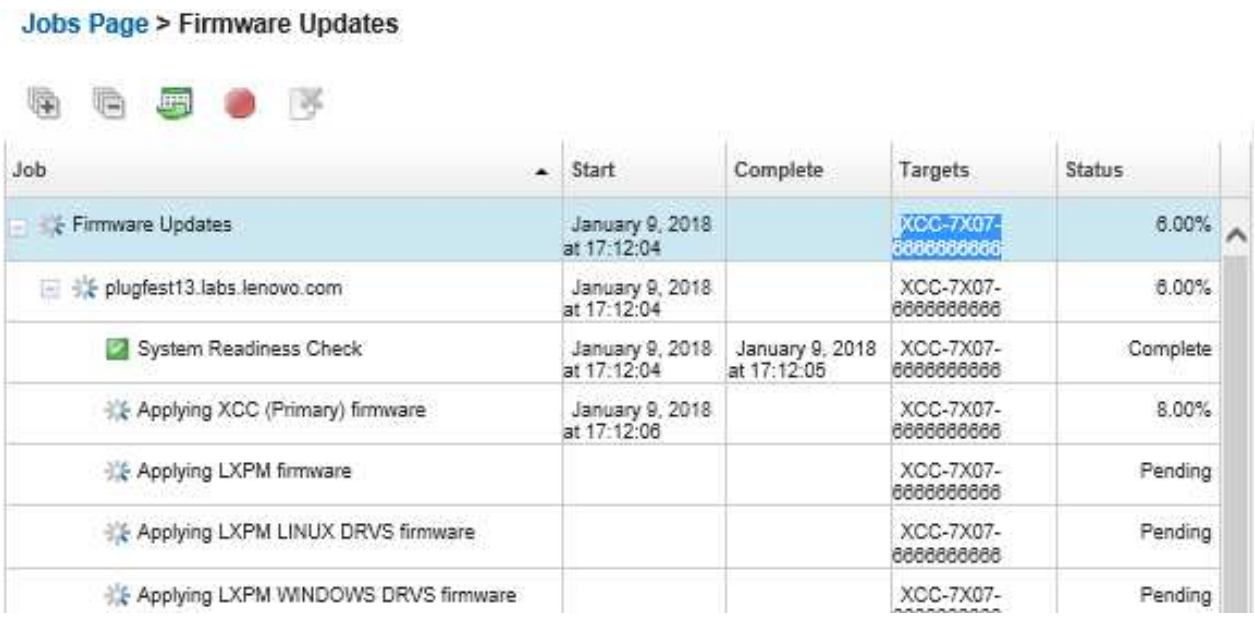
  Note: The CSV file contains only filtered information in the current view. Information that is filtered out of the view and information in hidden columns are not included.

- Cancel an update that is being applied to a device by selecting the device and clicking the **Cancel Update** icon ( ).

  Note: You can cancel firmware updates that are in the queue to start. After the update process starts, the firmware update is cancelable only when the update process is performing a task other than applying the update, such as changing to maintenance mode or restarting the device.

- View the status of the firmware update directly from the Apply / Activate page in the **Status** column.
- Monitor the status of the update process from the jobs log. From the Lenovo XClarity Administrator menu, click **Monitoring → Jobs**.

  For more information about the jobs log, see Monitoring jobs .



When the firmware-update jobs are complete, you can verify that the devices are compliant by clicking **Provisioning → Firmware Updates: Apply/Activate** to go back to the Firmware Updates: Apply/Activate page, and then clicking the **Refresh** icon ( ). The current firmware version that is active on each device is listed in the **Installed Version** column.

Chapter 14. Updating Windows device drivers on managed servers

Using windows UpdateXpress System Packs (UXSPs), you can update OS device drivers on deployed Windows operating systems.

Before you begin

You must have **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** or **lxc-hw-admin** authority to manage and deploy OS device drivers and to perform power actions on managed servers from the Windows Driver Updates pages.

Updating firmware and updating device drivers are separate processes in XClarity Administrator; there is no connection between these processes. XClarity Administrator does not maintain compliance between firmware and devices drivers on managed devices, even though it is recommended that you update device drivers at the same time as the firmware.

About this task

Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows.

Only device drivers for Windows Server 2012 R2 and later are supported. XClarity Administrator does not support updating Linux or VMware devices drivers.

For information about installing device drivers when deploying operating systems, see Installing operating systems on bare-metal servers.

Procedure

Step 1. **Configuring Windows Server for OS device-driver updates**

Lenovo XClarity Administrator uses the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems. The WinRM service must be correctly configured on the target servers before attempting to update OS device drivers (see Configuring Windows Server for OS device-driver updates).

Step 2. **Manage the OS device-driver repository**

The *OS device-driver repository* contains a catalog of available Windows device drivers and the device-drivers packages that can be applied to the managed devices.

The *catalog* contains information about all Windows UpdateXpress System Packs (UXSPs) and device-driver updates that are available for all Lenovo servers that support Windows. The catalog organizes the device-driver updates by device type. When you refresh the catalog, XClarity Administrator retrieves information about the available UXSPs from the Lenovo Data Center Support website (including the metadata .xml and readme .txt files) and stores the information to the repository. The payload file (.exe) is not downloaded. For more information about refreshing the catalog, see Refreshing the OS device-driver catalog.

You can download or import Windows UXSPs in the repository. Windows UXSPs contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. UXSPs must be available in the repository before you can update Windows device drivers on

© Copyright Lenovo 2015, 2022

managed severs. For more information about downloading device drivers, see Downloading Windows device drivers .

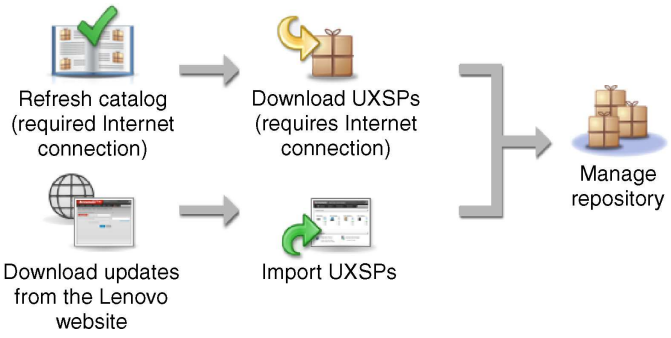
You can determine whether UXSPs are stored in the OS device-driver repository from the Download Status column on the Individual Updates tab of the Windows Driver Updates Repository page. This column contains the following values.

- **Downloaded**. The entire package or the individual update is stored in the repository.
- ***x* of *y* Downloaded**. Some but not all updates in the package are stored in the repository. The numbers in parentheses indicate the number of available updates and the number of stored updates, or there are no updates for the specific device type.
- **Not Downloaded**. The entire package or the individual update is available but not stored in the repository.

Note: When you download or import UXSPs from the Windows Driver Updates Repository page, only device drivers are downloaded and stored in the repository. Firmware updates are discarded. For information about downloading or importing firmware updates, see Managing the firmware-updates repository.

XClarity Administrator must be connected to the Internet to refresh the catalog and download UXSPs. If it is not connected to the Internet, you can manually download the UXSPs to a workstation that has network access to the XClarity Administrator host using a web browser. This UXSPs download is a zip format file and contains all the required device driver files for the UXSP, including the payload (.exe), metadata (.xml), and change history file (.chg), and readme files (.txt).

Note: You might see messages that the firmware (fw) files are not needed and have been removed. This is normal because only windows device drivers are updated using this process.



Attention:

- Do not unzip the UXSP before importing the it.
- The Windows UXSPs include device drivers and firmware updates. The firmware updates in the Windows UXSPs are discarded when the UXSPs are imported to the repository and a warning message displayed. Only the device drivers are imported.

Step 3. **Applying OS device drivers**

XClarity Administrator does not automatically update device drivers to managed servers. To update device drivers, you must manually apply the device drivers on selected servers.

Attention: Before you attempt to update device drivers on managed servers, ensure that you reviewed the following considerations and completed any applicable prerequisite actions.

- Devices that are not supported cannot be selected for updates.

- Read the device-driver update considerations before you attempt to update device drivers on your managed servers (see OS device-driver update considerations).
- Ensure that the repository contains the UXSPs and device drivers that you intend to deploy (see Downloading Windows device drivers).

  Note: When XClarity Administrator is initially installed, the catalog and repository are empty.
- XClarity Administrator can use the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems HTTPS is the default. To use HTTP, click **All Actions → Global Settings** on the Windows Driver updates: Apply page, and then clear **Use HTTPS for Windows driver updates**.

  Attention: When using HTTP, Windows user credentials are sent over the network *without* encryption and can be easily viewed using commonly available network troubleshooting tools.

  Important:

  – Ensure that Windows Remote Management (WinRM) on the target server is configured to use the same setting (HTTPS or HTTP) that is defined in XClarity Administrator (see Configuring Windows Server for OS device-driver updates).

  – Ensure that WinRM on the target server is configured with basic authentication.

  – When using HTTPS, ensure that WinRM on the target server is configured with **allowUnencrypted=false**.
- Ensure that PowerShell is supported on the target server.
- Ensure that the target server is powered on before attempting to update device drivers. If the server is not powered on, select the target server, and click **All Actions → Power Actions → Power On**.
- Ensure that XClarity Administrator has information that it needs to access the host operating system (see Managing access to operating-systems on managed servers.
- If you want to use a domain account when updating OS device drivers, ensure that you created the required configuration file (see Configuring a domain account for OS device-drivers updates).
- Ensure that no jobs are currently running on the target server. You cannot update device drivers on a managed server that is locked by a running job. If another update job is running on the target server, this update job is queued until the current update job completes. To see a list of active jobs, click **Monitoring → Jobs**.

For more information about updating device drivers, see Applying Windows device drivers.

OS device-driver update considerations

Before you begin updating OS device drivers for managed devices by using Lenovo XClarity Administrator, review the following important considerations.

Note: You must have **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** or **lxc-hw-admin** authority to manage and deploy device drivers and to perform power actions on managed servers from the Windows Driver Updates pages.

Network considerations

- Required ports and Internet addresses must be available before you attempt to download UpdateXpress System Packs (UXSPs). For more information, see Port availability and Firewalls and proxy servers in the XClarity Administrator online documentation.

- XClarity Administrator must have access to management and data network to access the operating system.
- XClarity Administrator must be able to communicate with the target server (both the baseboard management controller and the server's data network) over the network interface (Eth0 or Eth1) that was selected when you configured the XClarity Administrator network access and that the interface is configured with an IPv4 address or an IPv6 auto ULA address.

  To specify an interface to be used for operating-system deployment, see Configuring network access).

  For more information about the operating-system deployment network and interfaces, see Network considerations in the XClarity Administrator online documentation.
- IP addresses must be are unique for the host operating system.
- XClarity Administrator can use the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems HTTPS is the default. To use HTTP, click **All Actions → Global Settings** on the Windows Driver updates: Apply page, and then clear **Use HTTPS for Windows driver updates**.

  Attention: When using HTTP, Windows user credentials are sent over the network *without* encryption and can be easily viewed using commonly available network troubleshooting tools.

Managed-device considerations

- For ThinkSystem SR635 and SR655 servers, updating Windows device drivers is not supported.
- Only ThinkSystem, Lenovo System x, and Lenovo Flex System servers are supported.
- XClarity Administrator does not validate the relationship between the management controller and operating system. The baseboard management controller is used to power on or off the server.
- Ensure that the LAN-over-USB interface is enabled. LAN-over-USB is used when updating OS device drivers.

Operating-system and device-driver considerations

- You can update device drivers for the following operating systems.
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

  Note: XClarity Administrator is tested with only Windows versions that are supported by Microsoft at the time when the XClarity Administrator version was released.
- Windows Remote Management (WinRM) must be configured for HTTPS on the target server (see Configuring Windows Server for OS device-driver updates).
- PowerShell must be supported on the target server.
- You must provide information that is needed to access the host operating system on the target server, including the OS IP address and credentials (see Managing access to operating-systems on managed servers). You must provide credentials for a user account that has administrator authority.
- XClarity Administrator updates only device drivers that are out of compliance. Device drivers are out of compliance when the version on the server is earlier than version in the selected UXSP. Device drivers that are equal to or later than version in the selected UXSP are skipped.
- Device-driver compliance is accurate only when hardware is present. If hardware is not present, device drivers are still applied to the server. When the missing hardware is added to the server, Windows loads the latest version.
- System x servers do not support some predefined device drivers that come with XClarity Administrator. To deploy device drivers to these servers, create a custom profile that includes only the needed device drivers.

Managing the OS device-drivers repository

The *OS device-driver repository* includes the catalog and downloaded Windows device drivers.

About this task

The *catalog* contains information about all Windows UpdateXpress System Packs (UXSPs) and device-driver updates that are available for all Lenovo servers that support Windows. The catalog organizes the device-driver updates by device type. When you refresh the catalog, XClarity Administrator retrieves information about the available UXSPs from the Lenovo Data Center Support website (including the metadata .xml and readme .txt files) and stores the information to the repository. The payload file (.exe) is not downloaded. For more information about refreshing the catalog, see Refreshing the OS device-driver catalog.

Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. You can download or import Windows UXSPs in the repository. Windows UXSPs contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. UXSPs must be available in the repository before you can update Windows device drivers on managed severs.For more information about downloading device drivers, see Downloading Windows device drivers .

XClarity Administrator must be connected to the Internet to refresh the catalog and download UXSPs. If it is not connected to the Internet, you can manually download the UXSPs to a workstation that has network access to the XClarity Administrator host using a web browser. This UXSPs download is a zip format file and contains all the required device driver files for the UXSP, including the payload (.exe), metadata (.xml), and change history file (.chg), and readme files (.txt).

After a UXSP is downloaded in the repository, information about each device driver in the pack is added to the Windows Driver Updates Repository page. This includes the release date, size, and severity. The severity indicates the impact and the need to apply the update to help you to assess how your environment might be affected.

- **Initial Release**. This is the first release of the device driver.
- **Critical**. The device driver contains urgent fixes for data corruption, security, or stability issues.
- **Suggested**. The device driver contains significant fixes for problems that you are likely to encounter.
- **Non-Critical**. The device driver contains minor fixes, performance enhancements, and textual changes.

Notes:

- The severity is relative to the previously released version of the device driver. For example, if the installed device driver is v1.01, and update v1.02 is Critical, and update v1.03 is Recommended, this means that the update from 1.02 to 1.03 is recommended, but the update from v1.01 to v1.03 is critical because it is cumulative (v1.03 includes v1.02 critical issues).
- Special cases might arise where an update is only critical or recommended for a specific machine type. Refer to the Release Notes for additional information.

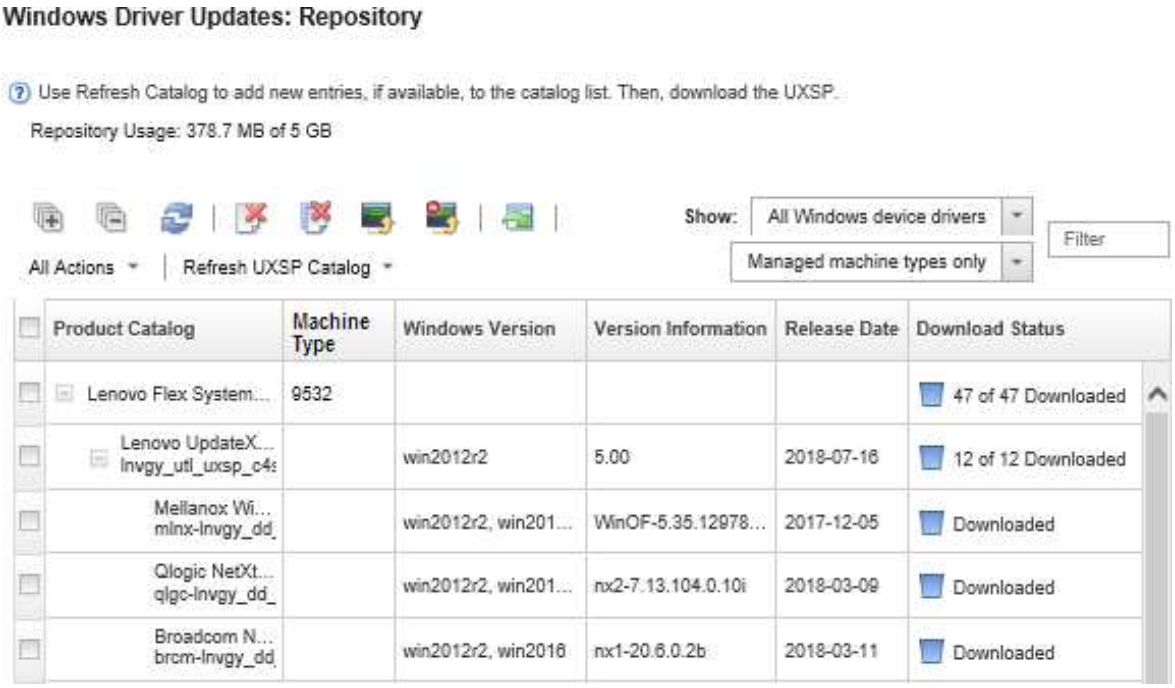
Procedure

To view UXSPs and device drivers that are available in the repository, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Repository**. The Windows Driver Updates Repository page is displayed with a list of available UXSPs, organized by device type.

Step 2. Expand a server type, and then expand the UXSPs that are available for that server type to list the device drivers that are available for that server type.

You can sort the table columns and click the **Expand** all icon ( ) and **Collapse** all icon ( ) to make it easier to find specific device drivers. In addition, you can filter the list of displayed server types and device drivers by selecting an option in the **Show** menu to list only device drivers of a specific age, device drivers for all server types or only managed-server types or by entering text in the **Filter** field.



From this page, you can perform the following actions:

- Retrieve the latest information about available UXSPs by clicking **Refresh Catalog**.

  Retrieving this information might take several minutes to complete. For more information, see Refreshing the OS device-driver catalog.
- Download UXSPs and device drivers using XClarity Administrator by refreshing the catalog and then clicking the **Download** icon ( ). When the UXSPs and device drivers are downloaded and added to the repository, the status changes to "Downloaded."

  For more information about downloading UXSPs and device drivers, see Downloading Windows device drivers .
- Import UXSPs that you manually downloaded to a workstation from the web or device drivers that you exported from XClarity Administrator (see Downloading Windows device drivers).
- Stop selected downloads that are currently in progress by clicking the **Cancel Downloads** icon ( ).
- Delete selected UXSPs or individual device drivers from the repository by clicking the **Delete** icon ( ).

Refreshing the OS device-driver catalog

The OS device-driver catalog contains information about all Windows UpdateXpress System Packs (UXSPs) and device drivers that are available for all Lenovo servers that support Windows device driver updates.

Before you begin

Ensure that Lenovo XClarity Administrator is connected to the Internet.

About this task

When you refresh the catalog, XClarity Administrator retrieves information about the available UXSPs from the Lenovo Data Center Support website (including the metadata .xml and readme .txt files) and stores the information to the repository. The payload file (.exe) is not downloaded. You must download the desired UXSP and OS device-driver payloads before updating device drivers on managed servers. For more information about downloading device drivers, see Downloading Windows device drivers .

Note: Refreshing the catalog might take several minutes to complete.

Procedure

To refresh the catalog, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Repository** to display the Windows Driver Updates Repository page.

Step 2. Click **Refresh Catalog**, and then click one of the following options to obtain information about the latest available UXSPs.

- **Refresh Selected - Latest Only**. Retrieves information about the most current UXSP versions that are available for only the selected servers.
- **Refresh All - Latest Only**. Retrieves information about the most current UXSP versions for all supported servers.
- **Refresh Selected**. Retrieves information about all UXSP versions that are available for only the selected servers.
- **Refresh All**. Retrieves information about all UXSP versions that are available for all supported servers.

Step 3. Click **Refresh Catalog** to refresh immediately, or click **Schedule** to schedule this refresh to run at a later time.

Downloading Windows device drivers

Windows UpdateXpress System Packs (UXSPs) contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. You can download or import Windows UXSPs in the repository. Windows UXSPs contain Windows device drivers for supported Windows versions and for Lenovo servers that supports Windows. UXSPs must be available in the repository before you can update Windows device drivers on managed severs.

Before you begin

Ensure that all required ports and Internet addresses are available before you attempt to download UpdateXpress System Packs (UXSPs). For more information, see Port availability and Firewalls and proxy servers in the XClarity Administrator online documentation.

To download UXSPs using XClarity Administrator, ensure that XClarity Administrator is connected to the Internet.

Internet Explorer and Microsoft Edge web browsers have an upload limit of 4 GB. If the file that you are importing is greater than 4 GB, consider using another web browser (such as Chrome or Firefox).

About this task

XClarity Administrator must be connected to the Internet to refresh the catalog and download UXSPs. If XClarity Administrator is not connected to the Internet, you can manually download the files to a workstation

that has network access to the XClarity Administrator host using a web browser and then import the updates into the firmware-updates repository.

You can determine whether UXSPs are stored in the repository from the **Download Status** column on Windows Driver Updates Repository page. This column contains the following values:

- **Downloaded**. All device drivers in the UXSP or the individual device driver is downloaded in the repository.
- *x* **of** *y* **Downloaded**. Some but not all device drivers in the UXSP are downloaded in the repository. The numbers in parentheses indicate the number of available device drivers and the number of download device drivers.
- **Not Downloaded**. The UXSP or individual device driver is available on the Lenovo Support site but not downloaded in the repository.

A message is displayed on the Windows Driver Updates Repository page when the space that is available for UXSPs and device drivers is more than 50% full. Another message is displayed on the page when the repository is more than 85% full. To reduce the space that is used in the repository, you can remove unused files by selecting the target files and then clicking the **Delete** icon ( ). For more information, see Managing disk space.

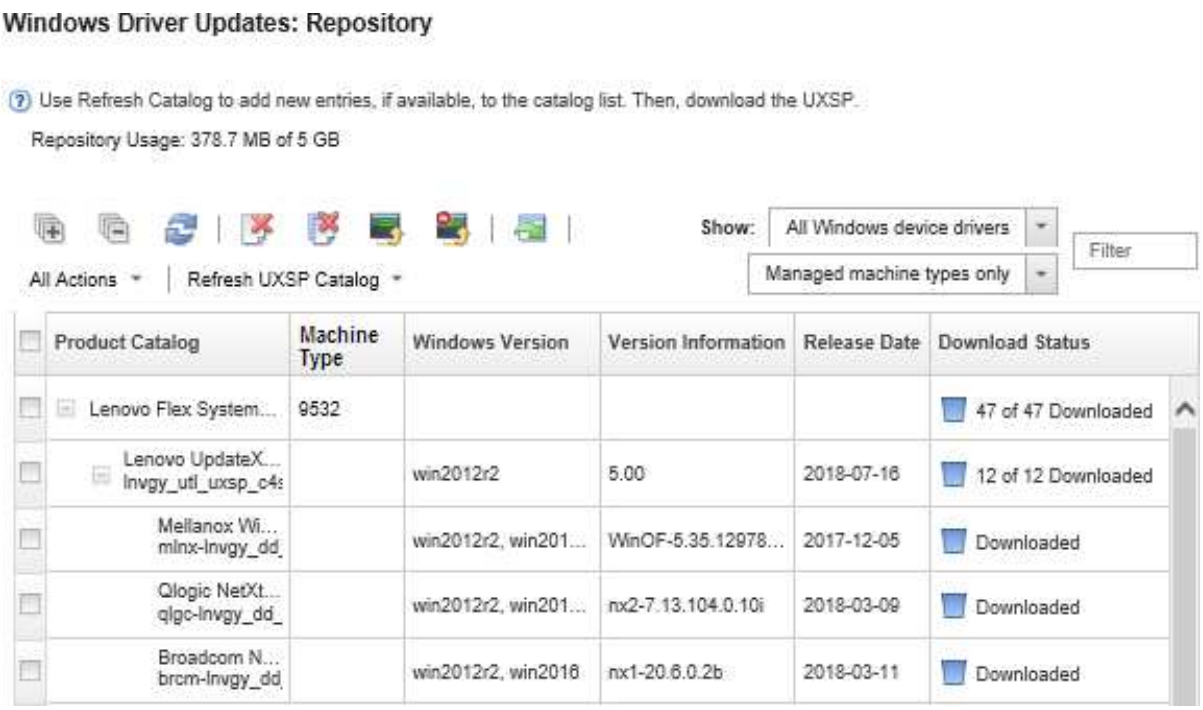
Attention: The Windows UXSPs include device drivers and firmware updates. The firmware updates in the Windows UXSPs are discarded when the UXSPs are imported to the repository and a warning message displayed. Only the device drivers are imported.

Procedure

To download UXSPs and specific device drivers, perform one of the following procedures.

- When XClarity Administrator is connected to the Internet:
  1. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Repository** to display the Windows Driver Updates Repository page.
  2. Click **Refresh Catalog**, and then click one of the following options to obtain information about the latest available UXSPs.
     - **Refresh Selected - Latest Only**. Retrieves information about the most current UXSP versions that are available for only the selected servers.
     - **Refresh All - Latest Only**. Retrieves information about the most current UXSP versions for all supported servers.
     - **Refresh Selected**. Retrieves information about all UXSP versions that are available for only the selected servers.
     - **Refresh All**. Retrieves information about all UXSP versions that are available for all supported servers.

     Note: Refreshing the catalog might take several minutes to complete.
  3. Expand the server type to display the list of available UXSPs. Expand the UXSP to see a list of available device drivers.



4. Select one or more target UXSPs and device drivers to download.
5. Click the **Download Selected** icon ( ).
6. Click **Download** to download immediately, or click **Schedule** to schedule this download to run at a later time.

   Downloading the UXSPs might take a few minutes. When the UXSPs and device drivers have been downloaded and stored in the repository, the row in the catalog is highlighted, and the **Download Status** column is changed to "Downloaded."

   You can monitor the status of the download process from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**. For more information about the jobs log, see Monitoring jobs.

- When XClarity Administrator *is not* connected to the Internet:
  1. Download the UXSPs to a workstation that has network connection to the XClarity Administrator host from the Lenovo Data Center Support website.
  2. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Repository** to display the Windows Driver Updates Repository page.
  3. Click the **Import** icon ( ).
  4. Click **Select Files**, and browse to the location of the UXSP on the workstation.
  5. Select the UXSP .zip file (do not unzip the zip file before importing), and then click **Open**.

     The UXSP .zip file contains the metadata file (.xml), payload (.exe), change history file (.chg), and readme file (.txt).
  6. Click **Import**.

     You can monitor the status of the import process from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**. For more information about the jobs log, see Monitoring jobs.

After you finish

From this page, you can perform the following actions on selected UXSPs.

- Cancel a download that is currently in process by clicking the **Cancel download** icon ( ).
- Delete all file associated with the UXSP by clicking the **Delete** icon ( ).

Configuring Windows Server for OS device-driver updates

Lenovo XClarity Administrator uses the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems. The WinRM service must be correctly configured on the target servers before attempting to update OS device drivers.

Before you begin

Required ports must be available. For more information, see Port availability in the XClarity Administrator online documentation.

For more information about configuring Windows Server before updating OS device driver, see the XClarity Administrator: Preparing for OS Device Driver Updates (white paper).

Procedure

To configure Windows Server to support updating OS device drivers, complete the following steps.

- **For HTTPS**
  1. Sign and install a server certificate on each of your target Windows systems.

     Important: The certificate must contain the following information.

     – In the Subject, ensure that the Domain Component is set (for example, DC=labs, DC=com, DC=company).
     – In the Subject Alternative Name, ensure that the DNS Name and host IP Address are set (for example, DNS Name=node1325C554A6F.labs.company.com and IP Address=10.245.43.149).
  2. Configure the remote management commands and data over an HTTPS connection by running one of the following commands from an administrative command prompt, and then confirm the suggested configuration changes.

     –
     ```
     winrm quickconfig -transport:https
     ```
     –
     ```
     winrm create winrm/config/Listener?Address=*+Transport=HTTPS
     @{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
     ```

     To manually set up a WinRM HTTPS listener according to WinRM documentation, see the How to configure WinRM for HTTPS webpage.
  3. Enable basic authentication of local Windows users by running the following command from an administrative command prompt.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  4. To avoid a possible timeout and sending WinRM request errors in compliance checking and performing driver updates, increase the default value for the WinRM response timeout by running the following command from an administrative command prompt. A value of 280000 is recommended. For more information, see the Installation and Configuration for Windows Remote Management webpage.
     ```
     winrm set winrm/config @{MaxTimeoutms="280000"}
     ```
  5. Open the port in your firewall that you configured for the WinRM HTTPS listener. The default HTTPS port is 5986. For example

```
netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow
protocol=TCP localport=5986
```

6. If you are using HTTPS listeners, adds the certificate to the XClarity Administrator trust store by completing the following steps. Adding the certificate to the trust store allows XClarity Administrator to trust the WinRM HTTPS listeners to which it connects. Repeat the following steps for any additional certification paths that need to be trusted for the Windows Remote Management service.
   a. Identify and collect the Certificate Authority root certificate that you used to sign the server certificates for the target Windows systems. If you do not have access to the CA root certificate, collect the server certificate itself or another certificate in the certification path.
   b. From the XClarity Administrator menu bar, click **Administration → Security** to display the Security page.
   c. Click **Trusted Certificates** under the Certificate Management section.
   d. Click the **Create** icon ( ) to display the Add Certificate dialog.
   e. Either browse for the certificate file that you collected in step 1, or copy/paste the contents of the certificate file into the text box.
   f. Click **Create**.
7. After the WinRM listener is running on your target Windows systems, XClarity Administrator can connect to these systems and perform the device driver updates.

- **For HTTP**
  1. Configure the remote management commands and data over an HTTP connection by running the following command from an administrative command prompt, and then confirm the suggested configuration changes.
     ```
     winrm quickconfig
     ```
  2. Enable basic authentication of local Windows users by running the following command from an administrative command prompt.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  3. Allocate enough memory for the update commands on this system by running the following command from an administrative command prompt.
     ```
     winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
     ```
  4. Allow unencrypted data by running the following command from an administrative command prompt.
     ```
     winrm set winrm/config/service @{AllowUnencrypted="true"}
     ```
  5. Open the port in your firewall that you configured for the WinRM HTTP listener. The default HTTPS port is 5985. For example
     ```
     netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow
     protocol=TCP localport=5985
     ```

  After the WinRM listener is running on your target Windows systems, XClarity Administrator can connect to these systems and perform the device driver updates.

Configuring a domain account for OS device-drivers updates

You can choose to use domain accounts to easily manage the privileges with a domain controller. To use a domain account when updating OS device drivers, you need to configure a domain account.

Before you begin

Ensure the managed Windows servers are in a domain network before configuring domain accounts.

When you add the Windows user account in Lenovo XClarity Administrator, use the format `USER@DOMAIN`. The format `DOMAIN/USER` is not supported.

Procedure

To configure a domain account, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Apply**. The Windows Driver Updates: Apply page is displayed.

Step 2. Click **All Actions → Manage Domain Account**. The Domain Accounts page is displayed.

Step 3. Click the **Create** icon ( ). to add a realm for the domain account. The Create Realm dialog is displayed.

Step 4. Specify a name and one or more key distribution center hosts names for the realm. Use the **Add** icon ( ) to add another host name and use **Remove** icon ( ) to remove a host name.

Step 5. Click **OK** to save the realm.

Step 6. From the Domain Accounts page, optionally select the realm to use by default.

Step 7. Click **Save** to save the configuration.

After you finish

You can perform the following actions from the Configure Domain Account page.

- Modify a selected realm by clicking the **Edit** icon ( ).
- Delete a selected realm by clicking the **Delete** icon ( )..

Configuring global Windows device-driver update settings

Global settings serve as defaults settings when Windows device-driver updates are applied.

About this task

From the Global Settings page, you can configure the following settings:
- Use HTTPS for Windows driver updates
- Show Device Drivers for installed hardware

Procedure

To configure the global settings to be used for all servers, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Apply**. The Windows Driver Updates: Apply page is displayed.

Step 2. Click **All Actions → Global Settings** to display the Global Settings: Apply Windows driver updates dialog.

Step 3. Optionally select the following options.

- Select **Use HTTPS for Windows driver updates** to use the Windows Remote Management service (WinRM) listening over HTTPS to run device-driver update commands on target Windows systems HTTPS is the default.

  Clear this setting to use HTTP.

  Attention: When using HTTP, Windows user credentials are sent over the network *without* encryption and can be easily viewed using commonly available network troubleshooting tools.
- Select **Show Device Drivers for installed hardware** to list only device drivers for managed hardware.

  Clear this setting to list all device drivers in each imported UpdateXpress System Packs (UXSPs) are listed.

  Important: After selecting this option, you must perform a compliance check by clicking the **Check Compliance** icon ( ) from the Windows Driver Updates: Apply page.

Step 4. Click **OK** to close the dialog.

Applying Windows device drivers

You can apply device drivers to managed servers running Windows.

Before you begin

- Lenovo XClarity Administrator uses the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems. The WinRM service must be correctly configured on the target servers before attempting to update OS device drivers (see Configuring Windows Server for OS device-driver updates).
- Devices that are not supported cannot be selected for updates.
- Read the device-driver update considerations before you attempt to update device drivers on your managed servers (see OS device-driver update considerations).
- Ensure that the repository contains the UXSPs and device drivers that you intend to deploy (see Downloading Windows device drivers).

  Note: When XClarity Administrator is initially installed, the catalog and repository are empty.
- XClarity Administrator can use the Windows Remote Management service (WinRM) listening over HTTPS or HTTP to run device-driver update commands on target Windows systems HTTPS is the default. To use HTTP, click **All Actions → Global Settings** on the Windows Driver updates: Apply page, and then clear **Use HTTPS for Windows driver updates**.

  Attention: When using HTTP, Windows user credentials are sent over the network *without* encryption and can be easily viewed using commonly available network troubleshooting tools.

  Important:

  – Ensure that Windows Remote Management (WinRM) on the target server is configured to use the same setting (HTTPS or HTTP) that is defined in XClarity Administrator (see Configuring Windows Server for OS device-driver updates).

  – Ensure that WinRM on the target server is configured with basic authentication.

  – When using HTTPS, ensure that WinRM on the target server is configured with **allowUnencrypted= false**.
- Ensure that PowerShell is supported on the target server.

- Ensure that the target server is powered on before attempting to update device drivers. If the server is not powered on, select the target server, and click **All Actions → Power Actions → Power On**.
- Ensure that XClarity Administrator has information that it needs to access the host operating system (see Managing access to operating-systems on managed servers.
- If you want to use a domain account when updating OS device drivers, ensure that you created the required configuration file (see Configuring a domain account for OS device-drivers updates).
- Ensure that no jobs are currently running on the target server. You cannot update device drivers on a managed server that is locked by a running job. If another update job is running on the target server, this update job is queued until the current update job completes. To see a list of active jobs, click **Monitoring → Jobs**.

About this task

XClarity Administrator updates only device drivers that are out of compliance. Device drivers are out of compliance when the version on the server is earlier than version in the selected UXSP. Device drivers that are equal to or later than version in the selected UXSP are skipped.

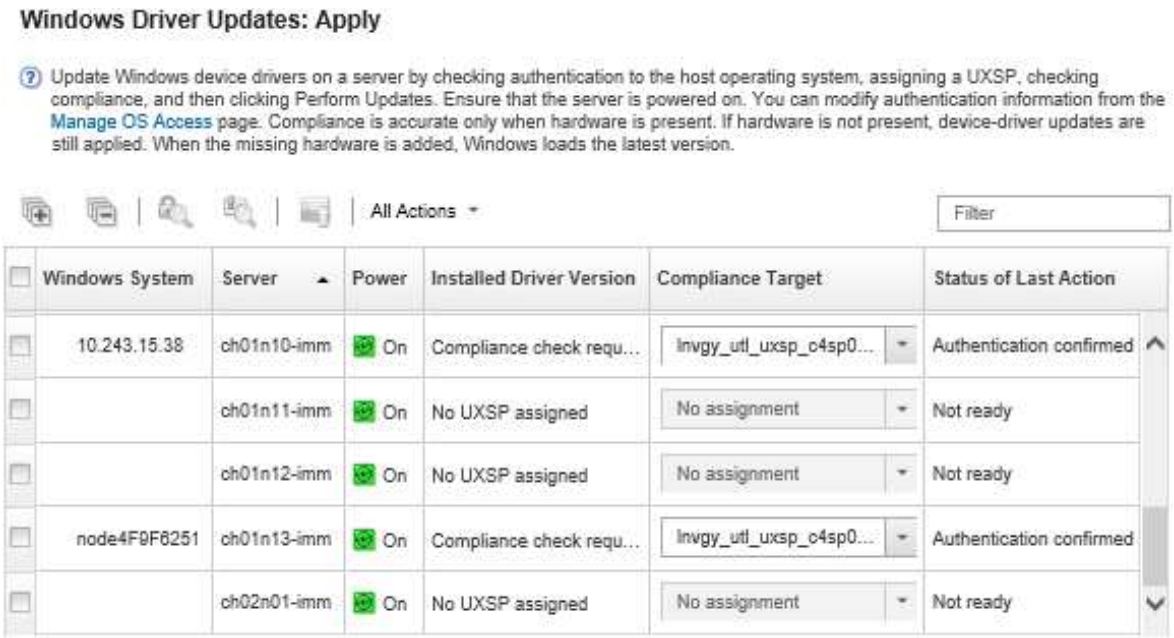
Procedure

To apply Windows device drivers to managed servers, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Windows Driver Updates: Apply** to display the Windows Driver Updates: Apply page.

Important:

- To discover the device drivers on the target server and determine compliance, you must select the target server and run the compliance check. After the compliance check is run for the first time, you can expand the row to see a list of device drivers on the target server.
- The **Windows System** column identifies the hostname or IP address of the host operating system.
- The **Server** column identifies the name and IP address of the managed server.



Step 2. Select one or more target servers and device drivers.

You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed servers by entering text (such as a name or IP address) in the **Filter** field.

Tip:

- You can choose to update all device drivers for a specific operating system, or you can expand an operating system and choose to update only specific devices
- The **Update Status** column shows the authentication status for each server and the update status for each device driver.
- The **OS Credential** column shows the stored credential that is used to authenticate to the operating system (for example, “901 – company\USER1.”

  If OS credentials are not defined for the host operating system on the target server, the Edit OS Credentials dialog is displayed. For a single target server, specify the user name and password that you want to use for this operation. For multiple target servers, select the stored credential to use for each server. Then, click **Save**.

  Note: The OS credentials that you select on the Edit OS Credentials dialog are not saved for the host operating system. To save OS credentials, see Managing access to operating-systems on managed servers.

Step 3. Click the **Check Authentication** icon ( ) to run authentication and prerequisite checks.

XClarity Administrator connects to the host operating system using the stored credential that is listed in the **OS Credential** column, determines the OS version, verifies that WinRM is enabled, performs additional prerequisite checks, and then disconnects from the host OS.

For information about changing the stored credential for the host operating system, see Managing access to operating-systems on managed servers.

Step 4. For each target server, select the target UXSP that you want to use to update device drivers from the **Compliance Target** column.

Step 5. Select the target servers again, and click the **Check Compliance** icon ( ) to verify the compliance of each device driver.

The compliance check updates the compliance status in the **Installed Driver Version** column. This column displays the overall compliance status for the server and the installed version and compliance status for each device driver as measured against the assigned UXSP.

- **Compliant**. The installed device driver is equal to or later than the version in the assigned UXSP.
- **Not compliant**. The installed device driver is earlier than the version in the assigned UXSP. You can click on the link to get more information about the non compliance.

Note: Device-driver compliance is accurate only when hardware is present. If hardware is not present, device drivers are still applied to the server. When the missing hardware is added to the server, Windows loads the latest version.

Step 6. Click the **Perform Updates** icon ( ).

Step 7. Select one of the following update rules.

- **Stop all updates on error**. If an error occurs while updating any of the device drivers on a target device, the update process stops for all target devices in the current device-driver update job. In this case, none of the device-driver updates in the UXSP for the target device are applied. The current device driver that is installed on all target devices remains in effect.

- **Continue on error**. If an error occurs while updating any of the device drivers on the target device, the update process does not update the device driver for that specific device; however, the update process continues to update other device drivers on the device and continues to update all other target devices in the current device-driver update job.
- **Continue to next system on error**. If an error occurs while updating any of the device drivers on the device, the -update process stops all attempts to update the device drivers for that specific device, so the current device drivers that are installed on that device remains in effect. The update process continues to update all other devices in the current device-driver update job.

Step 8. Click **Perform Updates** to update immediately, or click **Schedule** to schedule this update to run at a later time.

After you finish

When applying an update, if the target server fails to enter maintenance mode, attempt to apply the update again.

If updates were not completed successfully, see OS device-driver update considerations for troubleshooting and corrective actions.

From the Windows Driver Updates: Apply page, you can perform the following actions.

- View the status of the device-driver update directly from the Apply page in the **Update Status** column.
- Monitor the status of the device-driver update from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**.

  For more information about the jobs log, see Monitoring jobs.

  When the update job is complete, you can verify that the devices are compliant from the Windows Driver Updates: Apply page. The current driver version that is active on each device is listed in the **Installed Driver Version** column.

Chapter 15. Installing operating systems on bare-metal servers

You can use Lenovo XClarity Administrator to manage the OS images repository and deploy operating-system images to up to 28 bare-metal servers concurrently.

Learn more:

- XClarity Administrator: Bare metal to cluster
- XClarity Administrator: Operating-system deployment

Before you begin

After the 90-day free trial expires, you can continue to use XClarity Administrator to manage and monitor your hardware for free; however, you must purchase full-function-enablement licenses for each managed server that supports XClarity Administrator advanced functions to continue using the OS deployment function. Lenovo XClarity Pro provides entitlement to service and support and the full-function-enablement license. For more information about purchasing Lenovo XClarity Pro, contact your Lenovo representative or authorized business partner. For more information, see Installing the full-function enablement license in the XClarity Administrator online documentation.

About this task

XClarity Administrator provides a simple way to deploy operating-systems images to *bare-metal* servers, which typically do not have an operating system installed.

Attention: If you deploy an operating system to a server that has an operating system installed, XClarity Administrator performs a fresh installation that overwrites the partitions on the target disks

Several factors determine the amount of time that is required to deploy an operating system to a server:

- The amount of RAM that is installed in the server, which affects how long the server takes to start up.
- The number of and types of I/O adapters that are installed on the server, which affects the amount of time that it takes XClarity Administrator to perform an inventory of the server. It also affects the amount of time that it takes for the UEFI firmware to start when the server is started up. During an operating-system deployment, the server is restarted multiple times.
- Network traffic. XClarity Administrator downloads the operating-system image over the data network or the operating-system deployment network.
- The hardware configuration on the host on which Lenovo XClarity Administrator virtual appliance is installed. The amount of RAM, processors, and hard drive storage can affect download times.

Important: To deploy an operating-system image from XClarity Administrator, at least one of the XClarity Administrator interfaces (Eth0 or Eth1) must have IP network connectivity to the server network interface that is used to access the host operating system. Operating-system deployment uses the interface that is defined on the Network Access page. For more information about network settings, see Configuring network access.

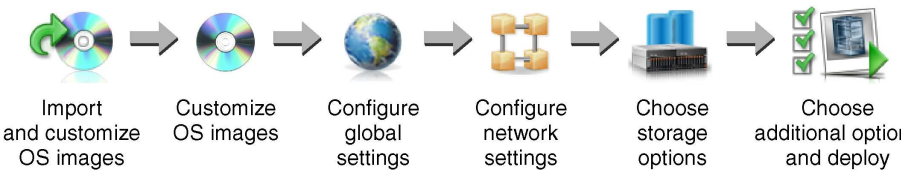
Before you perform a bare-metal operating-system deployment on a server, prepare the server by updating firmware to the latest levels and configuring the server using Configuration Patterns. For more information, see Updating firmware on managed devices and Configuring servers using configuration patterns.

Attention: It is recommended that you *do not* use XClarity Administrator to perform a bare-metal operating-system deployment on Converged and ThinkAgile appliances.

© Copyright Lenovo 2015, 2022

Procedure

The following figure illustrates the workflow for deploying an OS image to a server.



Step 1. **Import OS images.**

Before you can deploy an OS image to a server, you must first import the operating system into the repository. When you import an OS image, XClarity Administrator:

- Ensures that there is sufficient space in the OS images repository before importing the operating system. If you do not have sufficient space to import an image, delete an existing image from the repository and attempt to import the new image again.
- Creates one or more profiles of that image and stores the profile in the OS images repository. Each *profile* includes the OS image and installation options. For more information about predefined OS image profiles, see Operating-system image profiles.

A *base operating system* is the full OS image that was imported into the OS-images repository. The imported base image contains predefined profiles that describe the installation configurations for that image. You can create custom profiles in the base OS image that can be deployed for specific configurations.

You can also import supported *custom operating systems*. This custom image contains a predefined placeholder profile, which cannot be deployed. You must import a custom profile that can be deployed or create your own custom profile based on the placeholder profile. After the custom profile is added, the placeholder profile is removed automatically.

For Microsoft Windows Server 2016 and 2019, you can import a custom operating-system image for each release. The imported base image contains predefined profiles that describe the installation configurations for that image. You cannot create custom profiles in the custom OS image.

For a list of supported base and custom operating systems, see Supported operating systemsSupported operating systems in the Lenovo XClarity Administrator online documentation.

Step 2. **(Optional) Customize the OS image.**

You can customize an OS image by adding device drivers, boot files (for Windows only), configuration settings, unattend files, post-installation scripts, and software. When you customize a base OS image, XClarity Administrator creates a customized OS-image profile that includes the custom files and installation options.

The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Step 3. **Configure global settings.**

Global settings are configuration options that serve as defaults for operating system deployment. You can configure the following global settings.

- The password for the administrator user account to be used for deploying the operating systems
- The method to use to assign IP addresses to servers

- License keys to use when activating installed operating systems
- Optionally join an Active Directory domain as part of the Windows operating-system deployment

Step 4. **Configure network settings.**

You can specify the network settings for each server on which operating systems are to be deployed.

If you are using DHCP to assign IP addresses dynamically, you must configure the MAC address.

If you are using static IP addresses, you must configure the following network settings for a specific server before you can deploy an operating system to that server. After these settings are configured, the deployment status of the server changes to “Ready.” (Note that some fields are not available for static IPv6 addresses.)

- Hostname

  The hostname must comply with the following rules:
  – The hostname of each managed server must be unique.
  – The hostname can contain strings (labels) that are separated by a period (.).
  – Each label can contain ASCII letters, digits, and dashes (-); however, the string cannot start or end with a dash and cannot contain all digits.
  – The first label can be 2 - 15 characters in length. Subsequent labels can be 2 – 63 characters in length.
  – The total length of the hostname must not exceed 255 characters.
- MAC address of the port on the host where the operating system is to be installed.

  The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment.

  You can determine the status of the MAC address port that is used for OS deployment from the **MAC address** drop-down menu on the Network Settings dialog. If multiple ports are up or if all ports are down, AUTO is used by default.

  Notes:

  – Virtual network ports are not supported. Do not use one physical network port to simulate multiple virtual network ports.
  – When the server's network setting is set to AUTO, XClarity Administrator can automatically detect network ports in slots 1 – 16. At least one port in slots 1 – 16 must have a connection to XClarity Administrator.
  – If you want to use a network port in slot 17 or greater for the MAC address, you cannot use AUTO. Instead, you must set the server's network setting to the MAC address of the specific port that you want to use.
  – For ThinkServer servers, not all host MAC addresses are displayed. In most cases, MAC addresses for AnyFabric Ethernet adapters are listed on the Edit Network Settings dialog. MAC addresses for other Ethernet adapters (such as the Lan-On-Motherboard) are not listed. In cases where the MAC address for an adapter is not available, use the AUTO method for non-VLAN deployments.
- IP address and subnet mask
- IP gateway
- Up to two domain name system (DNS) servers

- Maximum transmission unit (MTU) speed
- VLAN ID, if VLAN IP mode is enabled

If you choose to use VLANs, you can assign a VLAN ID to the host network adapter that is being configured.

Step 5. **Choose the storage options**

For each deployment, you can choose the preferred storage location where the operating system is to be deployed. Depending on the operating system, you can choose to deploy to a local disk drive, embedded hypervisor key, or SAN.

Step 6. **Choose additional options and custom configuration settings, and deploy the OS image.**

You can configure additional deployment options, such as the license key for the OS deployment, and custom configuration settings. If you are installing Microsoft Windows, you can also configure the Active Directory domain to join.

Notes:

- If you defined custom configuration settings for a specific custom OS profile, you must define values for required custom configuration settings before you can deploy the profile to a server.
- When deploying a custom OS profile that includes custom settings, all target servers must use the same custom OS profile and the values for the custom settings apply to all target servers.

You can then choose the target servers for deployment and the OS images to be deployed. Remember that to deploy an operating system, the server must be have a deployment status of “Ready.”

You can deploy operating-system images on up to 28 servers concurrently.

Before you attempt to deploy an operating-system image, review the Operating-system deployment considerations.

Operating-system deployment considerations

Before you attempt to deploy an operating-system image, review the following considerations.

Lenovo XClarity Administrator considerations

- Ensure that no jobs are currently running on the target server. To see a list of active jobs, click **Monitoring → Jobs**.
- Ensure that the target server does not have a deferred or partially activated server pattern. If a server pattern has been deferred or partially activated on the managed server, you must restart the server to apply all configuration settings. Do not attempt to deploy an operating system to a server with a partially activated server pattern. To determine the configuration status of the server, see the **Configuration Status** field on the Summary page for the managed server (see Viewing the details of a managed server).
- Ensure that a password for the administrator account that is to be used to deploy the operating system is specified on the Global Settings: Deploy Operating Systems dialog. For more information about setting the password, see Configuring global OS-deployment settings.
- Ensure that the global default settings are correct for this operating-system deployment (see Configuring global OS-deployment settings).

Operating system considerations

- Ensure that you have all applicable operating-system licenses to activate the installed operating systems. You are responsible for obtaining licenses directly from the operating-system manufacturer.
- Ensure that the operating-system image that you intend to deploy is already loaded in the OS images repository. For information about importing images, see Importing operating-system images.
- Operating-system images in the XClarity Administrator repository might not be supported only on certain hardware platforms. Only OS-image profiles that are supported by the selected server are listed on the Deploy OS Images page. You can determine whether an operating system is compatible with a specific server from the Lenovo OS Interoperability Guide website.
- For Windows, you must import a boot file into the OS-images repository before you can deploy a Windows profile. Lenovo bundles the predefined WinPE_64.wim boot file along with a set of device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Because the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Files** tab.
- For SLES 15 and 15 SP1, you must import both the installer image and the associated package image from the Server OS Support Center webpage. For SLES 15 SP2 or later, you need to import only the Full Installation Media image because the Unified Installer and Packages DVDs from SUSE Linux Enterprise Server 15 and 15 SP1 are deprecated.
- For ThinkSystem servers, XClarity Administrator includes out-of-box device drivers to enable the installation of the operating system as well as basic network and storage configuration for the final operating system. For other servers, ensure that the operating-system image that you intend to deploy includes the appropriate Ethernet, Fibre Channel, and storage adapter device drivers for your hardware. If the I/O adapter device driver is not included in the operating system, the adapter is not supported for OS deployment. Always install the latest operating system to ensure that you have the latest inbox I/O adapter device drivers and boot files that you need. You can also add out-of-box device drivers and boot files to operating systems that have been imported into XClarity Administrator (see Customizing OS-image profiles in the XClarity Administrator online documentation).

  For VMware, use the latest Lenovo Custom Image for ESXi, which includes support for the latest adapters. For information about obtaining that image, see the VMware Support – Downloads webpage.
- For ThinkSystem servers, if you want to deploy SLES 12 SP2, you must use a kISO profile. To get the kISO profiles, you must import the appropriate SLES kISO image after you import the base SLES operating system. You can download the SLES kISO image from the Linux Support – Downloads webpage.

  Notes:

  – The SLES kISO image counts towards the maximum number of imported OS images.

    For a list of supported base and custom operating systems, see Supported operating systemsSupported operating systems in the Lenovo XClarity Administrator online documentation.

  – If you delete all kISO profiles, you must delete the base SLES operating system and then import the base operation system and kISO image again to deploy SLES 12 SP2 on a ThinkSystem server.

  – If you create a custom OS-profile based on a kISO profile, the predefined device drivers in the base operating system are not included. The device drivers that are included in the kISO are used instead. You can also add device drivers to the custom OS-profile (see Creating a custom OS-image profile).

For more information about limitations for specific operating systems, see Supported operating systems.

Network considerations

- Ensure that all required ports are open (see Port availability for deployed operating systems).

- Ensure that XClarity Administrator can communicate with the target server (both the baseboard management controller and the servers' data network) over the interface (Eth0 or Eth1) that was selected when you configured the XClarity Administrator network access.

  To specify an interface to be used for operating-system deployment, see Configuring network access).

  For more information about the operating-system deployment network and interfaces, see Network considerations in the XClarity Administrator online documentation.
- Ensure that the IP addresses are unique for the host operating system. XClarity Administrator checks for duplicate IP addresses that you specify for the network address during the deployment process.
- If the network is slow or unstable, you might see unpredictable results when deploying operating systems.
- The XClarity Administrator network interface that is used for management must be configured to connect to the baseboard management controller using the same IP address method that you choose on the Global Settings: Deploy Operating Systems dialog. For example, if XClarity Administrator is set up to use eth0 for management, and you choose to use manually assigned static IPv6 addresses when configuring the deployed OS, then eth0 must be configured with an IPv6 address that has connectivity to the baseboard management controller.
- If you choose to use IPv6 addresses for the OS deployment global settings, the IPv6 address for XClarity Administrator must be routable to the baseboard management controller and the servers' data network.
- IPv6 mode is not supported for ThinkServer (see IPv6 configuration limitations in the XClarity Administrator online documentation).
- If you are using DHCP to assign IP addresses dynamically, you must configure the MAC address.
- If you are using static IP addresses, you must configure the following network settings for a specific server before you can deploy an operating system to that server. After these settings are configured, the deployment status of the server changes to "Ready." (Note that some fields are not available for static IPv6 addresses.)
  - Hostname

    The hostname must comply with the following rules:
    - The hostname of each managed server must be unique.
    - The hostname can contain strings (labels) that are separated by a period (.).
    - Each label can contain ASCII letters, digits, and dashes (-); however, the string cannot start or end with a dash and cannot contain all digits.
    - The first label can be 2 - 15 characters in length. Subsequent labels can be 2 – 63 characters in length.
    - The total length of the hostname must not exceed 255 characters.
  - MAC address of the port on the host where the operating system is to be installed.

    The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment.

    You can determine the status of the MAC address port that is used for OS deployment from the **MAC address** drop-down menu on the Network Settings dialog. If multiple ports are up or if all ports are down, AUTO is used by default.

    Notes:

    - Virtual network ports are not supported. Do not use one physical network port to simulate multiple virtual network ports.
    - When the server's network setting is set to AUTO, XClarity Administrator can automatically detect network ports in slots 1 – 16. At least one port in slots 1 – 16 must have a connection to XClarity Administrator.

  - If you want to use a network port in slot 17 or greater for the MAC address, you cannot use AUTO. Instead, you must set the server's network setting to the MAC address of the specific port that you want to use.
  - For ThinkServer servers, not all host MAC addresses are displayed. In most cases, MAC addresses for AnyFabric Ethernet adapters are listed on the Edit Network Settings dialog. MAC addresses for other Ethernet adapters (such as the Lan-On-Motherboard) are not listed. In cases where the MAC address for an adapter is not available, use the AUTO method for non-VLAN deployments.
- IP address and subnet mask
- IP gateway
- Up to two domain name system (DNS) servers
- Maximum transmission unit (MTU) speed
- VLAN ID, if VLAN IP mode is enabled

- If you choose to use VLANs, you can assign a VLAN ID to the host network adapter that is being configured.

For more information about the operating-system deployment network and interfaces, see Configuring network settings for managed servers and Configuring network settings for managed servers and Network considerations in the XClarity Administrator online documentation.

Storage and boot-option considerations

- Ensure that the UEFI boot option on the target server is set to “UEFI boot only” before you deploy an operating system. The “Legacy-only” and “UEFI first, then legacy” boot options are not supported for operating-system deployment.
- Each server must have a hardware RAID adapter that is installed and configured.

  Attention:

  - Only storage that is set up with hardware RAID is supported.
  - The software RAID that is typically present on the onboard Intel SATA storage adapter or storage that is set up as JBOD are not supported; however, if a hardware RAID adapter is not present, setting the SATA adapter to **AHCI SATA mode** enabled for operating-system deployment or setting unconfigured good disks to JBOD might work in some cases. For more information, see OS installer cannot find the disk on which you want to install XClarity Administrator in the XClarity Administrator online documentation.

    This exception does not apply to M.2 drives.
  - If a managed device has both local drives (SATA, SAS, or SSD) that are not configured for hardware RAID and M.2 drives, you must disable the local drives if you want to use M.2 drives, or you must disable the M.2 drives if you want to use local drives. You can disable on-board storage controller devices and legacy and UEFI storage option ROMs using the using Configuration Patterns by selecting Disable local disk on the Local Storage tab of the wizard or by creating a Configuration Pattern from an existing server and then disabling the M.2 devices in the extended UEFI pattern.
  - If a SATA adapter is enabled, the SATA mode *must not* be set to “IDE.”
- The NVMe storage that is connected to a server motherboard or HBA controller is not supported and must not be installed in the device; otherwise, OS deployment to non-NVMe storage will fail.
- When deploying RHEL, multi ports that are connected to same LUN on the target storage is not supported.
- Ensure that secure-boot mode is disabled for the server. If you are deploying a secure-boot mode enabled operating system (such as Windows), disable secure-boot mode, deploy the operating system, and then re-enable secure-boot mode.

- When deploying Microsoft Windows to a server, attached drives must not have existing system partitions (see OS deployment fails due to existing system partitions on an attached disk drive in the XClarity Administrator online documentation).
- For ThinkServer servers, ensure that the following requirements are met:
  - The boot settings on the server must include a Storage OpROM Policy that is set to `UEFI Only`. For more information, see OS installer cannot boot on a ThinkServer server - XClarity Administrator in the XClarity Administrator online documentation.
  - If you are deploying ESXi and there are network adapters that are PXE bootable, disable PXE support on the network adapters before deploying the operating system. The deployment is completed, you can re-enable PXE support, if desired.
  - If you are deploying ESXi and there are bootable devices in the boot-order list other than the drive on which the operating system is to be installed, remove the bootable devices from the boot-order list before deploying the operating system. After deployment is complete, you can add the bootable device back to the list. Ensure that the installed drive is at the top of the list.

For more information about storage-location settings, see Choosing the storage location for managed servers.

Managed-device considerations

- For information about operating-system deployment limitations for specific devices, see Supported hardware in the XClarity Administrator online documentation.
- Ensure there is no mounted media (such as ISOs) on the target server. Additionally, ensure there are no active Remote Media sessions open to the management controller.
- Ensure that the timestamp in BIOS is set to the current date and time.
- For ThinkSystem and System x servers, ensure that the Legacy BIOS option is disabled. From the BIOS/UEFI (F1) Setup utility, click **UEFI Setup → System Settings**, and verify that Legacy BIOS is set to Disabled.
- For Flex System servers, ensure that the chassis is powered on.
- For Converged, NeXtScale, and System x servers, ensure that a Feature on Demand (FoD) key for remote presence is installed. You can determine whether remote presence is enable, disabled, or not installed on a server from the Servers page (see Viewing the status of a managed server). For more information about FoD keys that are installed on your servers, see Viewing Features on Demand keys.
- For ThinkSystem servers and ThinkAgile appliances, the XClarity Controller Enterprise feature is required for operating-system deployment. For more information, see Viewing Features on Demand keys.
- For Converged and ThinkAgile appliances, it is recommended that you *do not* use XClarity Administrator to perform a bare-metal operating-system deployment.

Supported operating systems

Lenovo XClarity Administrator supports the deployment of several operating-systems. Only supported versions of the operating systems can be loaded into the XClarity Administrator OS images repository.

Important:

- For information about operating-system deployment limitations for specific devices, see Supported hardware in the XClarity Administrator online documentation.
- The cryptographic management feature of XClarity Administrator allows limiting communication to certain minimum SSL/TLS modes. For example, if TLS 1.2 is selected, then only operating systems with an installation process that supports TLS 1.2 and strong cryptographic algorithms can be deployed through XClarity Administrator.

- Operating-system images in the XClarity Administrator repository might not be supported only on certain hardware platforms. Only OS-image profiles that are supported by the selected server are listed on the Deploy OS Images page. You can determine whether an operating system is compatible with a specific server from the Lenovo OS Interoperability Guide website.
- For OS and Hypervisor related compatibility and support information and resources for Lenovo servers and solutions, see the Server OS Support Center webpage.

The following table lists the 64-bit operating systems that XClarity Administrator can deploy.

Operating system	Versions	Notes
CentOS Linux	7.2 and later 8.0 8.1 8.2	**Notes:** • All existing and future minor versions are supported unless otherwise noted. • DHCP, static IPv4, and static IPv6 address are supported. • VLAN tagging is not supported. • Out-of-box drivers are not supported. • OS profile customization is not supported. • CentOS 8.3 is not supported.
Microsoft® Windows® Azure Stack HCI	20H2 21H2	OS profile customization is not supported.
Microsoft Windows Hyper-V Server	2016	
Microsoft Windows Server	2012 R2 2012 R2U1 2016 2019 2022	Both the retail and volume license copies are supported. **Note:** XClarity Administrator is tested with only Windows versions that are supported by Microsoft at the time when the XClarity Administrator version was released. The following are *not supported*: • Windows Reseller Option Kit (ROK) • Windows Server Semi-Annual Channel (SAC) v1709, v1803, and v1809 • Windows Server 2019 Essentials • Windows Server 2016 Nanoserver • Windows Server 2012 Evaluation Copy • Windows Server images to managed servers with embedded hypervisor keys Windows Server 2012 R2 on servers that contain Intel CLX processors You must physically remove the embedded hypervisor key from the target servers before deploying a Windows image. This includes Hyper-V through one of the virtualization profiles. – Datacenter – Datacenter Core – Datacenter Virtualization (Hyper-V) – Datacenter Virtualization Core (Hyper-V with Core) – Standard – Standard Core – Standard Virtualization (Hyper-V) – Standard Virtualization Core (Hyper-V with Core)

Operating system	Versions	Notes
Red Hat® Enterprise Linux (RHEL) Server	6.8 and later 7.2 and later 8.x	Includes KVM **Notes:** • All existing and future minor versions are supported unless otherwise noted. • When importing the DVD version of the OS image, only DVD1 is supported. • When installing RHEL on ThinkSystem servers, RHEL v7.4 or later is recommended. • To deploy RHEL 7.2, the global IP-assignment must be set to use IPv4 addresses. For information about global settings, see Configuring global OS-deployment settings. • OS deployment failures have been observed on IPv6 networks with lower bandwidths due to timeouts in the OS installer.
SUSE® Linux Enterprise Server (SLES)	12.x 15.x	Includes KVM and Xen hypervisors **Notes:** • All existing and future service packs are supported unless otherwise noted. • When importing the DVD version of the OS image, only DVD1 is supported. • OS deployment failures have been observed on IPv6 networks with lower bandwidths due to time outs in the OS installer. • If you want to deploy SLES 12 SP2 on a ThinkSystem server, you must use a kISO profile. To get the kISO profiles, you must import the appropriate SLES kISO image. For more information, see Operating-system deployment considerations. • For SLES 15 and 15 SP1, you must import both the installer image and the associated package image from the Server OS Support Center webpage. For SLES 15 SP2 or later, you need to import only the Full Installation Media image because the Unified Installer and Packages DVDs from SUSE Linux Enterprise Server 15 and 15 SP1 are deprecated.

Operating system	Versions	Notes
Ubuntu Server	20.04.x	**Notes:** • The image can be installed on the selected storage option (local disk drive, M.2 drive, or FC SAN volume). • All existing and future minor versions are supported unless otherwise noted. • Only DHCP is supported. Static IPv4 and static IPv6 address *are not* supported. • VLAN tagging *is not* supported. • Out-of-box drivers *are not* supported. • OS profile customization *is not* supported.
VMware vSphere® Hypervisor (ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x	Base VMware vSphere Hypervisor (ESXi) images and Lenovo VMware ESXi Custom images are supported. Lenovo VMware ESXi Custom images are customized for select hardware to give you online platform management, including updating and configuring firmware, platform diagnostics, and enhanced hardware alerts. Lenovo management tools also support simplified management of the ESXi with select System x servers. This image is available for download from the VMware Support – Downloads webpage. The license that is provided with the image is a 60-day free trial. You are responsible for meeting all VMware licensing requirements. **Important:** • All existing and future update packs are supported for 6.0, 6.5, 6.7, and 7.0 unless otherwise noted. • Base ESXi images (without Lenovo customization) include only basic in-box device drivers for network and storage. The base image does not include the out-of-box device drivers (which are included in Lenovo VMware ESXi Custom images). You can add out-of-box device drivers by creating your own custom OS0image profiles (see Customizing OS-image profiles). • For some versions of Lenovo VMware ESXi Custom images, separate images might be available for System x, ThinkSystem, and ThinkServer. Only one image for a specific release can exist in the OS-images repository at a time. • ESXi deployment is not supported for certain older servers. For information about which servers are supported, see the Lenovo OS Interoperability Guide website. • The following versions are supported for ThinkServer devices: ESXi 6.0u3, 6.5 and later. • During the installation of ESXi 5.5 (any update), or 6.0 onto a server in a Flex System chassis, the server might become unresponsive or restart shortly after the following message: `Loading image.pld` • ESXi 5.5 requires Memory Mapped I/O (MMIO) space to be configured within the initial 4 GB of the system. Depending on the configuration, certain systems attempt to use memory higher than 4 GB, which can cause a failure. To resolve the issue, see VMware deployment causes system hang or restart in the XClarity Administrator online documentation. • When deploying ESXi using a static IPv6 mode, the hostname that is defined on the Network Settings page in XClarity Administrator is not configured in the deployed ESXi instance. Instead, the default hostname `localhost` is used. You must manually set the hostname in the deployed ESXi to match the hostname that is defined in XClarity Administrator.

Operating system	Versions	Notes
		• When deploying ESXi on a managed server, the operating system does not explicitly move the drive on which the operating system is installed to the top of the boot-order list. If a boot device containing a bootable OS or a PXE server is specified before the boot device containing ESXi, then ESXi does not boot. For ESXi deployment, XClarity Administrator updates the boot-order list for most servers to ensure the ESXi boot device is at the top of the boot-order list; however, ThinkServer servers do not provide a way for XClarity Administrator to update the boot-order list. You must disable PXE boot support or remove bootable devices other than the installation drive before deploying the operating system. For more information, see Operating system does not boot after deploying ESXi on a ThinkServer server in the XClarity Administrator online documentation. **Tip:** Instead of setting **MM Config** through the Setup utility for each server, consider using one of the predefined extended UEFI patterns that are related to virtualization, which sets the MM Config option to 3 GB and disables the PCI 64-bit resource allocation. For more information about these patterns, see Defining extended UEFI settings.

Operating-system image profiles

When you import an OS image into the OS images repository, Lenovo XClarity Administrator creates one or more profiles for that image and stores the profiles in the OS images repository. Each predefined *profile* includes the OS image and installation options for that image.

OS image profile attributes

OS image profile attributes provide additional information about an OS-image profile. The following attributes can be shown.

- **kISO**. You must use a kISO profile to deploy SLES 12 SP2 to a ThinkSystem server. You can download the SLES kISO image from the Linux Support – Downloads webpage.

Predefined OS image profiles

The following table lists the profiles that are predefined by XClarity Administrator when you import an operating-system image. This table also lists the packages that are included in each profile.

You can create a customized OS image profile for a base operating system. For more information, see Customizing OS-image profiles.

Operating system	Profile	Packages included in the profile

CentOS Linux	Basic	`@X Window System`
		`@Desktop`
		`@Fonts`
		`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`

	Minimal	`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`

Operating system	Profile	Packages included in the profile	
	Virtualization	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Microsoft® Windows® Azure Stack HCI	Azure	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="Containers" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	
Microsoft Windows Hyper-V Server 2016	Hyper_V	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	
Microsoft Windows Server **Note:** Includes Hyper-V through the *Virtualization Profile*.	Datacenter	GUI	
	Datacenter virtualization	GUI Hyper-V role	
	Datacenter virtualization core	Hyper-V role	
	Datacenter core		
	Standard	GUI	
	Standard virtualization	GUI Hyper-V role	

Operating system	Profile	Packages included in the profile	
	Standard virtualization core	Hyper-V role	
	Standard core		
Customized Microsoft Windows Server	Datacenter_ customized		
	Standard_ customized		
Red Hat Enterprise Linux (RHEL) **Note:** Includes KVM	Basic	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Minimal	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualization	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms

Operating system	Profile	Packages included in the profile
SUSE Linux Enterprise Server (SLES) 12	Basic and Basic with kISO	<pattern>32bit</pattern> <pattern>Basis-Devel</pattern> <pattern>Minimal</pattern> <pattern>WBEM</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>gateway_server</pattern> <pattern>lamp_server</pattern> <pattern>mail_server</pattern> <pattern>ofed</pattern> <pattern>printing</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	Minimal and Minimal with kISO	<pattern>Minimal</pattern> <pattern>file_server</pattern> <pattern>sap_server</pattern>
	Virtualization-KVM and Virtualization-KVM with kISO	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>kvm_server</pattern> <pattern>kvm_tools</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	Virtualization-Xen and Virtualization-Xen with kISO	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern>
SUSE Linux Enterprise Server (SLES) 15	Basic and Basic	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>

Operating system	Profile	Packages included in the profile
	Minimal and Minimal	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Virtualization-KVM and Virtualization-KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
	Virtualization-Xen and Virtualization-Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
Ubuntu	Minimal	Openssh-server
	Virtualization	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
VMware vSphere® Hypervisor (ESXi)	Virtualization	Base VMware vSphere Hypervisor (ESXi) images and Lenovo VMware ESXi Custom images are supported.

Port availability for deployed operating systems

Some ports are blocked by certain operating-system profiles. The following tables list the ports that are open (not blocked).

Ensure that the hypervisor that is running the Lenovo XClarity Administrator appliance allows network traffic (TCP/UDP) on ports 139, 445, 3001, 3900, 8443. These are required for operating-system deployment.

RHEL Virtualization profile

By default, the Red Hat Enterprise Linux (RHEL) Virtualization profile blocks all ports except for those that are listed in the following table.

Table 8. Port availability for RHEL Virtualization profiles

Port	TCP or UDP	Direction	Communication description
22	TCP	Inbound	SSH communication
53	TCP, UDP	Outbound/Inbound	Communication with RHEL KVM networking devices
67	TCP, UDP	Outbound/Inbound	Communication with RHEL KVM networking devices
161	UDP	Outbound	Communication with SNMP agents
162	UDP	Inbound	Communication with SNMP agents
427	TCP, UDP	Outbound/Inbound	Communication with SLP service agent, SLP directory agent
3001	TCP	Outbound/Inbound	Communication with management software image-deployment service
15988	TCP	Outbound	CIM-XML over HTTP communication
15989	TCP	Outbound	CIM-XML over HTTP communication
49152 - 49215	TCP	Outbound/Inbound	KVM Virtual Server communication

RHEL Basic and Minimal profiles

By default, the RHEL Basic and Minimal profiles block all ports except for those that are listed in the following table.

Table 9. Port availability for RHEL Basic and Minimal profiles

Port	TCP or UDP	Direction	Communication description
22	TCP	Inbound	SSH communication
3001	TCP	Outbound/Inbound	Management software image-deployment service communication

SLES Virtualization, Basic, and Minimal profiles

For SUSE Linux Enterprise Server (SLES), some open ports are dynamically assigned based on the operating system version and profiles. For a complete list of open ports, see your SUSE Linux Enterprise Server documentation.

VMware ESXi Virtualization profile

For a complete list of open ports for VMware vSphere Hypervisor (ESXi) with Lenovo customization, see the VMware documentation for ESXi on the VMware Knowledge Base website.

Windows profiles

The following ports must be available for Windows profiles.

Table 10. Port availability for Windows profiles

Port	TCP or UDP	Direction	Communication description
137	UDP	Outbound/Inbound	NetBIOS Name Service
138	UDP	Outbound/Inbound	NetBIOS Datagram
139	TCP	Outbound/Inbound	NetBIOS Session
445	TCP	Outbound/Inbound	SMB over TCP

Configuring a remote file server

You can import OS images, device drivers, and boot files into the OS images repository from the local system or from a remote file server. To import files from a remote file server, you must first create a profile that is used to authenticate the connection to the remote file server.

About this task

The following cryptographic algorithms are supported:
- RSA–2048 bits
- RSA–4096 bits
- ECDSA–521 bits (secp521r1 curve)

The following protocols are supported:
- HTTP with no authentication.
- HTTP with basic authentication.
- HTTPS (certificate validation) with basic authentication.
- HTTPS (certificate validation) with no authentication.
- FTP with password authentication.
- SFTP (client validation) with password authentication.
- SFTP (client validation) with public-key authentication

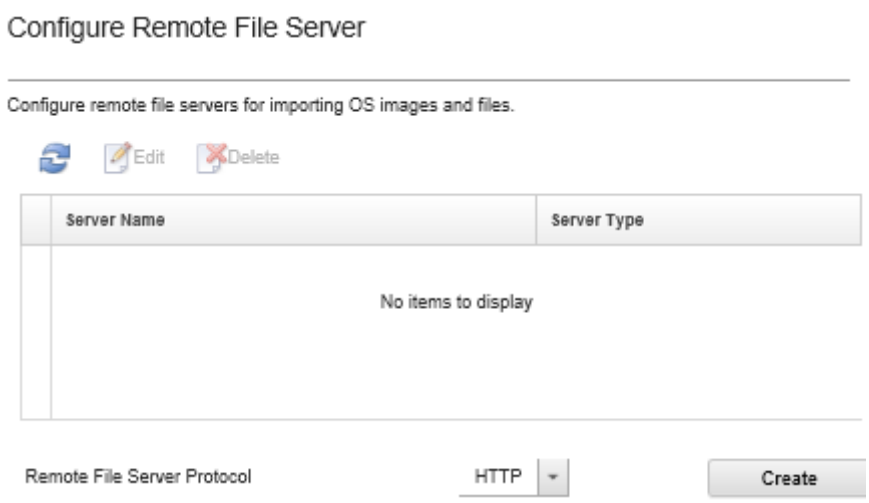
For SFTP public key authentication and HTTPS certificate validation, Lenovo XClarity Administrator validates that the remote file server' certificate. If the server certificate is not in the trust store, you are prompted to accept the server certificate and add it to the trust store. For information about troubleshooting validation issues, see Server certification validation fails in the XClarity Administrator online documentation.

Procedure

To configure a remote file server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS images** to display the Deploy Operating System: Manage OS images page.

Step 2. Click the **Configure File Server** icon ( ) to display the Configure Remote File Server dialog.



Step 3. Select the protocol for the remote file server from the **Remote File Server Protocol** list.

Step 4. Click **Create**. The Configure Remote File Server dialog is displayed.

Note: This dialog differs depending on the protocol that you selected.

Step 5. Enter the server name, address, and port.

Step 6. For HTTP, HTTPS, FTP, and SFTP with basic authentication, enter a user name and password if authentication is required to access the server.

Step 7. For SFTP with basic authentication, click **Validate Server Certificate** to obtain the public key signature.

Note: A dialog might be displayed informing you that the OS deployment process does not trust the public key of the SFTP file server. Click **OK** to store and trust the SFTP public key in the OS deployment trusted key store. If successful, the public key signature is shown in the **SFTP Server Public Key Signature** field.

Step 8. For SFTP with public-key authentication:

a. Enter a key passphrase and password and select the key type if authentication is required to access the server.

b. Click **Generate Management Server Key** to obtain the public-key signature.

c. Copy the generated key to the authorized_keys file in your SFTP remote file server.

d. Select the **The Management key was copied onto the server** checkbox in XClarity Administrator.

e. Click **Validate Server Certificate** to validate the public key signature.

Note: A dialog might be displayed informing you that the OS deployment process does not trust the public key of the SFTP file server. Click **OK** to store and trust the SFTP public key in the OS deployment trusted key store. If successful, the public key signature is shown in the **SFTP Server Public Key Signature** field.

f. Click **Save**.

Step 9. Click **Save Server**.

After you finish

From the Configure Remote File Server dialog, you can perform the following actions:

- Refresh the list of remote file server by clicking the **Refresh** icon ( ).

- Modify a selected remote file-server by clicking the **Edit** icon ( ).
- Remove a selected remote file server by clicking the **Delete** icon ( ).

Importing operating-system images

Before you can deploy a licensed operating system to managed servers, you must import the image into the XClarity Administrator OS images repository.

About this task

For information about operating system images that you can import and deploy, see Supported operating systems.

For a list of supported base and custom operating systems, see Supported operating systemsSupported operating systems in the Lenovo XClarity Administrator online documentation.

You can import only one image at a time. Wait until the image is displayed in the OS images repository before attempting to import another image. Importing the operating system might take a while.

For ESXi only, you can import multiple ESXi images with same major/minor version to the OS images repository.

For ESXi only, you can import multiple customized ESXi images with same major/minor version and build number to the OS images repository.

When you import an operating system image, XClarity Administrator:

- Ensures that there is sufficient space in the OS images repository before importing the operating system. If you do not have sufficient space to import an image, delete an existing image from the repository and attempt to import the new image again.
- Creates one or more profiles of that image and stores the profile in the OS images repository. Each *profile* includes the OS image and installation options. For more information about predefined OS image profiles, see Operating-system image profiles.

Note: Internet Explorer and Microsoft Edge web browsers have an upload limit of 4 GB. If the file that you are importing is greater than 4 GB, consider using another web browser (such as Chrome or Firefox) or copy the file to a remote file server and import using the **Remote import** option.

Procedure

To import an operating-system image into the OS images repository, complete the following steps.

Step 1. Obtain a licensed ISO image of the operating system.

Note: You are responsible for obtaining applicable licenses for the operating system.

Step 2. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating Systems: Manage OS Images page.

Step 3. Click the **Import Files** icon ( ) to display the Import OS Images and Files dialog.

Step 4. Click the **Local** tab to upload files from the local system, or click the **Remote** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote-file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Enter the path and ISO-image file name, or click **Browse** to find the ISO image that you want to import.

If you chose to use the *local file server*, you must enter the absolute path to the ISO-image file. If you chose to use a *remote file server*, you must enter the absolute path (for example, `/home/user/isos.osimage.iso`) or relative path (for example, `/isos.osimage.iso`) to the ISO-image file (depending on the configuration of the remote file server). If the file is not found, verify that the path to the file is correct, and try again.

Step 7. Optional: **Optional:** Enter a description for the OS image.

Step 8. Optional: **Optional:** Select a checksum type to verify that the ISO image being imported into XClarity Administrator is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded OS image. The value must come from a secure source from an organization that you trust. If the uploaded image matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the image again or check the checksum value.

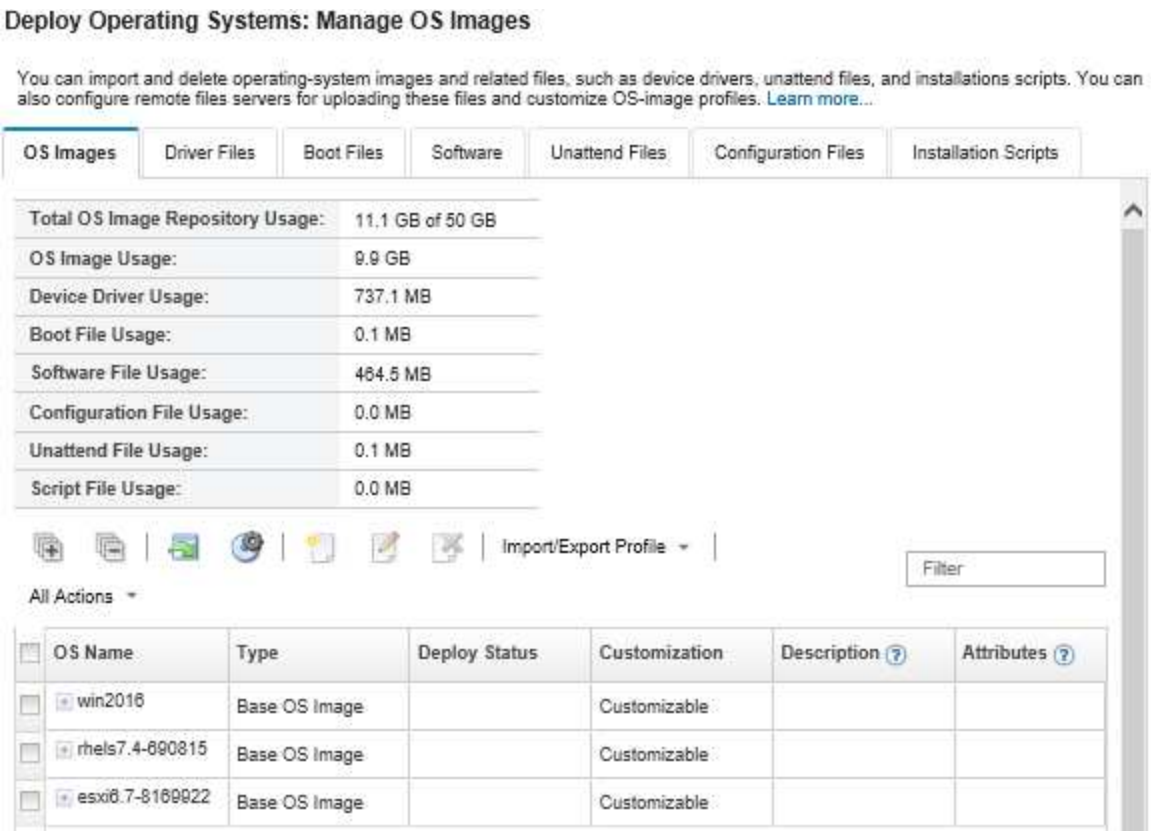
Three checksum types are supported:
- **MD5**
- **SHA1**
- **SHA256**

Step 9. Click **Import**.

Tip: ISO image is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the image. If you close the web browser tab or window in which the operating-system image is being uploaded before the upload completes, the import fails.

Results

XClarity Administrator uploads the OS image and creates an image profile in the OS images repository.



From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).
- Customize an OS image by clicking the **Create Customized Profile** icon ( ).
- Modify an OS image by clicking the **Edit** icon ( ).
- Import a customized OS image profile and apply to a base OS image by clicking **Import/Export Profile → Import Customized Profile Image** (see Importing a customized OS image profile).
- Delete a selected OS image or customized OS image profile by clicking the **Delete** icon ( ).
- Export a selected customized OS image profile by clicking **Import/Export Profile → Export Customized Profile Image**.

Note: When importing Windows Server images, you must also import the associated bundle file. Lenovo bundles the predefined WinPE_64.wim boot file along with a set of device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Because the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Files** tab.. For more information, see Importing boot files and Importing device drivers.

Customizing OS-image profiles

A *base operating system* is the full OS image that was imported into the OS-images repository. The imported base image contains predefined profiles that describe the installation configurations for that image. You can also create custom profiles in the base OS image that can be deployed for specific configurations. The custom profile contains the custom files and installation options.

Note: You cannot create a custom OS-image profile for a custom Microsoft Windows Server image.

Several example scenarios for customizing and deploying OS-images, including Windows and SLES, are available in English only. For more information, see End-to-end scenarios for setting up new devices.

You can add the following types of files to a custom OS image profile.

- **Boot files**

  A boot file acts as the bootstrap install environment. For Windows, this is a Windows Pre-installation (WinPE) file. A WinPE boot file is required to deploy Windows

  Lenovo XClarity Administrator supports predefined and custom boot files.

  – **Predefined boot files**. Lenovo provides a WinPE_64.wim boot file that can be used to deploy predefined OS-image profiles.

    Lenovo bundles the predefined WinPE_64.wim boot file along with a set of device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Because the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Files** tab.

    Notes:

    – A predefined boot file is not preloaded with XClarity Administrator. You must import a boot file into the OS-images repository before you can deploy a Windows profile.

    – If you migrated your Windows images to XClarity Administrator v2.1.0 from an earlier release, a preloaded WinPE_64.wim boot file was migrated to the OS-images repository. It is recommended that you import the bundle file for the specific Windows release that you want to deploy instead of using the preloaded boot file.

    – You cannot delete predefined boot files that were loaded when you installed XClarity Administrator; however, you can delete predefined boot files that were imported from a Lenovo bundle.

    – XClarity Administrator requires that imported bundle files be signed by Lenovo. When importing a bundle file, an .asc signature file must also be imported.

  – **Custom boot files**. You can create a WinPE boot file to customize boot options for a Windows deployment. You can then add the boot file to custom Windows profiles.

    XClarity Administrator provides scripts for creating boot files in the correct format. For information about creating a custom boot files, see Creating a boot (WinPE) file and Introduction to Windows PE (WinPE) website.

    The following file types are supported for importing custom boot files.

Operating system	Supported Boot File Types	Supported Bundle File Types
CentOS Linux	Not supported	Not supported
Microsoft® Windows® Azure Stack HCI	Not supported	Not supported
Microsoft Windows Hyper-V Server	A .zip file that contain a WinPE file that is created using the **genimage.cmd** script	A .zip file containing device drivers and boot files
Microsoft Windows Server	A .zip file that contain a WinPE file that is created using the **genimage.cmd** script	A .zip file containing device drivers and boot files
Red Hat® Enterprise Linux (RHEL) Server	Not supported	Not supported

Operating system	Supported Boot File Types	Supported Bundle File Types
SUSE® Linux Enterprise Server (SLES)	Not supported	Not supported
Ubuntu	Not supported	Not supported
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Not supported	Not supported

- **Device drivers**

  You must ensure that the operating-system image that you intend to deploy includes the appropriate Ethernet, Fibre Channel, and storage adapter device drivers for your hardware. If the I/O adapter device driver is not included in the operating system image or profile, the adapter is not supported for OS deployment. You can create custom OS-image profiles that include the out-of-box device drivers that you need.

  Lenovo XClarity Administrator supports in-box device drivers as well as predefined and custom out-of-box device drivers.

  – **In-box device drivers**. XClarity Administrator does not manage in-box device drivers. Always install the latest operating system to ensure that you have the latest in-box device drivers that you need.

    Note: You can add in-box device drivers to a customized Windows profile by creating a custom WinPE boot file and copying the device-driver files to the host system in the `C:\drivers` directory. When you create a custom OS-images profile that uses the custom boot-file, the device drivers that are in the C:\drivers directory are included in both WinPE and the final OS. They are treated as though they were inbox. Therefore, you do not need to import these in-box device drivers into XClarity Administrator when you specify device drivers to use in the custom OS-images profile creation.

  – **Predefined device drivers**. For ThinkSystem servers, XClarity Administrator is preloaded with a set of out-of-box device drivers for Linux to enable the installation of the operating system as well as basic network and storage configuration for the final operating system. You can add these predefined device drivers to your custom OS-image profiles, and then deploy the profiles to your managed servers

    Lenovo also bundles sets of predefined device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Currently, the bundle files are available only for Windows. If the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Image** tab.

    Notes:

    – By default, the predefined OS-image profiles include the predefined device drivers.

    – You cannot delete predefined device drivers that were loaded when you installed XClarity Administrator; however, you can delete predefined device drivers that were imported from a Lenovo bundle.

    – XClarity Administrator requires that imported bundle files be signed by Lenovo. When importing a bundle file, an .asc signature file must also be imported.

  – **Custom device drivers**. You can import out-of-box device drivers into the OS-images repository, and then add those device drivers to a custom OS-image profile.

    You can obtain device drivers from the Lenovo YUM Repository webpage, from the vendor (such as Red Hat), or through a custom device driver that you generated yourself. For some Windows device drivers, you can generate a custom device driver by extracting the device driver from the installation .exe to your local system and creating a .zip archive file.

    The following file types are supported for importing custom device drivers.

Operating system	Supported Device Driver File Types	Device Driver
CentOS Linux	Not supported	Not supported
Microsoft® Windows® Azure Stack HCI	Not supported	Not supported
Microsoft Windows Hyper-V Server	A .zip file containing the raw device-driver files, which are typically grouping of .inf, .cat, and .dll files.	A .zip file containing device-driver files
Microsoft Windows Server	A .zip file containing the raw device-driver files, which are typically grouping of .inf, .cat, and .dll files.	A .zip file containing device-driver files
Red Hat® Enterprise Linux (RHEL) Server	Driver update disk (DUD) in either an .rpm or .iso image format **Note:** If you apply a DUD .rpm to the custom profile, the .rpm is installed only to the final operating system. It is not installed in the install environment (initrd). To install a custom device driver to the initrd, import a DUD .iso and apply the .iso to the custom profile.	Not supported
SUSE® Linux Enterprise Server (SLES)	Driver update disk (DUD) in .rpm or .iso image format **Note:** If you apply a DUD .rpm to the custom profile, the .rpm is installed only to the final operating system. It is not installed in the install environment (initrd). To install a custom device driver to the initrd, import a DUD .iso and apply the .iso to the custom profile.	Not supported
Ubuntu	Not supported	Not supported
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Device drivers in .vib image format	Not supported

Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

- **Custom configuration settings**

  Configuration settings describe data that needs to be gathered dynamically during OS deployment. Lenovo XClarity Administrator uses a set of predefined configuration settings, including global, network, and storage location settings. You can use these predefined configuration settings and add custom configuration setting that are not available through the XClarity Administrator.

  The custom configuration settings are defined in the form of a JSON schema. The schema must conform to the JSON specification.

  When you import custom configuration settings to XClarity Administrator, XClarity Administrator validates the JSON schema. If the validation passes, XClarity Administrator generates custom macros for each setting.

  You can use the custom macros in the unattend file and post-installation script.

In unattend files

You can associate the custom configuration file with an unattend file and include these custom macros (and predefined macros) in that unattend file.

You can add one or more custom configuration settings files in a custom profile. When you deploy the OS profile to a set of target servers, you can choose which configuration settings file to use. XClarity Administrator renders the **Custom Settings** tab on the Deploy OS Images dialog based on the JSON schema in the configuration settings file and allows you to specify values for each setting (JSON object) that is defined in the file.

Note: OS deployment will not proceed if input is not specified for any required custom configuration settings.

In post-installation scripts

After the data is gathered during OS deployment, XClarity Administrator creates an instance of the configuration settings file (which includes the custom settings in the selected file and a subset of predefined settings) on the host system that can be used by the post installation script.

Notes:

- Configuration settings file is unique to a custom OS-image profile.
- You cannot modify configuration settings for predefined OS-image profiles.
- Configuration settings are supported for only the following operating systems:
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) with Lenovo Customization 6.0u3 and later updates and 6.5 and later.

The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

- **Custom unattend files**

  You can customize OS image profiles to use unattend files to automate the deployment of the operating system.

  The following file types are supported for custom unattend files.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Azure Stack HCI	Not supported	
Microsoft Windows Hyper-V Server	Not supported	
Microsoft Windows Server	Unattend (.xml)	For more information about unattend files, see the Unattended Windows Setup Reference webpage.

Operating system	Supported File Types	More information
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	For more information about unattend files, see the Red Hat: Automating the Installation with Kickstart webpage. Consider the following when adding %pre, %post, % firstboot sections in the file. – You can include multiple %pre, %post, %firstboot sections to the unattend file; however, be aware of the ordering of the sections. – When the recommended **#predefined.unattendSettings.preinstallConfig#** macro is present in the unattend file, XClarity Administrator adds a %pre section before all other %pre sections in the file. – When the recommended **#predefined.unattendSettings.postinstallConfig#** macro is present in the unattend file, XClarity Administrator adds %post and %firstboot sections before all other %post and %firstboot sections in the file.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	For more information about unattend files, see the SUSE: AutoYaST webpage.
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Kickstart (.cfg)	Supported only for ESXi 6.0u3 and later updates and 6.5 and later. For more information about unattend files, see the VMware: Installing or Upgrading Hosts by Using a Script webpage. Consider the following when adding %pre, %post, % firstboot sections in the file. – You can include multiple %pre, %post, %firstboot sections to the unattend file; however, be aware of the ordering of the sections. – When the recommended **#predefined.unattendSettings.preinstallConfig#** macro is present in the unattend file, XClarity Administrator adds a %pre section before all other %pre sections in the file. – When the recommended **#predefined.unattendSettings.postinstallConfig#** macro is present in the unattend file, XClarity Administrator adds %post and %firstboot sections before all other %post and %firstboot sections in the file.

Attention:

– You can inject predefined and custom macros (configuration settings) in the unattend file using the unique name of the object. Predefined values are dynamic based on the XClarity Administrator instances. Custom macros are dynamic based on user input that is specified during OS deployment.

  Notes:

  – Surround the macro name with a hash symbol (#).
  – For nested objects, separate each object name using a period (for example, **#server_settings.server0.locale#**).
  – For custom macros, do not include the top-most object name. For predefined macros, prefix the macro name with "predefined."

  - When an object is created from a template, the name is appended with a unique number, starting with 0 (for example, **server0** and **server1**).
  - You can see the name for each macro from the Deploy OS Images dialog on the Custom Settings tabs by hovering over the Help icon ( ) next to each custom setting.
  - For a list of predefined macros, see Predefined macros. For information about custom configuration settings and macros, see Custom macros.
- XClarity Administrator provides the following predefined macros that are used to communicate status from the OS installer, as well as several other critical installation steps. It is strongly recommended that you include these macros in unattend file (see Injecting predefined and custom macros to an unattend file).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

- **Custom installation scripts**

  You can customize OS image profiles to run an installation script after the OS deployment completes.

  Currently, only post-installation scripts are supported.

  The following table lists the file types for installation scripts that Lenovo XClarity Administrator supports for each operating system. Note that certain operation system versions do not support all of the file types that XClarity Administrator supports (for example, some RHEL versions might not include Perl in the minimal profile and, therefore, Perl scripts will not run). Ensure that you use the correct file type for the operating system versions that you want to deploy.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Azure Stack HCI	Not supported	
Microsoft Windows Hyper-V Server	Not supported	
Microsoft® Windows® Server	Command file (.cmd), PowerShell (.ps1)	The default custom data and files path is `C:\lxca`. For more information about installation scripts, see the Add a custom script to Windows Setup webpage
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm or .pl), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the RHEL: Post-installation Script webpage.
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm or .pl), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the SUSE: Custom user script webpage
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Bash (.sh), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the VMware: Installation and Upgrade Scripts webpage

- **Custom software**

  You can customize OS image profiles to install custom software payloads after the OS deployment and post-installation scripts complete.

  The following file types are supported for custom software.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Azure Stack HCI	Not supported	
Microsoft Windows Hyper-V Server	Not supported	
Microsoft Windows® Server	A .zip file containing the software payload.	The default custom data and files path is `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.

Importing a customized OS image profile

You can import a customized OS image profile and add it to an existing compatible base OS image.

About this task

The base OS image must be imported before you can import a custom profile.

A custom OS-image profile can be added only to a based OS image of the same type. For example, if the exported profile is for a Windows 2016 image, the profile can only be imported and added to a Windows 2016 image that exists in the OS-images repository.

The OS images repository can store an unlimited number of custom profiles, if space is available to store the files.

Procedure

To import a customized OS image profile, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. From the **OS Images** tab, select the base OS image to which you want to add the customized OS image profile.

Step 3. Click **Import/Export Profile → Import Customized Profile Image**. The Import Customized OS Image Profile dialog is displayed

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Enter the profile name or click **Browse** to find the profile that you want to import.

Step 7. Optional: **Optional:** For local imports, select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:
- **MD5**
- **SHA1**
- **SHA256**

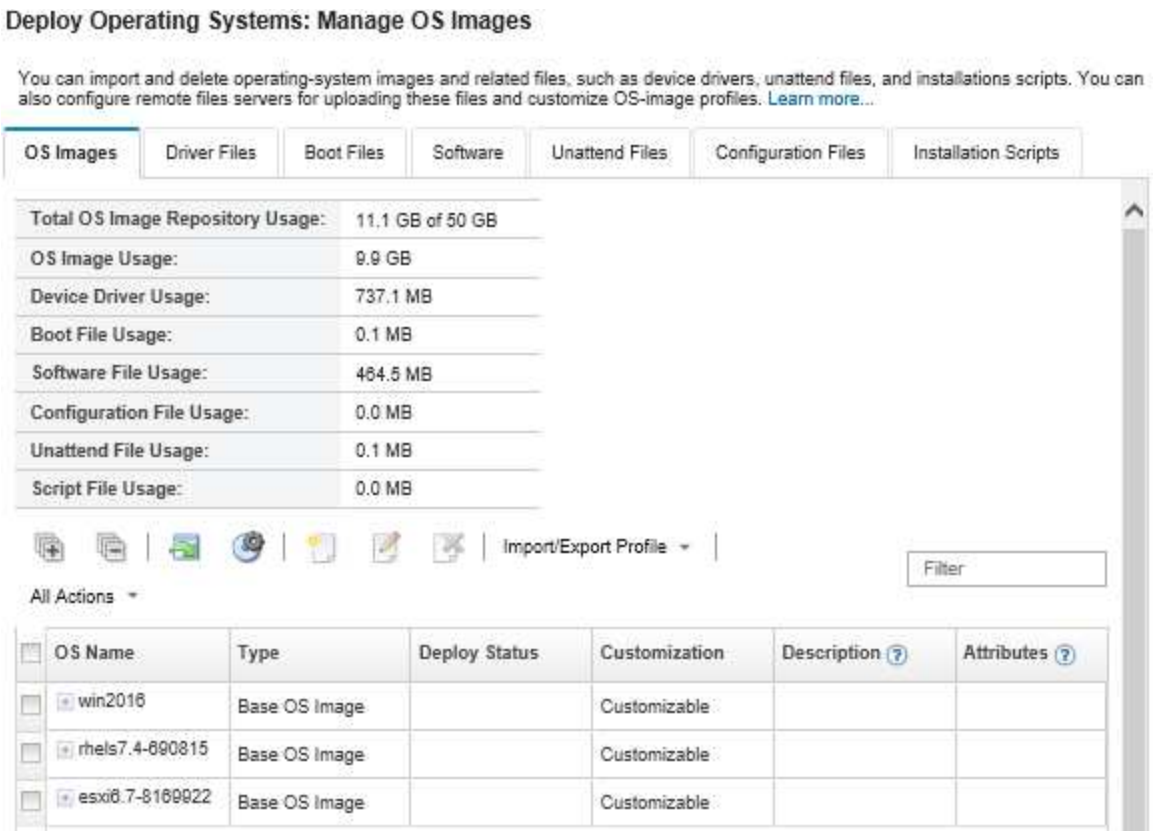
Step 8. Click **Import**.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

After you finish

The customized OS image profile is listed under the base operating system on the Manage OS Images page.



From this page, you can perform the following actions:

- Create a customized OS-image profile (see Creating a custom OS-image profile).
- Export a selected customized OS image profile by clicking **Import/Export Profile → Export Customized Profile Image**.

  Important: You can export customized OS image profiles to a remote file server that is set up to use FTP or SFTP protocols. You cannot export to a remote file server that is set up to use HTTP or HTTPS.
- Modify a selected customized OS image profile by clicking the **Edit** icon ( ).
- Remove a selected customized OS image profile by clicking the **Delete** icon ( ).

Importing boot files

You can import boot files into the OS images repository. These files can then be used to customize and deploy Windows images.

About this task

A boot file acts as the bootstrap install environment. For Windows, this is a Windows Pre-installation (WinPE) file. A WinPE boot file is required to deploy Windows

Lenovo XClarity Administrator supports predefined and custom boot files.

- **Predefined boot files**. Lenovo provides a WinPE_64.wim boot file that can be used to deploy predefined OS-image profiles.

  Lenovo bundles the predefined WinPE_64.wim boot file along with a set of device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage

and then imported into OS-images repository. Because the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Files** tab.

Notes:

- A predefined boot file is not preloaded with XClarity Administrator. You must import a boot file into the OS-images repository before you can deploy a Windows profile.
- If you migrated your Windows images to XClarity Administrator v2.1.0 from an earlier release, a preloaded WinPE_64.wim boot file was migrated to the OS-images repository. It is recommended that you import the bundle file for the specific Windows release that you want to deploy instead of using the preloaded boot file.
- You cannot delete predefined boot files that were loaded when you installed XClarity Administrator; however, you can delete predefined boot files that were imported from a Lenovo bundle.
- XClarity Administrator requires that imported bundle files be signed by Lenovo. When importing a bundle file, an .asc signature file must also be imported.

- **Custom boot files**. You can create a WinPE boot file to customize boot options for a Windows deployment. You can then add the boot file to custom Windows profiles.

  XClarity Administrator provides scripts for creating boot files in the correct format. For information about creating a custom boot files, see Creating a boot (WinPE) file and Introduction to Windows PE (WinPE) website.

  The following file types are supported for importing custom boot files.

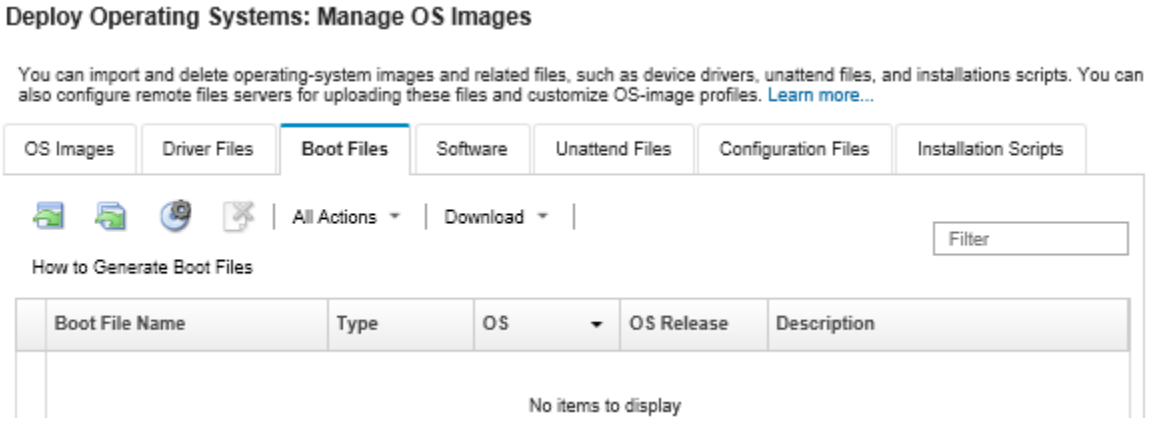
Operating system	Supported Boot File Types	Supported Bundle File Types
CentOS Linux	Not supported	Not supported
Microsoft® Windows® Azure Stack HCI	Not supported	Not supported
Microsoft Windows Hyper-V Server	A .zip file that contain a WinPE file that is created using the **genimage.cmd** script	A .zip file containing device drivers and boot files
Microsoft Windows Server	A .zip file that contain a WinPE file that is created using the **genimage.cmd** script	A .zip file containing device drivers and boot files
Red Hat® Enterprise Linux (RHEL) Server	Not supported	Not supported
SUSE® Linux Enterprise Server (SLES)	Not supported	Not supported
Ubuntu	Not supported	Not supported
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Not supported	Not supported

Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

- To import a Windows bundle file that contains boot files into the OS images repository, complete the following steps.
  1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

2. Click the **Boot Files** tab.



3. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the appropriate bundle file and the associated signature file for the OS image to the local system.
4. Click the **Import Bundle File** icon ( ). The Import Bundle File dialog is displayed.
5. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

   Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .
6. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.
7. Select the operating-system type and release.
8. Enter the file name for the bundle file and the associated signature file or click **Browse** to find the files that you want to import.
9. **Optional:** Enter a description for the bundle file.
10. Click **Import**.

    Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

    If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

- To import an individual boot file into the OS images repository, complete the following steps.
  1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
  2. Click the **Boot Files** tab.
  3. Click the **Import File** icon ( ). The Import File dialog is displayed.
  4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

     Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .
  5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

6. Select the operating-system type and release.
7. Enter the file name or click **Browse** to find the boot file that you want to import.
8. **Optional:** Enter a description for the boot file.
9. **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

   If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

   Three checksum types are supported:
   - **MD5**
   - **SHA1**
   - **SHA256**
10. Click **Import**.

    Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

    If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

After you finish

The boot file is listed on the **Boot Files** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).
- Remove a selected boot file by clicking the **Delete** icon ( ).
- Add a boot file to an customized OS image profile (see Creating a custom OS-image profile).

Creating a boot (WinPE) file

You can create boot files that can be used to customize Windows images.

Before you begin

- Ensure that the operating system you intend to provision is installed on the host. For example, if you plan to provision Windows 2016 using the WinPE files, then install Windows 2016 on the host.
- Ensure that the Microsoft ADK that is compatible with the installed operating system is also installed on the host. For example, Windows 2012R2 requires ADK version 8.1 Update.
- Obtain the device drivers, in .inf format, that you want to add to the boot file.

  You can obtain device drivers from the Lenovo YUM Repository webpage, from the vendor (such as Red Hat), or through a custom device driver that you generated yourself. For some Windows device drivers, you can generate a custom device driver by extracting the device driver from the installation .exe to your local system and creating a .zip archive file.

  Lenovo also bundles sets of predefined device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Currently, the bundle files are available only for Windows. If the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Image** tab.

- Download the **genimage.cmd** and **startnet.cmd** files to the host in a temporary directory, such as `C:\customwim`.

  The **genimage.cmd** command is used to generate the WinPE boot files, including the .wim file. The **startnet.cmd** command is used by XClarity Administrator to bootstrap the Windows installer.
- Decide how you want to inject device drivers into the boot file. You can do this in one of the following ways:
  - Add in-box device drivers to a customized Windows profile by copying the device-driver files to the host system in the C:\drivers directory. These will be included in the boot file when genimage.cmd runs later.

    Note: When you create a custom OS-images profile that uses the custom boot-file, the device drivers that are in the C:\drivers directory are included in both WinPE and the final OS. They are treated as though they were inbox. Therefore, you do not need to import these in-box device drivers into XClarity Administrator when you specify device drivers to use in the custom OS-images profile creation.
  - Add out-of-box device drivers directly to the boot file.

    Note: If you use this method, the device drivers are only applied to the boot file and therefore to the WinPE install environment. The device drivers are not applied to the final installed OS. You must manually import the device drivers into the OS-images device driver repository and select them for use as part of the OS-image profile customization.
- For more information about boot files, see the Introduction to Window PE (WinPE) website.

Procedure

To create a boot file, complete the following steps.

Step 1. Using a user ID with administrator authority, run the Windows ADK command “Deployment and Imaging Tools Environment.” A command session is displayed.

Step 2. From the command session, change to the directory where the **genimage.cmd** and **starnet.cmd** files were downloaded (for example, `C:\customwim`).

Step 3. Ensure that no previously mounted images are on the host by running the following command:
```
dism /get-mountedwiminfo
```

If there are mounted images, discard them by running the following command:

```
dism /unmount-wim /MountDir:C:\<mount_path> /Discard
```

Step 4. If you are adding in-box device drivers to a customized Windows profile, copy the raw device-driver files, in .inf format, to the host system in the `C:\drivers` directory.

Step 5. Run the following command to generate the boot file, in .wim format, and then wait a few minutes for the command to complete.
```
genimage.cmd amd64 <ADK_Version>
```

Where <*ADK_Version*> is one of the following values.

- **8.1**. For Windows 2012 R2
- **10**. For Windows 2016

This command creates the boot file: `C:\WinPE_64\media\Boot\WinPE_64.wim`.

Step 6. Mount the boot file by running the following command:
```
DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
```

Step 7. If you are adding out-of-box device drivers directly to the boot file, complete the following steps.

1. Create the following directory structure, where <*os_release*> is `2012`, `2012R2`, or `2016`

`drivers\<os_release>\`

2. Copy the device drivers, in .inf format, to a directory inside that path, for example:
   `drivers\<os_release>\<driver1>\<driver1_files>`
3. Copy the `drivers` directory to the mount directory, for example:
   `C:\WinPE_64\mount\drivers`

Step 8. Optional: Make additional customizations to the boot file, such as adding folders, files, startup scripts, language packs, and apps. For more information about customizing boot files, see the WinPE: Mount and Customize website.

Step 9. Unmount the image by running the following command.
```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```

Step 10. Compress the contents of the `C:\WinPE_64\media` directory into a zip file called `WinPE_64.zip`.

Step 11. Import the .zip file into XClarity Administrator (see Importing boot files).

Importing device drivers

You can import individual device drivers and bundles files into the OS images repository. These files can then be used to customize Linux and Windows images.

About this task

You must ensure that the operating-system image that you intend to deploy includes the appropriate Ethernet, Fibre Channel, and storage adapter device drivers for your hardware. If the I/O adapter device driver is not included in the operating system image or profile, the adapter is not supported for OS deployment. You can create custom OS-image profiles that include the out-of-box device drivers that you need.

Lenovo XClarity Administrator supports in-box device drivers as well as predefined and custom out-of-box device drivers.

- **In-box device drivers**. XClarity Administrator does not manage in-box device drivers. Always install the latest operating system to ensure that you have the latest in-box device drivers that you need.

  Note: You can add in-box device drivers to a customized Windows profile by creating a custom WinPE boot file and copying the device-driver files to the host system in the `C:\drivers` directory. When you create a custom OS-images profile that uses the custom boot-file, the device drivers that are in the C:\drivers directory are included in both WinPE and the final OS. They are treated as though they were inbox. Therefore, you do not need to import these in-box device drivers into XClarity Administrator when you specify device drivers to use in the custom OS-images profile creation.

- **Predefined device drivers**. For ThinkSystem servers, XClarity Administrator is preloaded with a set of out-of-box device drivers for Linux to enable the installation of the operating system as well as basic network and storage configuration for the final operating system. You can add these predefined device drivers to your custom OS-image profiles, and then deploy the profiles to your managed servers

  Lenovo also bundles sets of predefined device drivers into a single package that can be downloaded from the Lenovo Windows drivers and WinPE Images Repository webpage and then imported into OS-images repository. Currently, the bundle files are available only for Windows. If the bundle file contains both device drivers and boot files, you can import the bundle file from the **Device Driver** or **Boot Image** tab.

  Notes:

  – By default, the predefined OS-image profiles include the predefined device drivers.

  – You cannot delete predefined device drivers that were loaded when you installed XClarity Administrator; however, you can delete predefined device drivers that were imported from a Lenovo bundle.

  - XClarity Administrator requires that imported bundle files be signed by Lenovo. When importing a bundle file, an .asc signature file must also be imported.
- **Custom device drivers**. You can import out-of-box device drivers into the OS-images repository, and then add those device drivers to a custom OS-image profile.

  You can obtain device drivers from the Lenovo YUM Repository webpage, from the vendor (such as Red Hat), or through a custom device driver that you generated yourself. For some Windows device drivers, you can generate a custom device driver by extracting the device driver from the installation .exe to your local system and creating a .zip archive file.

  The following file types are supported for importing custom device drivers.

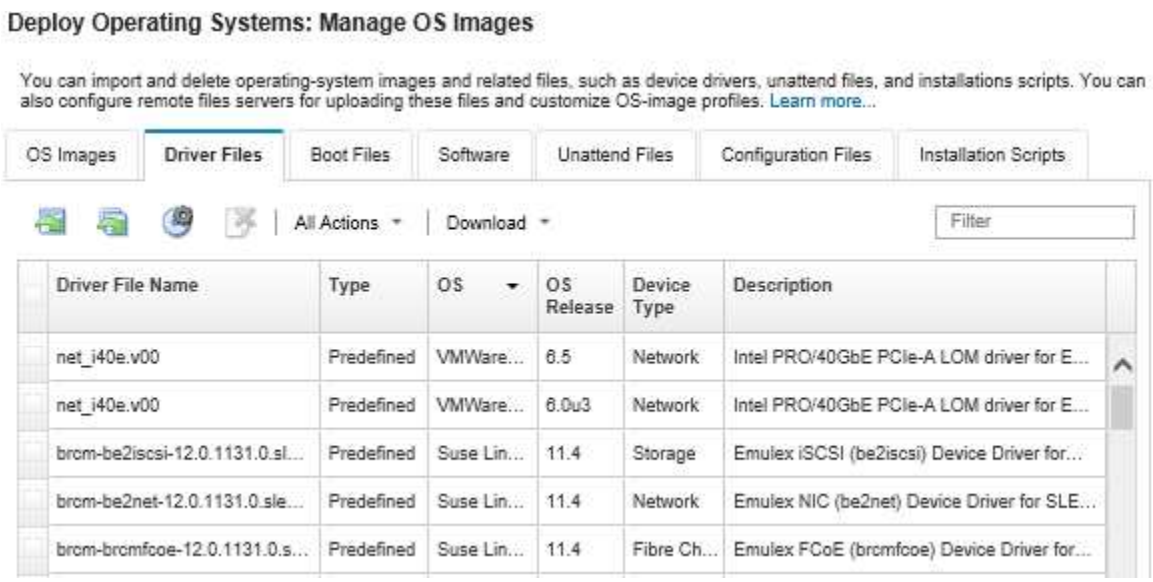
Operating system	Supported Device Driver File Types	Device Driver
CentOS Linux	Not supported	Not supported
Microsoft® Windows® Azure Stack HCI	Not supported	Not supported
Microsoft Windows Hyper-V Server	A .zip file containing the raw device-driver files, which are typically grouping of .inf, .cat, and .dll files.	A .zip file containing device-driver files
Microsoft Windows Server	A .zip file containing the raw device-driver files, which are typically grouping of .inf, .cat, and .dll files.	A .zip file containing device-driver files
Red Hat® Enterprise Linux (RHEL) Server	Driver update disk (DUD) in either an .rpm or .iso image format **Note:** If you apply a DUD .rpm to the custom profile, the .rpm is installed only to the final operating system. It is not installed in the install environment (initrd). To install a custom device driver to the initrd, import a DUD .iso and apply the .iso to the custom profile.	Not supported
SUSE® Linux Enterprise Server (SLES)	Driver update disk (DUD) in .rpm or .iso image format **Note:** If you apply a DUD .rpm to the custom profile, the .rpm is installed only to the final operating system. It is not installed in the install environment (initrd). To install a custom device driver to the initrd, import a DUD .iso and apply the .iso to the custom profile.	Not supported
Ubuntu	Not supported	Not supported
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Device drivers in .vib image format	Not supported

Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

- To import a Windows bundle file that contains device-drivers into the OS images repository, complete the following steps.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **Driver File** tab.



3. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the appropriate bundle file and the associated signature file for the OS image to the local system.
4. Click the **Import Bundle File** icon ( ). The Import Bundle File dialog is displayed.
5. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

   Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .
6. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.
7. Select the operating-system type and release.
8. Enter the file name for the bundle file and the associated signature file or click **Browse** to find the files that you want to import.
9. **Optional:** Enter a description for the bundle file.
10. Click **Import**.

    Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

    If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

- To import an individual device driver into the OS images repository, complete the following steps.
  1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
  2. Click the **Driver Files** tab.
  3. Click the **Import File** icon ( ). The Import File dialog is displayed.

4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

   Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.
6. Select the operating-system type and release.
7. Enter the file name or click **Browse** to find the device driver that you want to import.
8. **Optional:** Enter a description for the device driver.
9. **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

   If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

   Three checksum types are supported:
   - **MD5**
   - **SHA1**
   - **SHA256**

10. Click **Import**.

    Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

    If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

After you finish

The device-drive image is listed on the **Driver Files** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).
- Remove a selected device driver by clicking the **Delete** icon ( ).
- Add a device driver to an customized OS image profile (see Creating a custom OS-image profile).

Importing custom configuration settings

Configuration settings describe data that needs to be gathered dynamically during OS deployment. Lenovo XClarity Administrator uses a set of predefined configuration settings, including global, network, and storage location settings. You can use these predefined configuration settings and add custom configuration setting that are not available through the XClarity Administrator.

About this task

The custom configuration settings are defined in the form of a JSON schema. The schema must conform to the JSON specification.

When you import custom configuration settings to XClarity Administrator, XClarity Administrator validates the JSON schema. If the validation passes, XClarity Administrator generates custom macros for each setting.

You can use the custom macros in the unattend file and post-installation script.

In unattend files

You can associate the custom configuration file with an unattend file and include these custom macros (and predefined macros) in that unattend file.

You can add one or more custom configuration settings files in a custom profile. When you deploy the OS profile to a set of target servers, you can choose which configuration settings file to use. XClarity Administrator renders the **Custom Settings** tab on the Deploy OS Images dialog based on the JSON schema in the configuration settings file and allows you to specify values for each setting (JSON object) that is defined in the file.

Note: OS deployment will not proceed if input is not specified for any required custom configuration settings.

In post-installation scripts

After the data is gathered during OS deployment, XClarity Administrator creates an instance of the configuration settings file (which includes the custom settings in the selected file and a subset of predefined settings) on the host system that can be used by the post installation script.

Notes:

- Configuration settings file is unique to a custom OS-image profile.
- You cannot modify configuration settings for predefined OS-image profiles.
- Configuration settings are supported for only the following operating systems:
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) with Lenovo Customization 6.0u3 and later updates and 6.5 and later.

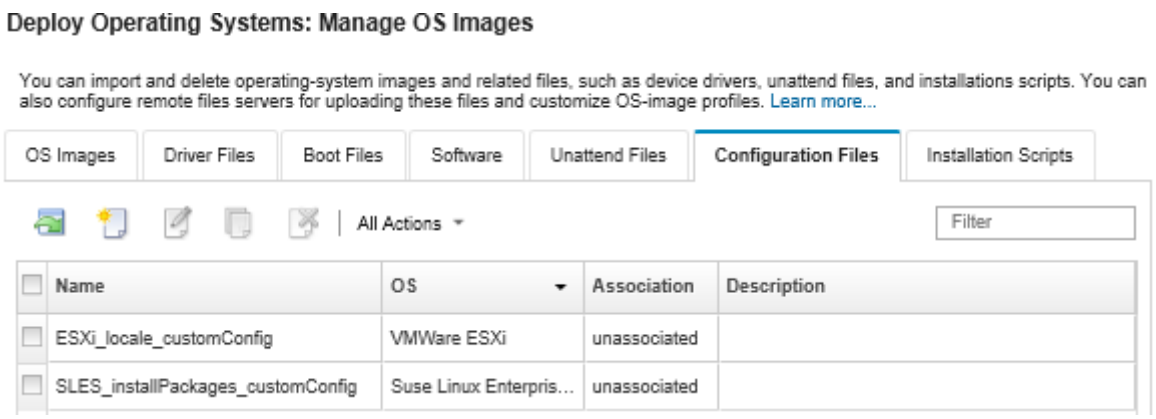
The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

To import configuration-settings files into the OS-images repository, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Configuration Settings** tab.



Step 3. Click the **Import File** icon ( ). The Import Configuration Settings dialog is displayed.

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Select the operating-system type.

Step 7. Enter the file name of the configuration-settings file, or click **Browse** to find the file that you want to import.

Step 8. Optional: **Optional:** Enter a description of the configuration-settings.

Tip: Use the **Description** field to distinguish between custom files with the same name.

Step 9. Optional: **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:

- **MD5**
- **SHA1**
- **SHA256**

Step 10. Click **Import**. The JSON format is validated when you import the file. If errors are found, a dialog is displayed with the error message and location.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

Attention: If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

After you finish

The configuration-settings files are listed on the **Configuration Settings** tab on the Manage OS Images page.

From this page, you can also perform the following actions.

- Create a configuration-setting file by clicking the **Create** icon ( ), and then specifying the file name, description, OS type, and configuration settings and values. Click **Validate** to validate the schema before saving the file.

  The editor identifies the location of any errors that are found in the file. Note that some messages are English only.

- View and modify a configuration-settings file by clicking the **Edit** icon ( ).

  You cannot edit a configuration-settings file that is associated with an unattend file.

  The editor identifies the location of any errors that are found in the file. Note that some messages are English only.

- Copy a configuration-settings file by clicking the **Copy** icon ( ).

  If you copy a configuration-settings file that is associated with an unattend file, the associated unattend file is also copied and the association is automatically created between both copied files.

- Remove selected configuration-setting files by clicking the **Delete** icon ( ).

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).

For information about adding an configuration-settings to a customized OS image profile, see Creating a custom OS-image profile.

Custom macros

Macros give you the ability to add variable data (configuration settings) to an unattend file or post-installation script. Lenovo XClarity Administrator allows you to define your own custom settings by creating a custom configuration-settings file, using JSON format.

The value for each custom configuration setting varies based on user input that is specified during OS deployment.

When you import custom configuration settings in XClarity Administrator, XClarity Administrator validates the JSON schema. If the validation passes, XClarity Administrator generates custom macros for each setting.

To inject custom macros in to an unattend file or post-installation script, use the unique name of the object, separate nested objects using a period, and then surround the macro name with a hash symbol (#), for example, **#server_settings.server0.locale#**.

Notes:

- Do not include the top-most object name.
- When an object is created from a template, the name is appended with a unique number, starting with 0 (for example, server0 and server1).
- You can see the name for each macro from the Deploy OS Images dialog on the Custom Settings tabs by hovering over the **Help** icon ( ) next to each custom setting.

Configuration settings

You can define custom configuration settings that:

- Are common to all target servers or unique to a specific target server.
- Have static (non-configurable) values or with dynamic (configurable) values that are entered when you deploy the OS-image profile.
- Have a variable number of elements based on a template. For example, you can define a configuration setting that let's you specify 0 – 3 NTP servers during deployment.

Common settings

During OS deployment, the UI elements on the **Common Settings** tabs on the Deploy OS Image dialog are rendered based on the objects that are represented in the **content** object. The objects describe the settings and values that the all target servers need for OS deployment.

To represent settings that are common to all servers, the JSON file must contain a parent object with a nested object that contains the `"common":true` name/value pair.

The following example uses the same configurable (dynamic) NTP servers for all servers.

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": true,
      "description": "NTP Servers",
      "label": "NTP Servers",
      "maxElements": 3,
      "minElements": 0,
      "name": "common-ntpservers",
      "optional": true,
      "template": [{
         "autoCreateInstance": true,
         "category": "dynamic",
         "common": true,
         "description": "A NTP Server",
         "label": "NTP Server",
         "name": "ntpserver",
         "optional": true,
         "regex": "[\\w\\.]{1,64}$",
         "type": "string"
      }],
      "type": "array"
   },
   ...,
}
```

The following example uses the same non-configurable (static) post-installation script log directory.

```
{
   "category": "dynamic",
   "content": [{
      "category": "static",
      "common": true,
      "description": "Directory location for post-installation script logging.",
      "name": "logpath",
      "optional": false,
      "type": "string",
      "value": "/tmp/mylogger.log"
   },
   ...,
}
```

Server-specific settings

During OS deployment, the UI elements on the **Server-Specific Settings** tab on the Deploy OS Image dialog are rendered based on the objects that are represented in the template's **content** objects. The objects describe the settings and values that a specific target server needs for OS deployment.

After the server-specific values are gathered in the UI, a **content** object is created in the JSON for each target server based on the **template** object. Each **content** object contain a unique **name** and **targetServer** field, and any values that were inputted for that server.

To represent the server-specific settings, the JSON file must contain a parent object with the following content:

- The `"category":"dynamic"` name/value pair.
- A nested object that contains the `"common":false` name/value pair. Only one `"common": false` object is supported in the content of the parent object.
- A template object with an embedded content object. This template array can contain only one object.

For example, if you want to define a unique OS locale for each target server

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": false,
      "name": "server-settings",
      "optional": false,
      "template": [{
         "category": "dynamic",
         "common": false,
         "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
         }],
         "name": "server",
         "optional": false,
         "type": "assoc_array"
      }],
      "type": "assoc_array"
   },
   ...,
}
```

JSON specification

The following table describes the fields that are allowed in the JSON specification.

Parameter	Required / Optional	Type	Description
autoCreateInstance	Optional	Boolean	Indicates whether an instance of the template object is created automatically in JSON file at deployment time. This can be one of the following values. • **true**. An instance of the template object is created automatically in JSON file at deployment time. • **false**. (default) An instance of the template object *is not* created automatically in JSON file at deployment time **Note:** This field can be placed only in the template object.
category	Required	String	Indicates how the value of each setting is populated. This can be one of the following values: • **dynamic**. The value is input by the user at run time. Lenovo XClarity Administrator prompts you for this value during OS deployment. • **predefined**. The value is preset by Lenovo XClarity Administrator. • **static**. The value is specified in the schema and does not change at run time. Nested objects inherit the value of this field from its parent object. If **category** is set to `static` in the parent object, then it must be set to `static` in all nested objects as well. If **category** is set to `dynamic` in the parent object, it can be either `static` or `dynamic` in the nested objects.
choices	Optional	Array of values that match the **type** property	Array of static values (such as strings or integers) for the configuration setting from which the user can select during OS deployment (for example, `["enabled","disabled"]`).
common	Optional	Boolean	Indicates whether this configuration schema applies to all target servers. • **true**. The object applies to all target servers. • **false**. (default) The object applies to a specific target server. Nested objects inherit the value of this field from its parent object. If **common** is set to `true` in the parent object, then it must be set to `true` in all nested objects as well. If **common** is set to `false` in the parent object, then it must be set to `false` in all nested objects.
content	Optional	Array of objects	Pattern that represents nested objects in the schema. After user-inputted data is gathered during OS deployment, this field is used to represent the final values for a given template in the instance of the configuration-settings file that is created for the deployment.
default	Optional	Varies depending on the **type**	The default value.

Parameter	Re-quired / Optional	Type	Description
description	Optional	String	Description of the object
label	Optional	String	Label for the setting in the user interface that is displayed during OS deployment
max	Optional	Integer	Maximum value, when **type** is set to integer. The default value is unlimited.
maxElements	Optional	Integer	Maximum number of entries in the array for this object.
min	Optional	Integer	Minimum value, when **type** is set to integer. The default value is 0.
minElements	Optional	Integer	Minimum number of entries in the array for this object.
name	Required	String	Unique name of the object. This name can contain only the following characters: alphanumeric characters (a-z, A-Z, and 0-9), underscore (_), and dash (-). You can reference the **name** as a custom macro in the unattend file. When referencing a nested **name** object, separate each object using a period (for example, `mydeploy.node.locale`).
optional	Required	Boolean	Indicates whether the object is optional. This can be one of the following values. • **true**. The field is optional • **false**. The field is required.
regex	Optional	String	Regular expression for validating the value (for example, `"[\\w\\.]{1,64}$"`)
script	Optional	Array of strings	List of scripts, separated by a comma, that have dependencies on the data in this object (for example, `["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]`). **Note:** The scripts must be available to the OS-image profile as an installation script or custom software.
targetServer	Optional	String	UUID of the server that is the target for the OS deployment. If common is true, this field can be empty or null, and the target server is specified during OS deployment.

Parameter	Re-quired / Optional	Type	Description

template	Optional	Array of objects	Pattern that represents reusable objects.
			During OS deployment, this template can represent multiple instances of the object. The **minElements** and **maxElements** fields can be used to limit the number of instances.
			
			The following example uses a template to represent an array of 1 - 3 NTP servers.
			{
			"category": "dynamic",
			"common": true,
			"description": "NTP Servers",
			"label": "NTP Servers",
			"maxElements": 3,
			"minElements": 0,
			"name": "common-ntpservers",
			"optional": true,
			"template": [{
			"autoCreateInstance": true,
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			},
			
			After user-inputted values are gathered during OS deployment, an instance of the configuration-settings file is created with specific content for each device on which the OS is to be deployed.
			{
			"category": "dynamic",
			"common": true,
			"description": "NTP Servers",
			"label": "NTP Servers",
			"maxElements": 3,
			"minElements": 0,
			"name": "common-ntpservers",
			"optional": true,
			"content": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver0",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string",
			"value": "192.0.2.1"
			}],
			"template": [{
			"category": "dynamic",

Parameter	Re-quired / Optional	Type	Description

			<pre>"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			}</pre> **Notes:** • A template is *required* at the top level of server-specific objects (common=false). • If **category** is `static`, the template field is ignored.

type	Required	String	Data type for the object. This can be one of the following values. • **array** • **assoc_array** • **boolean** • **integer** • **password** • **string** • **user_data**
value	Optional	String	A single static value for the configuration setting. **Notes:** • If **default** is set, this field can be empty or null; otherwise, specify a value that matches **type**. • If **type** is `password`, specify a non-encrypted string. • If **type** is `assoc_array` or `array`, you must also specify an empty **content** field. • If **type** is `user_data`, specify valid JSON-formatted **value**. • If **regex** is set, this value is validated using the specified regular expression.

The following example configuration settings define locale settings for SLES deployments that can be added to a custom profile.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "template": [{
            "autoCreateInstance": true,
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
```

```
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
        "category": "dynamic",
        "common": true,
        "description": "A NTP Server",
        "label": "NTP Server",
        "name": "ntpserver",
        "optional": true,
        "regex": "[\\w\\.]{1,64}$",
        "type": "string"
    }],
    "type": "array"
},
{
    "category": "static",
    "common": true,
    "description": "Directory for post-installation script logging.",
    "name": "logpath",
    "optional": false,
    "type": "string",
    "value": "/tmp/mylogger.log"
}],
"description": "Custom configuration file for deployment of custom locale, NTP server,
                and directory for post-installation script logs.",
"label": "My Custom Deployment",
"name": "myCustomDeploy",
```

```
    "optional": false,
    "type": "array"
}
```

The following example is the instance of the configuration settings file that is created on the host system after user-inputted values are defined during deployment.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "content": [{
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
                "category": "dynamic",
                "choices": ["english-us", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the keyboard locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "Keyboard Locale",
                "name": "keyboardLocale",
                "optional": false,
                "type": "string",
                "value": "english-us"
            }],
            "name": "server0",
            "optional": false,
            "type": "assoc_array",
            "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
        },
        {
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
```

```
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server1",
        "optional": false,
        "type": "assoc_array",
        "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
    }],
    "template": [{
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "content": [{
        "category": "dynamic",
        "common": true,
```

```
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver0,
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.1"
        },
        {
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver1",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.2"
        }],
        "template": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
        }],
        "type": "array"
    },
    {
        "category": "static",
        "common": true,
        "description": "Directory for post-installation script logs.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Predefined macros

Macros give you the ability to add variable data (configuration settings) to an unattend file or post-installation script. Lenovo XClarity Administrator provides a set of predefined configuration settings that you can use.

To inject predefined macros to an unattend or post-installation script file, prefix the macro with "predefined" for predefined macros, separate nested objects using a period, and then surround the macro name with a hash symbol (#), for example **#predefined.globalSettings.ipAssignment#**.

The value for each predefined macro varies based on the XClarity Administrator instance. For example, the **Deploy OS Images → Global Settings → IP Assignment** field allows you to specify the IP mode. After the user-inputted value is gathered during OS deployment, the value is represented in the predefined

configurations settings by the predefined macro **#predefined.globalSettings.ipAssignment#** and in the instance of the configuration-settings JSON file under the ipAssignment Object name.

The following table lists the predefine macros (configuration settings) that are available in XClarity Administrator.

Macro name	Type	Description
predefined	Object	Information about all predefined OS-deployment settings
globalSettings	Object	Information about global OS-deployment settings
credentials	Array of objects	Information about user credentials
name	String	
type	String	Operating system type. This can be one of the following values. • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	String	Host network setting option for operating system deployment. This can be one of the following values. • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	String	Indicates whether VLAN mode is used. This can be one of the following values. • **true**. VLAN mode is used. • **false**. VLAN mode is not used.
hostPlatforms	Object	Deployment settings from the host platforms
licenseKey	String	License key to be used for Microsoft Windows or VMware ESXi. If you do not have a license key, you can set this field to null.
networkSettings	Array	Information about network settings
dns1	String	Preferred DNS server for the host server to be used after the operating system is deployed
dns2	String	Alternative DNS server for the host server to be used after the operating system is deployed
gateway	String	Gateway of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
hostname	String	Hostname for the host server. If a hostname is not specified, a default hostname is assigned.
ipAddress	String	IP address of the host server to be used after the operating system is deployed. This is used when the network setting is set to static in the Global OS deployment settings.
mtu	Long	Maximum transmission unit for the host to be used after the operating system is deployed.
prefixLength	String	Prefix length of the host IP address to be used after the operating system is deployed. This is used when the network setting is set to static IPv6 in the Global OS deployment settings.

Macro name	Type	Description
selectedMAC	String	MAC address of the host server to which the IP address is to be bound. The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment, and selectedMAC is set to the newly detected MAC address. VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only the MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server. **Tip:** To obtain the MAC address, use the **macaddress** response property in GET /hostPlatforms.
subnetCIDRNumber	Integer	Subnet mask of the host server to be used after the operating system is deployed, in Classless Inter-Domain Routing (CIDR) format. This is used when the network setting is set to static in the Global OS deployment settings. The CIDR number is typically preceded by a slash "/" and follows the IP address. For example, an IP address of 131.10.55.70 with a subnet mask of 255.0.0.0 (which has 8 network bits) would be represented as 131.10.55.70 /8. For more information, see the CIDR Notation Tutorial webpage. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
subnetMask	String	Subnet mask of the host server to be used after the operating system is deployed, in dotted decimal notation (for example, 255.0.0.0). This is used when the network setting is set to static in the Global OS deployment settings. **Tip:** To determine the IP mode, use GET /osdeployment/globalSettings.
vlanId	String	VLAN ID for operating-system VLAN tagging. This parameter is valid only if in VLAN mode is enabled. To determine if VLAN mode is enabled use GET /osdeployment/globalSettings in the XClarity Administrator online documentation). **Important:** Only specify a VLAN ID when a VLAN tag is required to function on the network. Using VLAN tags can affect the network routability between the host operating system and the XClarity Administrator.
selectedImage	String	Profile ID of the operating-system image to be deployed. **Tip:** To obtain the operating-system image profile IDs, use the **availableImages** response property in GET /hostPlatforms.
storageSettings	Array	Preferred storage location on which you want to deploy operating-system images

Macro name	Type	Description
targetDevice	String	Target device. This can be one of the following values. • **localdisk**. Local disk drive. The first enumerated local disk drive in the managed server is used. • **M.2drive**. M.2 drive. The first enumerated M.2 drive in the managed server is used. • **usbdisk**. Embedded USB Hypervisor. This location is applicable only when a VMware ESXi image is being deployed to managed servers. If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment. • **lunpluswwn=***LUN@WWN*. FC SAN storage (for example, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. iSCSI SAN Storage (for example, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Specifying the *IQN* is optional if only one iSCSI target is configured If the *IQN* is not specified, the first detected iSCSI target is selected for OSDN. If specified, and exact match is made. **Note:** For ThinkServer servers, this value is always “localdisk.”
unattendFileId	String	ID of the unattend file to be used with this deployment
uuid	String	UUID of the host server to which the operating system is to be deployed
imageSettings	Object	Information about each OS image and image profile
name	String	Operating-system image name
profile	String	Image profile name
otherSettings	Object	Additional settings that are related to the currently running OS deployment jobs
deployDataAndSoftwareLocation	String	Path to the extracted software payload, custom files, and deployment data (such as certificates and logs)

installRepoUrl	String	(SLES 15 and later only) URL for the imported package image
		You can use this predefined macro in the custom unattend for the media_url in the add-on section, for example:
		`<add-on>`
		`  <add_on_products config:type="list">`
		`  <listentry>`
		`  <media_url>`**#predefined.otherSettings.installRepoUrl#**
		`  </media_url>`
		`  <product>sle-module-basesystem</product>`
		`  <product_dir>/Module-Basesystem</product_dir>`
		`  </listentry>`
		`  </add_on_products>`
		`</add-on>`

lxcaIp	String	IP address of the XClarity Administrator instance
lxcaRelease	String	XClarity Administrator release (for example. 2.0.0)
jobId	String	ID of the currently running OS deployment job
ntpServer	String	NTP server that is associated with XClarity Administrator
statusSettings	Object	OS deployment status settings
urlStatus	String	HTTPS URL (including the port) that XClarity Administrator uses for reporting status

Macro name	Type	Description
certLocation	String	Folder containing the certificates that are needed to access the **urlStatus** web service from the host OS on first boot
sdkLocation	String	Location of XClarity Administrator provided helper scripts and interfaces for access to the XClarity Administrator
timezone	String	Time zone that is set for XClarity Administrator (for example, America/New_York)
unattendSettings	Object	Settings that are used to populate the unattend file. These values are specific to the version of XClarity Administrator
networkConfig	String	(ESXi and RHEL only) XClarity Administrator predefined content for use at unattend install time. This configures the network settings for the operating system
preinstallConfig	String	XClarity Administrator predefined content for use at pre-installation unattend time. This includes pre-installation status. • For ESXi and RHEL, this uses the %pre pre-installation scripts hook. • For SLES, this uses the <scripts> pre-installation scripts hook. **Attention:** It is strongly recommended that you include this macro in the custom unattend file. You can place the macro in the unattend file anywhere after line 1 (after the <xml> tag).
postinstallConfig	String	XClarity Administrator predefined content for use after the server is configured and booted for the first time. This includes post-installation status. • For ESXi and RHEL, this uses the %post post- installation scripts hook • For SLES, this uses the <scripts> post-installation scripts hook. • For Windows ,this uses the “specialize settings” section. **Attention:** It is strongly recommended that this macro be included in the custom unattend file. You can place the macro in the unattend file anywhere after line 1 (after the <xml> tag).
reportWorkloadNotComplete	String	When this macro is present, the postinstallConfig macro does not report OS Installation Completed (17) status. The custom profile must report complete.
storageConfig	String	(ESXi and RHEL only) XClarity Administrator predefined content for use at unattend install time. This configures the storage settings for the operating system.

Importing custom unattend files

You can import custom unattend files into the OS images repository. These files can then be used to customize Linux and Windows OS-images profiles.

About this task

The following file types are supported for custom unattend files.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Azure Stack HCI	Not supported	

Operating system	Supported File Types	More information
Microsoft Windows Hyper-V Server	Not supported	
Microsoft Windows Server	Unattend (.xml)	For more information about unattend files, see the Unattended Windows Setup Reference webpage.
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	For more information about unattend files, see the Red Hat: Automating the Installation with Kickstart webpage. Consider the following when adding %pre, %post, %firstboot sections in the file. • You can include multiple %pre, %post, %firstboot sections to the unattend file; however, be aware of the ordering of the sections. • When the recommended **#predefined.unattendSettings.preinstallConfig#** macro is present in the unattend file, XClarity Administrator adds a %pre section before all other %pre sections in the file. • When the recommended **#predefined.unattendSettings.postinstallConfig#** macro is present in the unattend file, XClarity Administrator adds %post and %firstboot sections before all other %post and %firstboot sections in the file.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	For more information about unattend files, see the SUSE: AutoYaST webpage.
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Kickstart (.cfg)	Supported only for ESXi 6.0u3 and later updates and 6.5 and later. For more information about unattend files, see the VMware: Installing or Upgrading Hosts by Using a Script webpage. Consider the following when adding %pre, %post, %firstboot sections in the file. • You can include multiple %pre, %post, %firstboot sections to the unattend file; however, be aware of the ordering of the sections. • When the recommended **#predefined.unattendSettings.preinstallConfig#** macro is present in the unattend file, XClarity Administrator adds a %pre section before all other %pre sections in the file. • When the recommended **#predefined.unattendSettings.postinstallConfig#** macro is present in the unattend file, XClarity Administrator adds %post and %firstboot sections before all other %post and %firstboot sections in the file.

Attention:

- You can inject predefined and custom macros (configuration settings) in the unattend file using the unique name of the object. Predefined values are dynamic based on the XClarity Administrator instances. Custom macros are dynamic based on user input that is specified during OS deployment.

  Notes:

  – Surround the macro name with a hash symbol (#).

  – For nested objects, separate each object name using a period (for example, **#server_settings.server0.locale#**).

  - For custom macros, do not include the top-most object name. For predefined macros, prefix the macro name with "predefined."
  - When an object is created from a template, the name is appended with a unique number, starting with 0 (for example, **server0** and **server1**).
  - You can see the name for each macro from the Deploy OS Images dialog on the Custom Settings tabs by hovering over the Help icon ( ) next to each custom setting.
  - For a list of predefined macros, see Predefined macros. For information about custom configuration settings and macros, see Custom macros.
- XClarity Administrator provides the following predefined macros that are used to communicate status from the OS installer, as well as several other critical installation steps. It is strongly recommended that you include these macros in unattend file (see Injecting predefined and custom macros to an unattend file).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

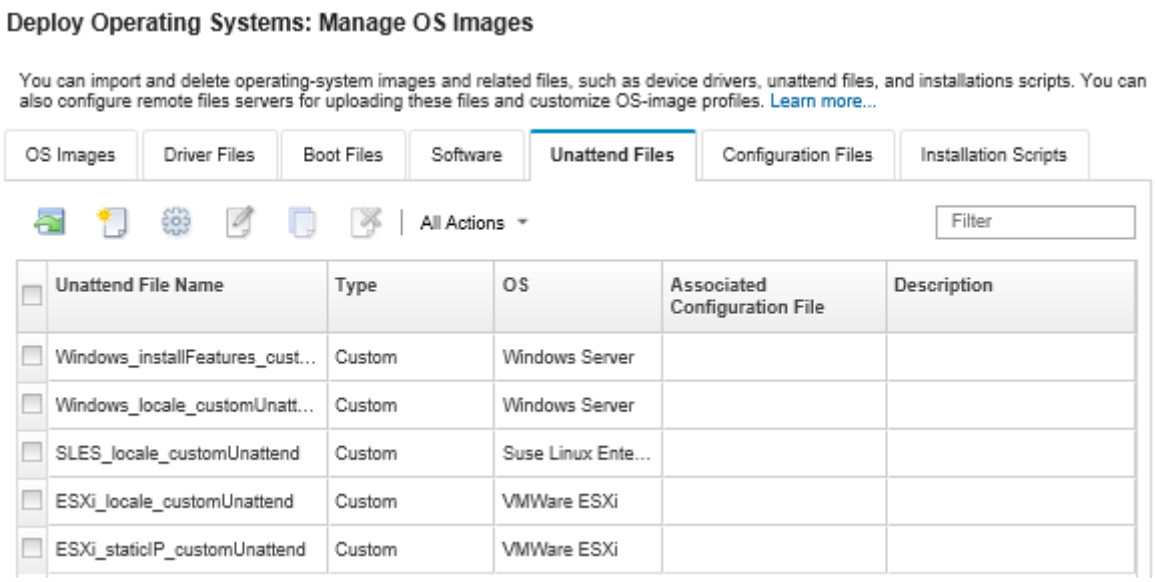
The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

To import unattended files into the OS-images repository, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Unattend Files** tab.



Step 3. Click the **Import File** icon ( ). The Import File dialog is displayed.

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Select the operating-system type.

Step 7. Enter the file name of the unattend file, or click **Browse** to find the file that you want to import.

Step 8. Optional: **Optional:** Enter a description for the unattend file.

Tip: Use the **Description** field to distinguish between custom files with the same name.

Step 9. Optional: **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:
- **MD5**
- **SHA1**
- **SHA256**

Step 10. Click **Import**.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

After you finish

The unattend-file image is listed on the **Unattend Files** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create an unattend file by clicking the **Create** icon ( ).

  The editor identifies the location of any errors that are found in the file. Note that some messages are English only.
- Associate an unattend file with a configuration-settings file (see Associating an unattend file with a configuration settings file).
- View and modify an unattend file by clicking the **Edit** icon ( ).

  The editor identifies the location of any errors that are found in the file. Note that some messages are English only.
- Copy an unattend file by clicking the **Copy** icon ( ).

  If you copy an unattend file that is associated with a configuration-settings file, the associated configuration-settings file is also copied and the association is automatically created between both copied files.
- Remove selected unattend files by clicking the **Delete** icon ( ).
- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).

For information about adding an unattend file to a customized OS image profile, see Creating a custom OS-image profile.

Injecting predefined and custom macros to an unattend file

You can add predefined and custom macros to an unattend file.

About this task

Macros give you the ability to add dynamic data (configuration settings) to an unattend file. You provide the data values when the OS-image profile is deployed.

Lenovo XClarity Administrator provides a set of *predefine* macros that you can add to an unattend file without associating a custom configuration-settings file. For a list of predefined macros, see Predefined macros.

It is strongly recommended that you include the following predefined macros in the custom unattend files.

- **#predefined.unattendSettings.preinstallConfig#** and **#predefined.unattendSettings postinstallConfig#**. Used to communicate status from the OS installer, as well as several other critical installation steps.

  See the following example OS-deployment scenarios for more information about how to include the installation-configuration macros.
  - Deploying RHEL and a Hello World PHP application using a custom unattend file
  - Deploying SLES 12 SP3 with a configurable locale and NTP servers
  - Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address
  - Deploying Windows 2016 with custom features
- **#predefined.unattendSettings.networkConfig#**. (For ESXi and RHEL only) Enables XClarity Administrator to configure the network. This macro uses the network settings that are specified on the Deploy OS Images page. If you do not include this macro in the unattend file or if the network settings are not defined in XClarity Administrator, you must configure the IP interface as part of the unattend file so that the host has a network route back to XClarity Administrator.

  See the following example OS-deployment scenarios for more information about how to include the network-configuration macro.
  - Deploying RHEL and a Hello World PHP application using a custom unattend file
  - Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address
- **#predefined.unattendSettings.storageConfig#**. (For ESXi and RHEL only) Enables XClarity Administrator to configure storage on the host. This macro uses the storage settings that are specified on the Deploy OS Images page. If you do not include this macro in the unattend file or if the storage settings are not defined in XClarity Administrator, you must specify the storage configuration in unattend file.

  See the following example OS-deployment scenarios for more information about how to include the storage-configuration macro.
  - Deploying RHEL and a Hello World PHP application using a custom unattend file
  - Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address

You can create *custom* macros by creating a configuration-settings file and then associating the unattend file with a custom configuration-settings file. When you import the custom configuration-settings file, XClarity Administrator creates a macro for each configuration setting in the file.

Procedure

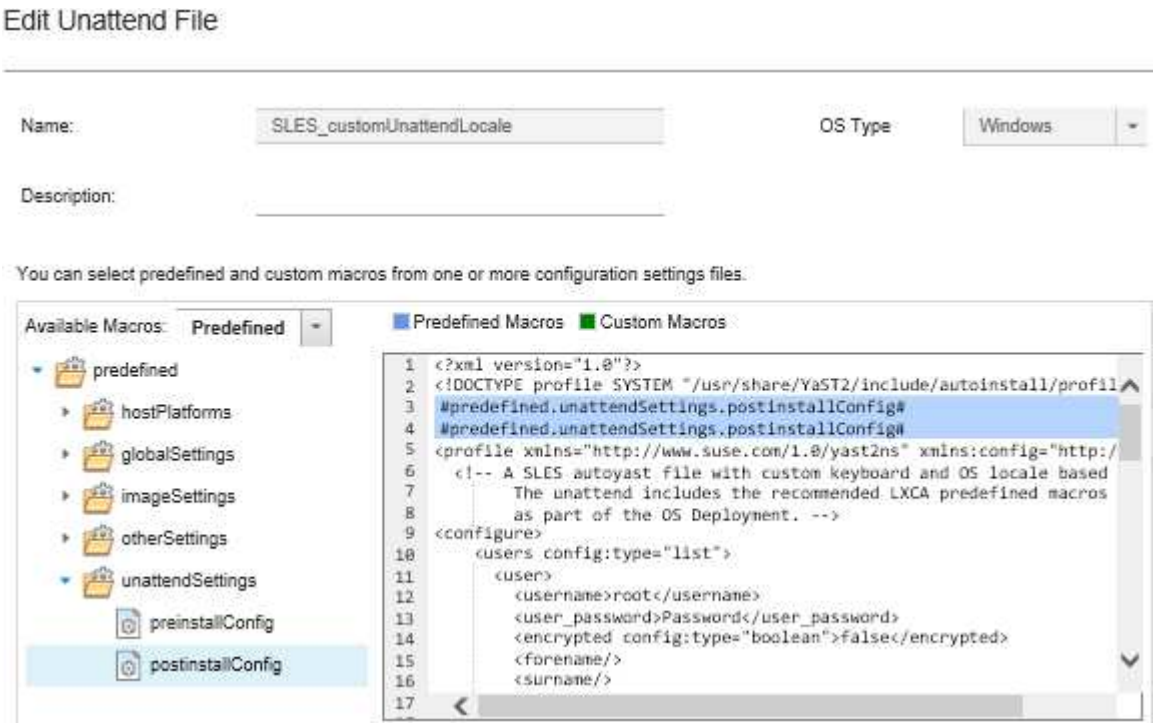
Complete the following steps to add macros to an unattend file.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Unattend Files** tab.

Step 3. Select the unattend file that you want to edit.

Step 4. Click the **Edit** icon ( ) display the Edit Unattend File dialog.



Step 5. Add the recommended predefined macros, for example:

1. Place the cursor in the unattend file anywhere after line 1 (after the <xml> tag).
2. Expand the **predefine → unattendSettings** list in the list of available macros.
3. Click the **preinstallConfig** and **postinstallConfig** to add the required predefined macros to the unattend file.

   The following code is added to the file:

   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#

Step 6. Add additional predefined or custom macros by placing the cursor in the correct location in unattend file and then clicking the macro from the list.

Step 7. Click **Save**.

Associating an unattend file with a configuration settings file

You can associate (bind) configuration settings to an unattend file, and then add the associated custom macros to the unattend file.

About this task

You can add predefined macros to an unattend file without associating a custom configuration settings file.

You cannot edit configuration settings files that are associated with unattend files. However, you can copy an associated file and then edit the copy.

Procedure

Complete the following steps to associate an unattend file with a configuration-settings file.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Unattend Files** tab.

Step 3. Select the custom attend file.

Step 4. Click the **Associate a Configuration File** icon ( ) to display the Associate an Unattend File dialog.

Step 5. Select a configuration-settings file to associate with the unattend file.

Step 6. Add predefined and custom macros to the unattend file by placing the cursor at the location in the editor where you want to add the macro and then clicking the macro in the available list (see Injecting predefined and custom macros to an unattend file).

You can inject macros in the unattend file using the unique name of the object. For nested name objects, separate each object using a period (for example, `server_specific_settings.server.locale`). Note that you do not include the top-most name.

Step 7. Click **Associate** to bind the files together.

Importing custom installation scripts

You can import installation scripts into the OS images repository. These files can then be used to customize Linux and Windows images.

About this task

Currently, only post-installation scripts are supported.

The following table lists the file types for installation scripts that Lenovo XClarity Administrator supports for each operating system. Note that certain operation system versions do not support all of the file types that XClarity Administrator supports (for example, some RHEL versions might not include Perl in the minimal profile and, therefore, Perl scripts will not run). Ensure that you use the correct file type for the operating system versions that you want to deploy.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Azure Stack HCI	Not supported	
Microsoft Windows Hyper-V Server	Not supported	
Microsoft® Windows® Server	Command file (.cmd), PowerShell (.ps1)	The default custom data and files path is `C:\lxca`. For more information about installation scripts, see the Add a custom script to Windows Setup webpage

Operating system	Supported File Types	More information
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm or .pl), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the RHEL: Post-installation Script webpage.
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm or .pl), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the SUSE: Custom user script webpage
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	Bash (.sh), Python (.py)	The default custom data and files path is `/home/lxca`. For more information about installation scripts, see the VMware: Installation and Upgrade Scripts webpage

Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

After the data is gathered during OS deployment, XClarity Administrator creates an instance of the configuration settings file (which includes the custom settings in the selected file and a subset of predefined settings) on the host system that can be used by the post installation script.

You can inject predefined and custom macros (configuration settings) in the post-installation script using the unique name of the object. Predefined values are dynamic based on the XClarity Administrator instances. Custom macros are dynamic based on user input that is specified during OS deployment.

Notes:

- Surround the macro name with a hash symbol (#).
- For nested objects, separate each object name using a period (for example, **#server_settings.server0.locale#**).
- For custom macros, do not include the top-most object name. For predefined macros, prefix the macro name with "predefined."
- When an object is created from a template, the name is appended with a unique number, starting with 0 (for example, **server0** and **server1**).
- You can see the name for each macro from the Deploy OS Images dialog on the Custom Settings tabs by hovering over the Help icon ( ) next to each custom setting.
- For a list of predefined macros, see Predefined macros. For information about custom configuration settings and macros, see Custom macros.

The recommended predefined macros in the unattend file report final operating-system deployment status and report status when downloading and running post-installation scripts. You can modify the post-installation script to include custom status reporting, depending on the target operating system. For more information, see Adding custom status reporting to installation scripts.

Procedure

To import installation scripts into the OS-images repository, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Installation Scripts** tab.

Step 3. Click the **Import File** icon ( ). The Import Installation Script dialog is displayed.

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Select the operating-system type.

Step 7. Enter the file name of the installation script, or click **Browse** to find the file that you want to import.

Step 8. Optional: **Optional:** Enter a description for the installation script.

Tip: Use the **Description** field to distinguish between custom files with the same name.

Step 9. Optional: **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:

- **MD5**
- **SHA1**
- **SHA256**

Step 10. Click **Import**.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

After you finish

The installation scripts are listed on the **Installation Scripts** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).
- Remove selected installation scripts by clicking the **Delete** icon ( ).

For information about adding an installation script to a customized OS image profile, see Creating a custom OS-image profile.

Adding custom status reporting to installation scripts

The recommended predefined macros in the unattend file report final operating-system deployment status and report status when downloading and running post-installation scripts. You can include additional status reporting in the post-installation scripts.

Linux

For Linux, you can use the following **curl** command to report status.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Where <*status_ID*> can be one of the following values.

- **44**. Workload deployment succeeded
- **45**. Workload deployment is running with warning
- **46**. Workload deployment failed
- **47**. Workload deployment message
- **48**. Custom post-install script error

Note that the **curl** command uses predefined macros for the HTTPS URL that Lenovo XClarity Administrator uses for reporting status (**predefined.otherSettings.statusSettings.urlStatus**) and for the folder that contains the certificates that are needed to access the urlStatus web service from the host OS on first boot (**predefined.otherSettings.statusSettings.certLocation**).The following example reports that an error occurred in the post-installation script.

The following example reports that an error occurred in the post-installation script.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

For Wiindows, you can import the **LXCA.psm1** script and then call the following commands to report status.

- **initializeRestClient**

  Initializes the REST client. Use the following syntax to run this command. This command is required before running the reporting commands.

  ```
  initializeRestClient
  ```

- **testLXCAConnection**

Verifies that the XClarity Administrator can connect to the host server. Use the following syntax to run this command. This command is optional but recommended in the installation script before running the reporting commands..

```
testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"
```

- **reportWorkloadDeploymentSucceeded**

  Reports a successful-completion message to be logged in the XClarity Administrator jobs log. Use the following syntax to run this command.

  Tip: If the **#predefined.unattendSettings.reportWorkloadNotComplete#** macro is included in a custom unatted file or post-installation script, include the **reportWorkloadDeploymentSucceeded** command in the post-installation script to signal a successful-completion. Otherwise, XClarity Administrator automatically reports a complete status after all post-installation scripts are run.

  ```
  reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#"
  ```

- **reportWorkloadDeploymentRunningWithWarning**

  Reports a warning message to be logged in the XClarity Administrator jobs log. Use the following syntax to run this command.

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- **reportWorkloadDeploymentFailed**

  Reports a failure message to be logged in the XClarity Administrator jobs log. Use the following syntax to run this command.

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
  ```

- **reportCustomPostInstallScriptError**

  Reports a post-installation script error message to be logged in the XClarity Administrator jobs log. Use the following syntax to run this command.

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- **reportWorkloadDeploymentMessage**

  Reports a general message to be logged in the XClarity Administrator jobs log without affecting the state of the deployment. Use the following syntax to run this command.

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

Where <*message_text*> is the message that you want to return to XClarity Administrator for each status condition.

Note that these commands use predefined macros for the IP address of the XClarity Administrator instance (**#predefined.otherSettings.lxcaIp#**) and for the UUID of the host server to which the operating system is to be deployed (**#predefined.hostPlatforms.uuid#**).

The following example is a PowerShell installation script that installs Java and reports an error if the installation fails

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"
```

```
Write-Output "Reporting status to Lenovo XClarity Administator..."
   reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
   -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java...."
   Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
   [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
   reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
      -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

Importing custom software

You can import software into the OS images repository. These files can then be used to customize Linux and Windows images

About this task

The custom software files are installed after the operating-system deployment and post-installation scripts are complete.

The following file types are supported for custom software.

Operating system	Supported File Types	More information
CentOS Linux	Not supported	
Microsoft® Windows® Azure Stack HCI	Not supported	
Microsoft Windows Hyper-V Server	Not supported	
Microsoft Windows® Server	A .zip file containing the software payload.	The default custom data and files path is `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.
Ubuntu	Not supported	
VMware vSphere® Hypervisor (ESXi) with Lenovo Customization	A .tar.gz file containing the software payload	The default custom data and files path is `/home/lxca`.

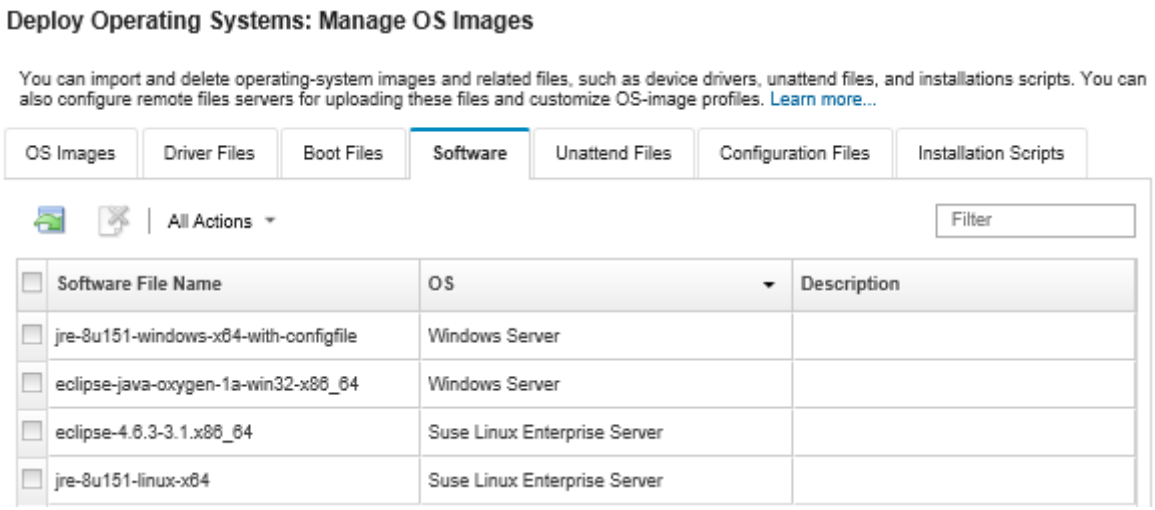
Note: The OS images repository can store an unlimited number of predefined and custom files, if space is available to store the files.

Procedure

To import software into the OS-images repository, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

Step 2. Click the **Software** tab.



Step 3. Click the **Import File** icon ( ). The Import Installation Script dialog is displayed.

Step 4. Click the **Local Import** tab to upload files from the local system, or click the **Remote Import** tab to upload files from a remote file server.

Note: To upload a file from a remote file server, you must first create a remote file-server profile by clicking the **Configure File Server** icon ( ). For more information, see Configuring a remote file server .

Step 5. If you chose to use a remote file server, select the server that you want to use from the **Remote File Server** list.

Step 6. Select the operating-system type.

Step 7. Enter the file name of the software file, or click **Browse** to find the file that you want to import.

Step 8. Optional: **Optional:** Enter a description of the software file.

Tip: Use the **Description** field to distinguish between custom files with the same name.

Step 9. Optional: **Optional:** Select a checksum type to verify that the file being uploaded is not corrupt, and copy and paste the checksum value in the provided text field.

If you select a checksum type, you must specify a checksum value to check the integrity and security of the uploaded file. The value must come from a secure source from an organization that you trust. If the uploaded file matches with the checksum value, it is safe to proceed with deployment. Otherwise, you must upload the file again or check the checksum value.

Three checksum types are supported:

- **MD5**
- **SHA1**
- **SHA256**

Step 10. Click **Import**.

Tip: The file is uploaded over a secure network connection. Therefore, network reliability and performance affects how long it takes to import the file.

If you close the web browser tab or window in which the file is being uploaded locally before the upload completes, the import fails.

After you finish

The installation scripts are listed on the **Software** tab on the Manage OS Images page.

From this page, you can perform the following actions.

- Create a remote-file-server profile by clicking the **Configure File Server** icon ( ).
- Remove selected software files by clicking the **Delete** icon ( ).

For information about adding a software file to a customized OS image profile, see Creating a custom OS-image profile.

Creating a custom OS-image profile

You can add custom device drivers, boot files (Windows only), configuration settings, unattend files, installation scripts, and software to a predefined OS-image profile that exists in the OS-images repository. When you add files to an OS image, Lenovo XClarity Administrator creates a custom profile for that OS image. The custom profile includes the custom files and installation options.

Before you begin

The custom files that you want to add must exist in the OS-images repository (see Importing boot files, Importing device drivers, Importing custom configuration settings, Importing custom unattend files, Importing custom installation scripts, and Importing custom software).

Procedure

To customize an OS image, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.

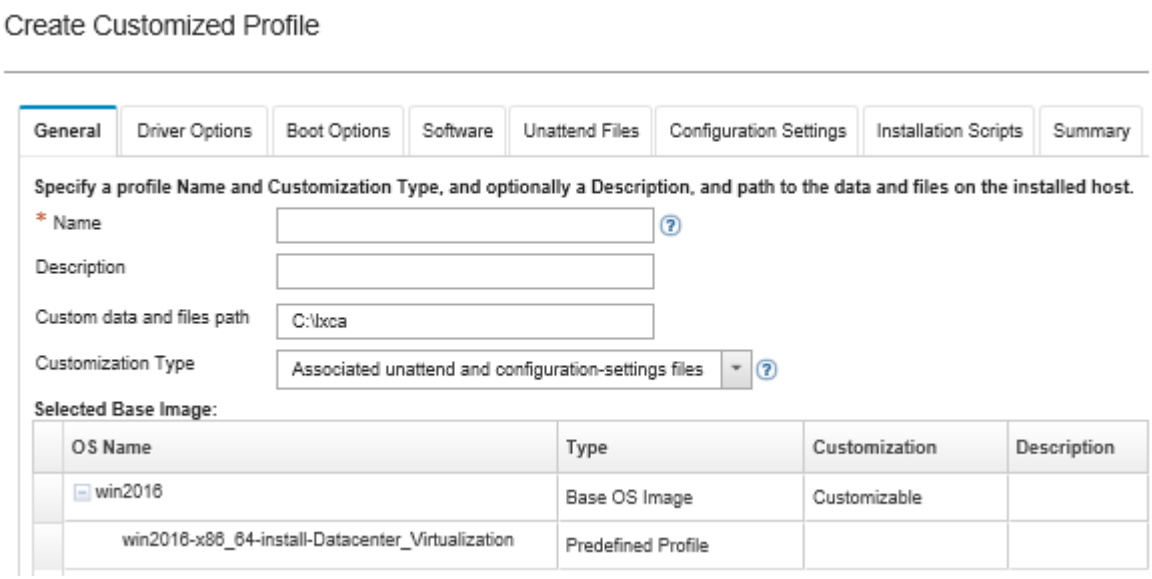
Step 2. Click the **OS Images** tab.

Step 3. Select the predefined OS-image profile that you want to customize.

The **Customization** column identifies which OS images can be customized. Click the **Help** icon ( ) for more information about the customization for a specific OS image.
- **Customizable**. The OS image support customization but is not customized.
- **Non Customizable**. The OS image does not support customization.

Note: You can import additional base OS images (in .iso format) from a local or remote system by clicking the **Import File** icon ( ).

Step 4. Click the **Create Customized Profile** icon ( ). The New Custom OS Image dialog is displayed.



Step 5. On the **General** tab, specify a name, description, path for the custom files and deployment data on the deployment host, and customization type for the new customized OS-image profile.

The customization type can be one of the following:
- **Only unattend files**
- **Only configuration files**
- **Unassociated unattend and configuration files**
- **Associated unattend and configuration files**
- **None**

Step 6. Click **Next**.

Step 7. On the **Device Drivers** tab, select the device drive that you want to add to the Linux OS-image profile.

For a list of supported formats, see Importing device drivers.

The selected file is applied after you complete the configuration wizard.

Note: You can import additional device drivers from a local or remote system by clicking the **Import File** icon ( ).

Step 8. Click **Next**.

Step 9. (Windows only) On the **Boot Options** tab, select the boot files that you want to add to the Windows OS-image profile.

For a list of supported formats, see Importing boot files.

The selected file is applied after you complete the configuration wizard.

Step 10. Click **Next**.

Step 11. On the **Configuration Settings** tab (if applicable), select one or more custom configuration files that you want to add to the OS-image profile. You can select at most one file

Step 12. Click **Next**.

Step 13. On the **Unattend Files** tab:

a. Select the unattend file that you want to add to the OS-image profile.

For a list of supported formats, see Importing custom unattend files.

The selected file is applied after you complete the configuration wizard.

b. Select a configuration file to associate with the unattend file from the **Associated Configuration File** column

c. Optionally select custom macros that are available in the selected configuration file or add custom macros in .xml format.

Step 14. Click **Next**.

Step 15. On the **Installation Scripts** tab (if applicable), select the installation scripts that you want to add to the Windows OS-image profile. You can select at most one post-installation script.

For a list of supported formats, see Importing custom installation scripts.

The selected file is applied after you complete the configuration wizard.

Note: You can import additional installation scripts from a local or remote system by clicking the **Import File** icon ( ).

Step 16. Click **Next**.

Step 17. On the **Software** tab, select the software that you want to add to the Linux OS-image profile.

For a list of supported formats, see Importing custom software.

The selected file is applied after you complete the configuration wizard.

Note: You can import additional software from a local or remote system by clicking the **Import File** icon ( ).

Step 18. Click **Next**.

Step 19. Review the settings on the **Summary** tab, and click **Customize** to create the customized OS-image profile.

After you finish

The customized OS images profile is listed under the base operating system on the **OS Images** tab on the Manage OS Images page.

From this page, you can perform the following actions:

- Import a customized OS image profile and apply to a base OS image by clicking **Import/Export Profile → Export Customized Profile Image** (see Importing a customized OS image profile).
- Export a selected customized OS image profile by clicking **Import/Export Profile → Export Customized Profile Image**.
- Modify a selected customized OS image profile by clicking the **Edit** icon ( ).
- Remove a selected customized OS image profile by clicking the **Delete** icon ( ).

Configuring global OS-deployment settings

Global settings serve as defaults settings when operating systems are deployed.

About this task

From the Global Settings page, you can configure the following settings:

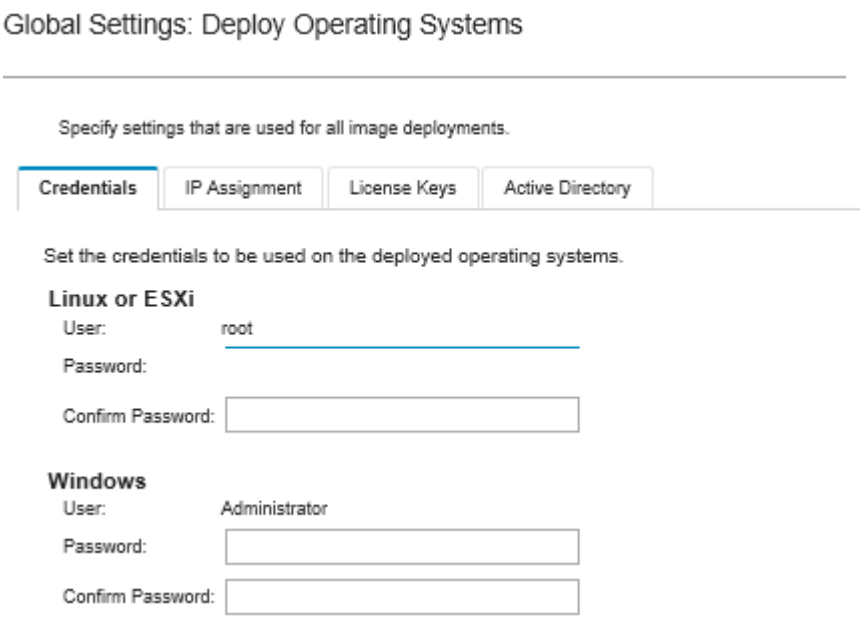
- The password for the administrator user account to be used for deploying the operating systems
- The method to use to assign IP addresses to servers
- License keys to use when activating installed operating systems
- Optionally join an Active Directory domain as part of the Windows operating-system deployment

Procedure

To configure the global settings to be used for all servers, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy OS Images page.

Step 2. Click the **Global Settings** icon ( ) to display the Global Settings: Deploy Operating Systems dialog.



Step 3. On the **Credentials** tab, enter the password for the administrator account to be used to log in to the operating system.

Step 4. On the **IP Assignment** tab, select the following options.

a. **Optional:** Select **Use VLANs** to allow configuring VLAN settings in the Network Settings dialog (see Configuring network settings for managed servers).

Notes: Notes:

- VLAN tagging is not supported for Linux operating-system deployments.
- VLAN tagging is not supported for operating-system deployments on ThinkServer devices.
- VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server.

b. Select the method for assigning IP addresses when configuring the deployed operating system:

Note: The XClarity Administrator network interface that is used for management must be configured to connect to the baseboard management controller using the same IP address

method that you choose on the Global Settings: Deploy Operating Systems dialog. For example, if XClarity Administrator is set up to use eth0 for management, and you choose to use manually assigned static IPv6 addresses when configuring the deployed OS, then eth0 must be configured with an IPv6 address that has connectivity to the baseboard management controller.

- **Manually assign a static IPv4 address**. If you choose to assign static IPv4 addresses, ensure that you configure the static IPv4 address, gateway address, and subnet mask for the server before deploying the operating system (see Configuring network settings for managed servers).
- **Use Dynamic Host Configuration Protocol (DHCP) to assign the addresses**. If you already have an existing DHCPv4 infrastructure in your network, you can use that infrastructure to assign IP addresses to servers.

  Note: DHCP IPv6 is not supported for operating-systems deployment.
- **Manually assign a static IPv6 address**. If you choose to assign static IPv6 addresses, ensure that you configure the static IPv6 address, gateway address, and subnet mask for the server before deploying the operating system (see Configuring network settings for managed servers).

Step 5. Optional: **Optional:** On the **License Keys** tab, specify the global volume-license keys to use when activating installed Windows operating systems.

When you specify global volume-license keys on this tab, you can select the specified license keys for any Windows OS-image profiles from the Deploy OS Images page.

Tip: XClarity Administrator supports global volume-license keys for Windows installations and individual retail-license keys for both Windows and VMware ESXi. You can specify individual retail-license keys as part of the deployment procedure (see Deploying an operating-system image).

Step 6. Optional: **Optional:** On the **Active Directory** tab, configure the Active Directory settings for Windows operating-system deployments. For information about integrating with Active Directory, see Integrating with Windows Active Directory.

Step 7. Click **OK** to close the dialog.

Configuring network settings for managed servers

Network settings are configuration options that are specific to each server. You must configure the network settings for a managed server before you can deploy an operating system to that server.

About this task

If you are using DHCP to assign IP addresses dynamically, you must configure the MAC address.

If you are using static IP addresses, you must configure the following network settings for a specific server before you can deploy an operating system to that server. After these settings are configured, the deployment status of the server changes to “Ready.” (Note that some fields are not available for static IPv6 addresses.)

- Hostname

  The hostname must comply with the following rules:
  - The hostname of each managed server must be unique.
  - The hostname can contain strings (labels) that are separated by a period (.).
  - Each label can contain ASCII letters, digits, and dashes (-); however, the string cannot start or end with a dash and cannot contain all digits.

  - The first label can be 2 - 15 characters in length. Subsequent labels can be 2 – 63 characters in length.
  - The total length of the hostname must not exceed 255 characters.
- MAC address of the port on the host where the operating system is to be installed.

  The MAC address is set to AUTO by default. This setting automatically detects the Ethernet ports that can be configured and used for deployment. The first MAC address (port) that is detected is used by default. If connectivity is detected on a different MAC address, the XClarity Administrator host is automatically restarted to use the newly detected MAC address for deployment.

  You can determine the status of the MAC address port that is used for OS deployment from the **MAC address** drop-down menu on the Network Settings dialog. If multiple ports are up or if all ports are down, AUTO is used by default.

  Notes:

  - Virtual network ports are not supported. Do not use one physical network port to simulate multiple virtual network ports.
  - When the server's network setting is set to AUTO, XClarity Administrator can automatically detect network ports in slots 1 – 16. At least one port in slots 1 – 16 must have a connection to XClarity Administrator.
  - If you want to use a network port in slot 17 or greater for the MAC address, you cannot use AUTO. Instead, you must set the server's network setting to the MAC address of the specific port that you want to use.
  - For ThinkServer servers, not all host MAC addresses are displayed. In most cases, MAC addresses for AnyFabric Ethernet adapters are listed on the Edit Network Settings dialog. MAC addresses for other Ethernet adapters (such as the Lan-On-Motherboard) are not listed. In cases where the MAC address for an adapter is not available, use the AUTO method for non-VLAN deployments.
- IP address and subnet mask
- IP gateway
- Up to two domain name system (DNS) servers
- Maximum transmission unit (MTU) speed
- VLAN ID, if VLAN IP mode is enabled

If you choose to use VLANs, you can assign a VLAN ID to the host network adapter that is being configured.

Procedure

To configure network settings for one or more servers, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy Operating System: Deploy OS images page.

Step 2. Select one or more servers to configure. You can select up to 28 servers to be configured at one time.

Step 3. Click **Changed Selected → Network Settings** to display the Edit Network Settings page.

Step 4. Complete the fields in the table for each server.

Tip: As an alternative to filling in each row, you can update all rows in the table for some of the fields:

a. Click **Change All Rows → Hostname** to set the hostnames for all servers, using either a predefined or a custom naming scheme.

b. Click **Change All Rows → IP address** to assign a range of IP addresses, subnet mask, and gateway. The IP address is assigned for each server, starting with the first IP address and

ending with the last IP address that is displayed. The subnet mask, and gateway IP address are applied to each server.

c. Click **Change All Rows → Domain Name System (DNS)** to set the DNS servers to be used by the operating system for DNS lookup. If the network defines DNS servers automatically, or if you do not want to define DNS servers, select **None**.

d. Click **Change All Rows → Maximum Transmission Unit (MTU)** to set the MTU to be used on the configured Ethernet adapter on the deployed operating system.

e. Click **Change All Rows → VLAN ID** to set a specific VLAN ID for operating-system VLAN tagging.

   You can specify a value from 1 – 4095. The default value is 1, which means VLAN mode is not used.

   This option is available only when Use VLANs is enabled on the Global Settings dialog (see Configuring global OS-deployment settings).

   Important:

   - Only specify a VLAN ID when a VLAN tag is required to function on the network. **Using VLAN** tags can affect the network routability between the host operating system and the XClarity Administrator.
   - Chassis or top-of-rack switches must be independently configured to handle VLAN tagged packets. Ensure that XClarity Administrator and the data network are configured to handle these packets correctly.
   - VLAN mode is supported only for servers that have MAC addresses in their inventory. If AUTO is the only MAC address that is available for a server, then VLANs cannot be used to deploy operating systems to that server.
   - VLAN tagging is not supported for Linux operating-system deployments; however, if you want to deploy with VLAN on some servers and also deploy on other servers without VLAN at the same time, you can force deploying under VLAN mode by setting the VLAN ID to 1.

Step 5. Click **OK** to save the settings. Settings are saved and persistent only in your web browser's local storage cache.

Results

Each configured server now shows **Ready** as the deployment status on the Deploy Operating System: Deploy OS images page.

Choosing the storage location for managed servers

Choose the preferred storage location where you want to deploy the operating-system image for one or more servers.

Before you begin

Review storage and boot-option considerations before choosing a storage location (see Operating-system deployment considerations).

You can deploy an operating system to the following types of storage:

- **Local disk drive**

  Only disks attached to a RAID-controller or SAS/SATA HBA are supported.

Lenovo XClarity Administrator installs the operating-system image on the first enumerated local RAID disk in the managed server.

If the RAID configuration on the server is not configured correctly, or if it is inactive, the local disk might not be visible to Lenovo XClarity Administrator. To resolve the issue, enable the RAID configuration through configuration patterns (see Defining local storage) or through the RAID management software on the server.

Notes:

- If an M.2 drive is also present, the local disk drive must be configured for hardware RAID.
- If an SATA adapter is enabled, the SATA mode *must not* be set to "IDE."
- For ThinkServer servers, operating systems can be deployed only to the local disk. SAN storage and embedded hypervisors are not supported.
- For ThinkServer servers, configuration is available only through the RAID management software on the server.

For an example scenario for deploying VMware ESXi 5.5 to a locally installed disk drive, see Deploying ESXi to a local hard drive.

- **(ESXi only) Embedded hypervisor (USB or SD media adapter)**

  This location is applicable only when a VMware ESXi image is being deployed to managed servers.

  The embedded hypervisor can be one of the following devices:

  - IBM License USB key (PN 41Y8298) or Lenovo Licensed USB key that is mount to a specific port on one of the following servers:
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - SD media adapter that is installed on the following servers:
    - Flex System x240 M5
    - System x3500 M5
    - System x3550 M5
    - System x3650 M5

    In addition, the drive must be configured as follows:
    - The appropriate drives on the media adapter must be defined.
    - The mode of the SD media adapter must be set to **Operational**.
    - The owner must be set to System or System Only.
    - Access must be set to Read/Write.
    - The drive must be assigned a LUN number of 0.

    Important: If the SD Media Adapter is not configured correctly, operating system deployment to the SD Media Adapter from the Lenovo XClarity Administrator will not be successful.

    You can change the mode of the SD Media Adapter to **Configuration** and configure the media adapter through the management controller CLI using the **sdraid** command. For additional information about setting the mode of the SD Media Adapter and configuring the adapter from the CLI, see the Integrated Management Module II online documentation.

If two hypervisor keys are installed on the managed server, the VMware installer selects the first enumerated key for deployment.

Note: Attempting to deploy Microsoft Windows to a managed server that has a hypervisor key installed might cause issues even if you do not select the embedded hypervisor key. If Windows deployment errors occur, remove the embedded hypervisor key from the managed server, and attempt to deploy Microsoft Windows to that server again.

- **M.2 drive**

  Lenovo XClarity Administrator installs the operating-system image on the first M.2 drive that is configured on the managed server.

  M.2 storage is supported only on ThinkSystem servers.

  Attention: If a managed device has both local drives (SATA, SAS, or SSD) that are not configured for hardware RAID and M.2 drives, you must disable the local drives if you want to use M.2 drives, or you must disable the M.2 drives if you want to use local drives. You can disable on-board storage controller devices and legacy and UEFI storage option ROMs using the using Configuration Patterns by selecting Disable local disk on the Local Storage tab of the wizard or by creating a Configuration Pattern from an existing server and then disabling the M.2 devices in the extended UEFI pattern.

- **SAN storage**

  Lenovo XClarity Administrator installs the operating-system image on the SAN boot target that is configured on the managed server.

  The following protocols are supported.
  - Fibre Channel
  - Fibre Channel over Ethernet
  - SAN iSCSI (using only Emulex VFA5.2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW or Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter and FCoE/iSCSI SW adapters)

  On managed rack servers, you can only deploy Windows or RHEL to SAN storage. Ensure that the SAN boot target is configured on the managed servers. You can also configure the FC SAN boot target using a server pattern (see Defining boot options)

  When deploying VMware ESXi:

  - Local hard disks must be disabled or removed from the server. You can disable the local hard disks using server patterns (see Defining local storage).
  - If multiple SAN volumes are available, only the first volume is used for deployment.

  Ensure that the OS volume to which you are installing is the only volume that is visible to the operating system.

  For an example scenario for deploying VMware ESXi 5.5 to SAN volumes that are attached to servers, see Deploying ESXi to SAN storage.

Note: Each server must have a hardware RAID adapter or SAS/SATA HBA that is installed and configured. The software RAID that is typically present on the onboard Intel SATA storage adapter or storage that is set up as JBOD are not supported; however, if a hardware RAID adapter is not present, setting the SATA adapter to **AHCI SATA mode** enabled for operating-system deployment or setting unconfigured good disks to JBOD might work in some cases. For more information, see OS installer cannot find the disk on which you want to install XClarity Administrator in the XClarity Administrator online documentation.

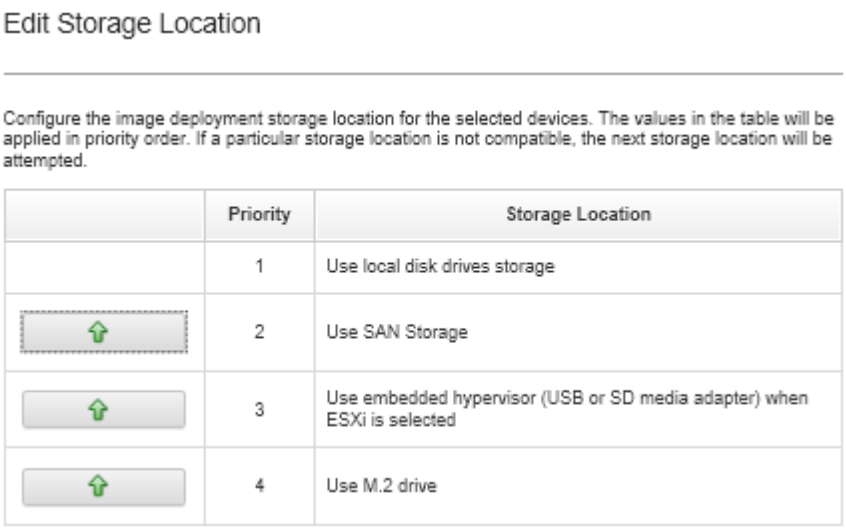
Procedure

To choose storage location for one or more managed servers, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy OS Images page.

Step 2. Select the servers for which you want to change the storage settings.

Step 3. Click **Change Selected → Storage Location** to change the priority order of storage locations for all selected servers. If the first storage location is not compatible, the next storage location is attempted.



You can set the priority for the following storage locations:
- **Use local disk drive storage**
- **Use embedded hypervisor (USB or SD media adapter) when ESXi is selected**
- **Use M.2 drive**
- **Use SAN storage**

Step 4. For each server, select the preferred storage location where you want to deploy the operating-system image from the **Storage** column. You can choose from the following values, which correspond to values in the previous step.
- **Local Disk Drive**
- **Embedded Hypervisor**
- **M.2 Drive**
- **SAN Storage**

If you select **SAN Storage**, a dialog is displayed to configure the SAN volume. Ensure that the target SAN volume is reachable during deployment.

If the selected storage location is not compatible with the server, Lenovo XClarity Administrator attempts to deploy the operating system to the next storage location in the priority defined in the previous step.

Deploying an operating-system image

You can use Lenovo XClarity Administrator to deploy an operating-system image to up to 28 servers concurrently.

Before you begin

Read the operating-system deployment considerations before you attempt to deploy operating systems on your managed servers (see Operating-system deployment considerations).

On the **OS Images** tab, ensure that the **Deploy Status** of the operating system that you want to deploy is set to “Ready.” To deploy the Windows operating system, a WinPE boot file is required. If a matching WinPE file

is not available, the **Deploy Status** is set to “Not Ready” and the operating system cannot be deployed. You must manually download and import a WinPE file (see Importing boot files).

From the Manage OS Images page, you can filter the list of OS images by clicking **Show All → Deploy Status**. You can filter the list to show only servers that have a status of “Ready,” “Not Ready,” and “Warning”.

Note: If the deployment status for an operating-system image is “Not Ready,” the operating system is not included in the list of deployable operating systems.

The English locale is supported by default. To specify a language-specific locale, you must use a custom configuration file and unattend file. For more information, see Deploying SLES 12 SP3 with a configurable locale and NTP servers and Deploying Windows 2016 for Japanese .

Note: Operating-system deployment to non-RAID attached storage is not supported.

Attention: If the server currently has an operating system installed, deploying an OS-image profile will overwrite the current operating system.

Procedure

To deploy an operating-system image to one or more managed servers, complete the following steps.

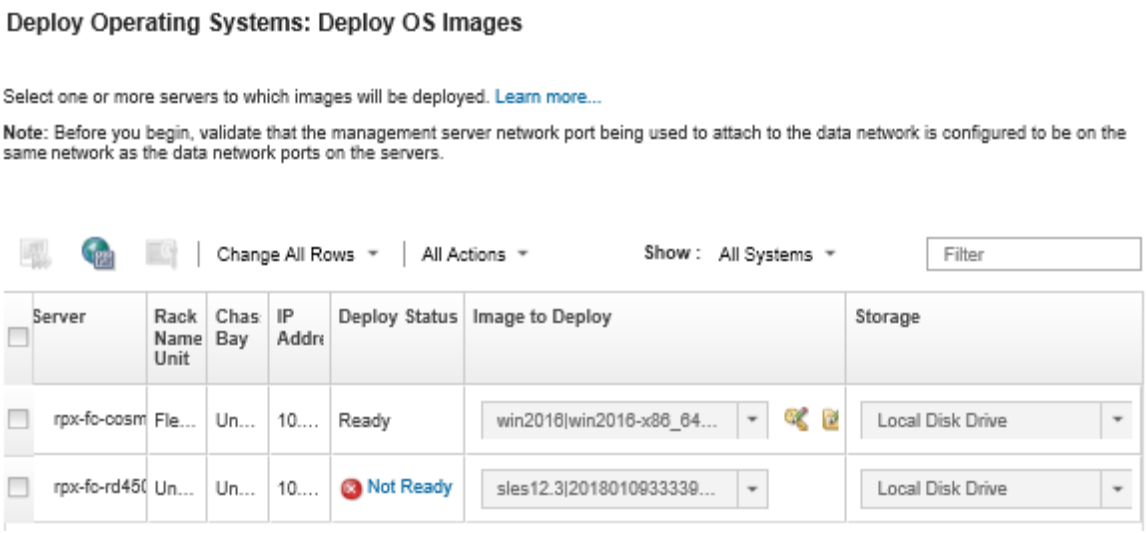
Step 1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy Operating System: Deploy OS images page.

Tip: For scalable complexes, the operating system is deployed on the primary partition; therefore, only the primary partition is included in the server list.

Step 2. Select one or more servers to which the operating system is to be deployed. You can deploy an operating system on up to 28 servers at one time.

You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed devices by selecting an option in the **Show** menu to list only devices in a specific chassis, rack, or group or by entering text (such as a name or IP address) in the **Filter** field.

Tip: You can choose multiple compute nodes from multiple chassis if you intend to deploy the same operating system to all compute nodes.



Step 3. Click **Change Selected → Network Settings** to configure network settings.

For more information, see Configuring network settings for managed servers.

Step 4. For each server, select the OS-image profile to be deployed from the drop-down list in the **Image to Deploy** column.

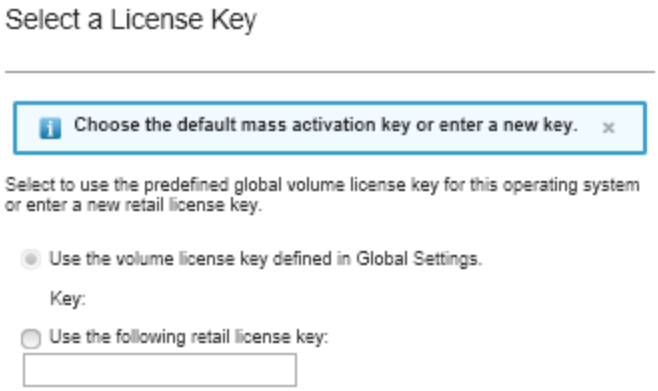
Ensure that you select an OS-image profile that is compatible with the selected server. You can determine compatibility from profile attributes that are listed the **Attribute** column on the Manage OS Images page. For information about profile attributes, see Operating-system image profiles.

Step 5. For each server, click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.

XClarity Administrator supports default volume-license keys for Windows installations and individual retail keys for both Windows and VMware ESXi.

To use the global volume-license key that you specified in the Global Settings dialog, select **Use the volume license key defined in Global Settings**. For more information about global volume-license keys, see Configuring global OS-deployment settings.

To use an individual retail-license key, select **Use the following retail license key**, and enter the key in the following field.



Step 6. Optional: **Optional:** If you selected a Windows operating system for any server, you can join the Windows operating system to an Active Directory domain as part of the operating-system deployment by clicking the **Folder** icon ( ) that is displayed next to the operating-system image, and then selecting the Active Directory name.

To use the default Active Directory that you specified in the Global Settings dialog, select **Use the Active Directory defined in Global Settings**. For more information about joining an Active Directory domain, see Integrating with Windows Active Directory.

To use an individual Active Directory, select **Use the following Active Directory**, and select the Active Directory domain.

Step 7. For each server, select the preferred storage location where you want to deploy the operating system image from the **Storage** column.
- **Local Disk Drive**
- **Embedded Hypervisor**
- **M.2 Drive**
- **SAN Storage**

If the selected storage location is not compatible with the server, XClarity Administrator attempts to deploy the operating system to the next storage location in the priority.

Note: For ThinkServer servers, only **Local disk** is available

For more information about how to configure the storage location, see Choosing the storage location for managed servers.

Note: To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

Step 8. Verify that the deployment status for all selected servers is Ready.

Important: Ensure that the deployment status of all selected servers is Ready. If the status of a server is Not Ready, you cannot deploy an operating-system image to that server. Click the **Not Ready** link to get information to help resolve the problem. If the network settings are not valid, click **Change Selected → Network Settings** to configure the network settings.

Step 9. Click the **Deploy images** icon ( ) to initiate the operating-system deployment.

If custom configuration settings were added to the OS-image profile, the **Custom Settings** tab is displayed on the Deploy OS Image dialog. Specify custom settings, common server settings, and specific server settings, and then click **Next** to continue with the OS deployment. Note that OS deployment will not proceed if input is not specified for any required custom configuration settings.

After you finish

You can monitor the status of the deployment process from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**. For more information about the job log, see Monitoring jobs.

You can also set up a remote-control session through the baseboard management controller for the server to watch the installation as it progresses. For more information about remote control, see Using remote control to manage Converged, Flex System, NeXtScale, and System x servers.

Deployment information is saved for the operating system. You can view the deployment information by clicking **Provisioning → Manage OS Access**, and then hovering over the server name.

Integrating with Windows Active Directory

When you deploy a Windows image using Lenovo XClarity Administrator, you are able to join an Active Directory domain as part of the operating-system deployment.

Before you begin

To join an Active Directory domain as part of a Windows image deployment, you must configure both the management server and the Windows Server that is running the affected Active Directory domain controller. To perform this configuration, you need the following access:

- An administrator account with the authority to authenticate and join the Active Directory servers domain. This account must have privileges similar to those of the default Domain Administrators group, and you can use an account in this group for this configuration.
- Access to a domain name system (DNS) that resolves to the Active Directory server that is running the domain controller. This DNS must be specified in the **Network Settings → DNS** option for the server to which you are deploying the operating system.
- The Active Directory server administrator must create the required computer name on the domain server before you deploy the operating system. The join attempt does not create computer name. If no name is specified, the join fails.

- The Active Directory server administrator must specify the hostname of the server to which the image is being deployed as a computer name under the target organizational unit by clicking the **Network Settings → Hostname** field.

  The specified hostname (computer name) must be unique. Specifying a name that is already in use by another Windows installation causes the join the fail.

You can join the Active Directory domain using one of the following methods:

- **Use an Active Directory domain**

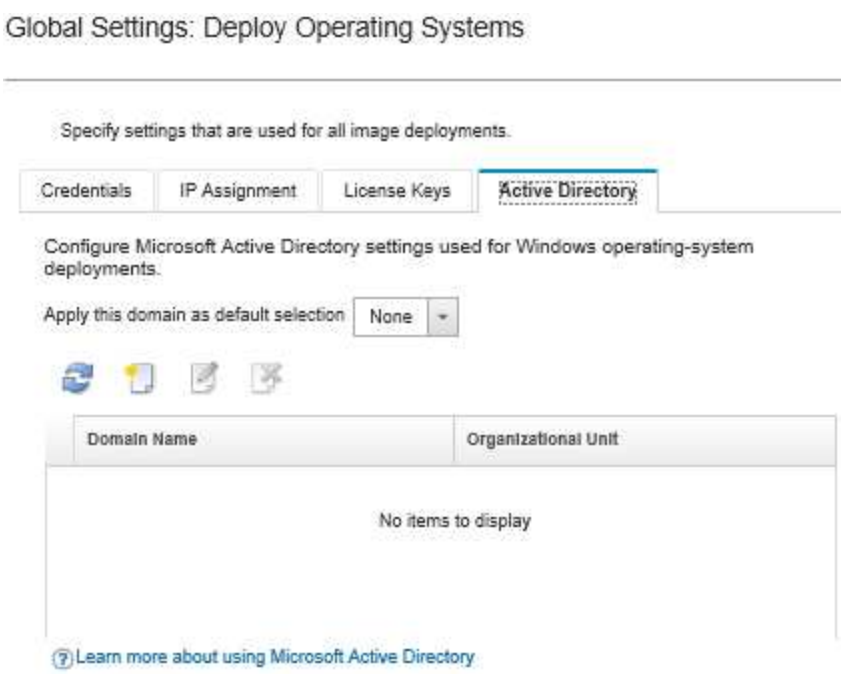
  You can choose to use a specific Active Directory domain from a list of predefined domains. Complete the following steps to define an Active Directory domain in XClarity Administrator. If you intend to use multiple domains, repeat these steps for each domain name.

  1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy OS Images page.
  2. Click the **Global Settings** icon ( ) to display the Global Settings: Deploy Operating Systems dialog.
  3. Click The **Active Directory** tab.
  4. Click the **Create** icon ( ) to display the Add New Active Directory Domain dialog.
  5. Specify the domain name and organizational unit.

     Operating-system deployment supports joining a domain and creating nested organizational units within a domain. If you are specifying organizational units, it is not necessary to specify the OU as part of the join explicitly. Active Directory is able to derive the correct OU using the domain name and computer name.
  6. Click **OK**.
- **Use the default Active Directory domain**

  You can choose to use the default Active Directory domain that is defined in global settings. Complete the following steps to set the default Active Directory domain in XClarity Administrator.

  1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS images** to display the Deploy OS Images page.
  2. Click the **Global Settings** icon ( ) to display the Global Settings: Deploy Operating Systems dialog.
  3. Click The **Active Directory** tab.



4. From the **Apply this domain as default selection** drop-down menu, select the Active Directory domain to be used by default for every Windows deployment.
5. Click **OK**.

- **Use metadata blob data**

  You can use Active Directory Computer Account Metadata (in Base-64 encoded blob format) to join the Active Directory domain for any server. Complete the following steps to generate metadata blob data.

  1. Use an administrator account to log in to the computer. The computer must be part of the Active Directory domain to which you are joining.
  2. Click **Start → Programs → Accessories**. Right-click **Command Prompt**, and then click **Run as administrator**.
  3. Change to the C:\windows\system32 directory.
  4. Run the **djoin** command using the following format to perform an offline domain join:
     `djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob`

     where:

     – *<AD_domain_name>* is the name of the Active Directory domain.
     – *<hostname>* is the hostname of the server to which the image is being deployed as a computer name under the target organizational unit by clicking the **Network Settings → Hostname** field.

     This command creates a file named `blob` that contains the metadata blob data. The content of this file is used by the operating-system deployment process to specify the Active Directory join details, so keep this data close by.

     The metadata blob data is sensitive data.

For detailed information about deploying an operating-system image, see Deploying an operating-system image.

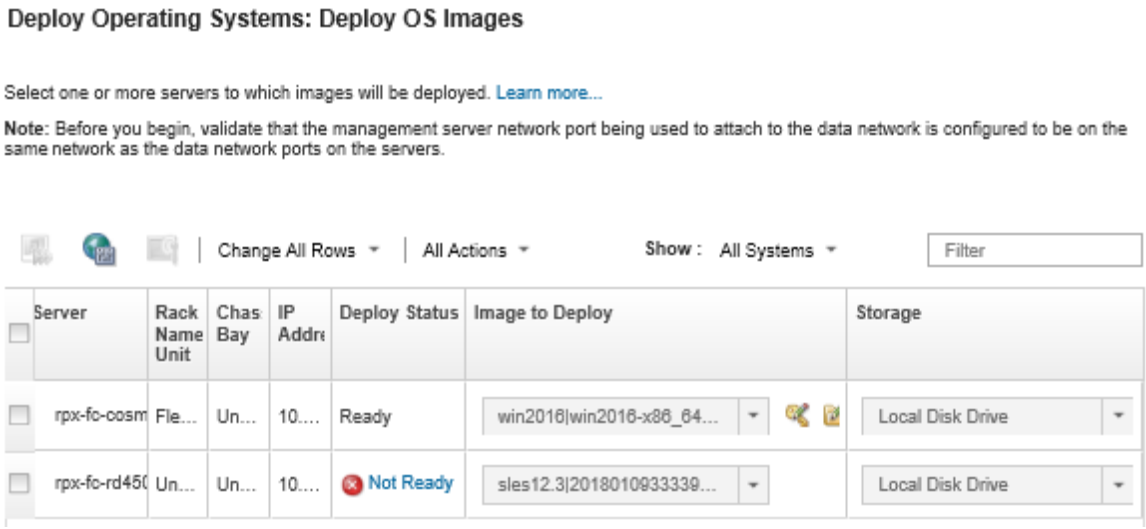
Procedure

To join an Active Directory domain, complete the following steps.

Step 1. Import the Windows operating-system image in to the OS images repository (see Importing operating-system images).

Step 2. Select one or more servers to which the operating system is to be deployed. You can deploy an operating system on up to 28 servers at one time.

Tip: You can choose multiple compute nodes from multiple chassis if you intend to deploy the same operating system to all compute nodes.



Step 3. Click **Change Selected → Network Settings** to configure network settings.

a. Click **Change All Rows → Domain Name System (DNS)**, and specify at a minimum a DNS that resolves to the Active Directory domain.

b. For each server, specify a hostname that matches an existing computer name in the domain and organizational unit that you are joining.

For more information about setting network settings, see Configuring network settings for managed servers.

Step 4. For each server, select the Windows operating-system image to be deployed in the **Image to Deploy** column. A folder and license key icons is displayed next to the image name.

Step 5. For each server, click the **License Key** icon (), and specify the license key to use to active the operating system after it is installed:

Step 6. For each server, click the **Folder** icon (), and specify the Active Directory domain. You can choose one of the following values:

- **Use the Active Directory defined in Global Settings** to use the default domain.
- **Use the following Active Directory** to select a specific domain.
- **Use metadata block data** to specify the contents of the blob file.

  The metadata blob data contains sensitive information and is not displayed in the field. This information is available only until the deployment operation is complete. It is not persistent.

Step 7. For each server, select the preferred storage location where you want to deploy the operating-system image from the **Storage** column.
- **Local Disk Drive**
- **Embedded Hypervisor**
- **M.2 Drive**
- **SAN Storage**

If the selected storage location is not compatible with the server, XClarity Administrator attempts to deploy the operating system to the next storage location in the priority.

For more information about how to configure the storage location, see Choosing the storage location for managed servers.

Note: To ensure that operating- system deployments are successful, detach all storage from the managed server except the storage chosen for the operating-system deployment.

Step 8. Verify that the deployment status for all selected servers is Ready.

If the status of a server is Not Ready, you cannot deploy an operating-system image to that server. Click the **Not Ready** link to get information to help resolve the problem. If the network settings are not valid, click **Changed Selected → Network Settings** to configure the network settings.

Step 9. Click the **Deploy images** icon ( ) to initiate the operating-system deployment.

The Deploy Confirmation dialog prompts you for the credentials to use for authenticating to the Active Directory server and joining the domain. For security reasons, these credentials are not stored in XClarity Administrator. You must supply the credential for every Windows deployment that joins the domain.

You can monitor the status of the deployment process from the jobs log. From the XClarity Administrator menu, click **Monitoring → Jobs**. For more information about the job log, see Monitoring jobs.

Results

When the operating-system deployment is complete, open a web browser to the IP address that you specified on the Edit Network Settings page, and log on to continue with the configuration process.

OS-deployment scenarios

Use these scenarios to help you customize and deploy operating systems to your managed servers.

Deploying RHEL with custom device drivers

This scenario installs the Red Hat Enterprise Linux (RHEL) operating system and additional device drivers that are not available in the base operating system. A custom profile is used that includes the additional device drivers. The custom profile can then be selected on the Deploy OS Images page.

Before you begin

When deploying operating systems using Lenovo XClarity Administrator, the operating system must include the appropriate Ethernet, Fibre Channel, and storage-adapter device drivers for your hardware. If a device driver is not included in the operating system, that adapter is not supported for OS deployment. In XClarity Administrator v1.2.0 and later, you can customize an operating system by adding device drivers.

You can obtain device drivers from the Lenovo YUM Repository webpage, from the vendor (such as Red Hat), or through a custom device driver that you generated yourself. For some Windows device drivers, you can generate a custom device driver by extracting the device driver from the installation .exe to your local system and creating a .zip archive file.

Note: RHEL device drivers must be in .rpm or .iso image format.

Procedure

To deploy RHEL with custom device drivers, complete the following steps.

Step 1. Download the base RHEL operating system from the Red Hat website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the RHEL image to import (for example, `RHEL-<ver>–<date>-Server-x86_64-dvd1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the custom device drivers to the local system and import the files into the OS-images repository. For more information, see Importing device drivers.

1. Click the **Device Drivers** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `RHEL` for the operating system.
5. Select the operating-system version.
6. Select the device type.
7. Click **Browse** to find and select the device driver to import (for example, `kmod-i40e-2.0.12-1.el7.x86_64.rpm`).
8. Click **Import** to upload the file to the OS-images repository.

Step 3. Create a custom OS-image profile that includes the custom device drivers. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom RHEL with device drivers`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **None** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, select the custom device drivers to include in profile, and click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, click **Next**.
7. Click **Customize** to create the custom OS-image profile.

Step 4. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.

b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

   Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.

c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>_Custom RHEL with device drivers) from the drop-down list in the **Image to Deploy** column.

   Note: Ensure that all target servers use the same custom profile.

d. (Optional) Click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.

e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

   Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

f. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Summary** tab, review the settings.
5. Click **Deploy** to deploy the operating system.

Deploying RHEL and a Hello World PHP application using a custom unattend file

This scenario installs the RHEL operating system along with custom software (Apache HTTP, PHP, and a hello-world PHP application). A custom OS-image profile is used that includes the custom unattend that registers the operating system with the internal Lenovo RHEL subscription service so that it can use the yum repositories, installs the Apache and PHP packages, configures the firewall to allow Apache connections, creates a Hello World PHP application and copies to the Apache web server directory, and configures the Apache configuration files to support PHP.

Before you begin

You can deploy RHEL with custom software in a few different ways. This example uses a custom attend file that you include in the custom OS-image profile. You can also use a post-installation script that installs custom software that you import into the repository and include in the custom OS-image profile. For installing software using a post-installation script, see Deploying RHEL and a Hello World PHP application using custom software and a post-installation script.

This scenario uses the following sample file.

- RHEL_installSoftware_customUnattend.cfg This custom unattend file uses values in predefined and custom macros and installs and configures the custom software.

Procedure

To deploy RHEL with custom software using a custom unatttend file, complete the following steps.

Step 1. Download the base RHEL operating system from the Red Hat website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the RHEL image to import (for example, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Modify the RHEL unattend (kickstart) file to register the operating system with your RHEL satellite subscription service, install HTTP (Apache) and PHP packages, and create a simple Hello World PHP application, add the required predefined macros and other predefined macros where applicable, such as the IP address, gateway, DNS and host name settings, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

Add commands to register the host with your RHEL satellite, for example:

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

Important: In the example unattend file, specify the IP address of your satellite server and your organization based on our subscription service configuration.

Add commands to update the host and to install and configure apache and php packages, for example:

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
php
php-mysql
php-gd
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
```

```
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original

sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

Note: The example unattend file modifies the default packages that are being installed with the kickstart file. It specifies the Apache and PHO packages as part of the %packages section.

For ESXi and RHEL only, XClarity Administrator provides the **#predefined.unattendSettings.networkConfig#** macro, which adds all network settings that are defined in the UI to the unattend file, and the **#predefined.unattendSettings.storageConfig#** macro, which adds all storage settings that are defined in the UI to the unattend file. The example unattend file already contains these macros.

XClarity Administrator also provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file. The example file already contains the required macros.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

The example file already contains the required macros and additional predefined macros for dynamically specifying network settings for the target server and timezone. For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file.

You can also add commands to send custom messages to the jobs log in XClarity Administrator. For more information, see Adding custom status reporting to installation scripts.

To import the custom installation script, complete these steps. For more information, see Importing custom installation scripts.

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `RHEL` for the operating system.
5. Click **Browse** to find and select the software file to import (for example, `RHEL_installSoftware_customUnattend.cfg`).
6. Click **Import** to upload the file to the OS-images repository.

Step 3. Create a custom OS-image profile that includes the custom software and post-installation script. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:

a. Enter a name for the profile (for example, `Custom RHEL with software using custom unattend`).
b. Use the default value for the **Custom data and file path** field.
c. Select **Only unattend files** for the customization type.
d. Click **Next**.

5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, click **Next**.
7. On the **Unattend Files** tab, select custom unattend file (for example, `RHEL_installSoftware_customUnattend.cfg`), and click **Next**.
8. On the **Installation Scripts** tab, click **Next**.
9. On the **Summary** tab, review the settings.
10. Click **Customize** to create the custom OS-image profile.

Step 4. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip:

      - VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
      - The network settings that you specify on the Network Settings dialog are added to the unattend file at runtime using the **#predefined.hostPlatforms.networkSettings.*<setting>*#** macros.

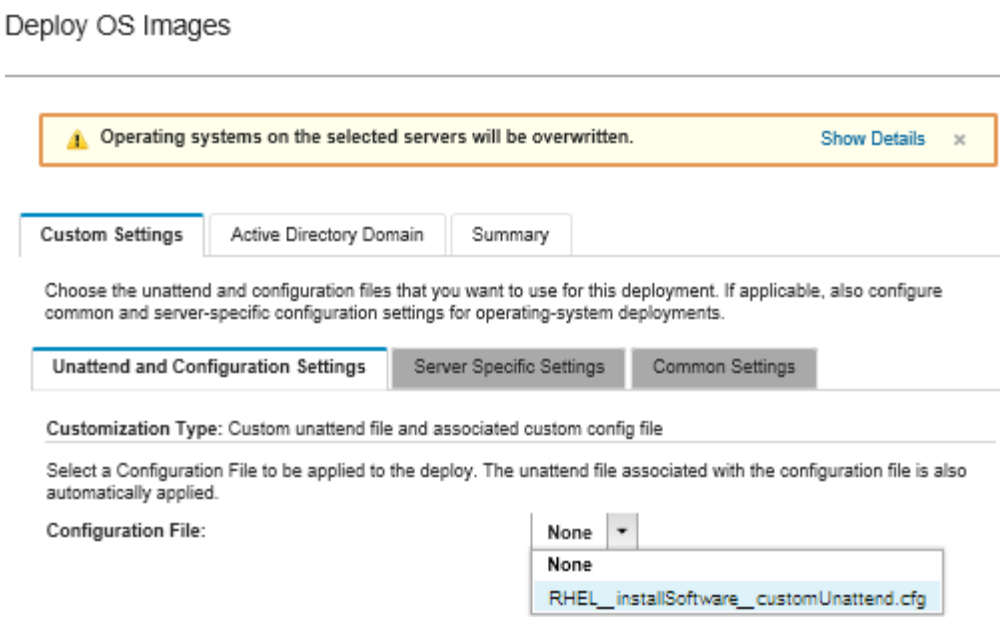
   c. Select the custom OS-image profile (for example, *<base_OS>*|*<timestamp>*`_Custom RHEL with software using custom unattend`) from the drop-down list in the **Image to Deploy** column

      Note: Ensure that all target servers use the same custom profile.

   d. (Optional) Click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.
   e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

   f. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the Custom Settings tab, click the **Unattend and Configuration Settings** subtab, and select the custom unattend file (for example, `RHEL_installSoftware_customUnattend.cfg`).



5. On the **Summary** tab, review the settings.
6. Click **Deploy** to deploy the operating system.

Deploying RHEL and a Hello World PHP application using custom software and a post-installation script

This scenario installs the RHEL operating system along with custom software (Apache HTTP, PHP, and a hello-world PHP application). A custom OS-image profile is used that includes the custom software and a post-installation script that registers the operating system with the internal Lenovo RHEL subscription service so that it can use the yum repositories, installs the Apache and PHP packages, configures the firewall to allow Apache connections, creates a Hello World PHP application and copies to the Apache web server directory, and configures the Apache configuration files to support PHP. The custom software packages are exported to the host during the deployment and made available for the custom post-installation script to use.

Before you begin

You can deploy RHEL and a Hello World PHP application in a few different ways. This example uses a post-installation script that installs custom software that you import into the repository and include in the custom OS-image profile. You can also use a custom attend file that you include in the custom OS-image profile. For installing software using a custom attend file, see Deploying RHEL and a Hello World PHP application using a custom unattend file.

This scenario uses the following sample files.

- httpd.conf. This is the installation file for Apache HTTP.
- hello_world.php This is the Hello World PHP application.
- RHEL_installSoftware_customScript.sh This post-installation script installs and configures the custom software.

Notes:

- RHEL installation scripts can be in one of the following formats: Bash (.sh), Perl (.pm or .pl), Python (.py)
- Software files and installation scripts are installed from the custom data and files path that you specify during deployment. The default custom data and files path is `/home/lxca`.

Procedure

To deploy RHEL with custom software using a post-installation script, complete the following steps.

Step 1. Download the base RHEL operating system from the Red Hat website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the RHEL image to import (for example, `RHEL-<ver>–<date>-Server-x86_64-dvd1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the custom software to the local system and import the files into the OS-images repository. For more information, see Importing custom software.

Tip: To import custom software into XClarity Administrator, the files must be contained in a tar.gz file. For this example, compress the example software files `httpd.conf` and `index.php` into a tar.gz file named `RHEL_installSoftware_customsw.tar.gz` before continuing

1. Click the **Software** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `RHEL` for the operating system.
5. Click **Browse** to find and select the software file to import (for example, `RHEL_installSoftware_customsw.tar.gz`).
6. Click **Import** to upload the file to the OS-images repository.

Step 3. Create a custom post-installation script, and import the file to the OS-images repository.

Add commands to register the host with the RHEL satellite, for example:

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

Add a command to update the host and install and configure apache and php packages, for example:

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

Add commands to add our PHP application to the web serversatellite, for example:

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/lxca/index.php /var/www/html/index.php
```

Add commands to configure Apache HTTP, for example:

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf /etc/httpd/conf/httpd.conf
```

Note that these commands use predefined macros for the path to the extracted data and software files (**predefined.otherSettings.deployDataAndSoftwareLocation**).

You can also add commands to send custom messages to the jobs log in XClarity Administrator. For more information, see Adding custom status reporting to installation scripts.

To import the custom installation script, complete these steps. For more information, see Importing custom installation scripts.

1. Click the **Installation Scripts** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `RHEL` for the operating system.
5. Click **Browse** to find and select the post-installation script to import (for example, `RHEL_installSoftware_customScript.sh`).
6. Click **Import** to upload the file to the OS-images repository.

Step 4. Create a custom OS-image profile that includes the custom software and post-installation script. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom RHEL with software using post-installation script`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **None** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, select the software installation files (for example `httpd.conf` and `index.php`), and click **Next**.
7. On the **Installation Scripts** tab, select the installation scripts (for example, `RHEL_installSoftware_customScript.sh`), and click **Next**.
8. On the **Summary** tab, review the settings.
9. Click **Customize** to create the custom OS-image profile.

Step 5. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.

c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>_Custom RHEL with software using post-installation script) from the drop-down list in the **Image to Deploy** column

Note: Ensure that all target servers use the same custom profile.

d. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

e. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Summary** tab, review the settings.
5. Click **Deploy** to deploy the operating system.

Deploying SLES 12 SP3 with custom packages and time zone

This scenario installs the SLES 12 SP3 operating system (in English) and several optional SLES packages. It also prompts for the time zone. A custom OS-image profile is used that includes a custom configuration file and custom unattend file. This custom profile can be selected on the Deploy OS Images page. Then, the SLE packages that you want to deploy can be selected and time zone can be specified on the **Custom Settings** tab. The selected values are substituted for the custom macros in the custom unattend, and the SLES autoyast installer uses those values in the unattend file to configure the operating system.

Before you begin

This scenario uses the following sample files.

- SLES_installPackages_customConfig.json. This configuration file prompts for the time zone and optional SLES packages (Linux, Apache, MySQL, PHP software package, SLES mail server package, and SLES file server package) to install.
- SLES_installPackages_customUnattend.xml This unattend file uses values in predefined macros and custom macros that are defined in the configuration file.

Procedure

To deploy SLES 12 SP3 to servers using a custom OS-image profile, complete the following steps.

Step 1. Download the base SLES operating system from the SUSE website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the SLES 12 SP3 image to import (for example, SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Create a custom configuration-settings file, and import the file to the OS-images repository.

The configuration-settings file is a JSON file that describe the data that needs to be gathered dynamically during the OS deployment process. For this scenario, we want to specify the optional SLES packages that can be installed (including SLES Linux, Apache, MySQL, PHP software package, SLES mail-server package, and SLES file-server package) and a time zone to use for each OS deployment. For more information about creating a configuration-settings file, see Custom macros.

To import the configuration-settings file, complete these steps. For more information, see Importing custom configuration settings.

1. Click the **Configuration Files** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the configuration-settings file to import (for example, `SLES_installPackages_customConfig.json`).
6. Click **Import** to upload the file to the OS-images repository.

   Note: When you import a custom configuration-settings file, XClarity Administrator generates custom macros for each setting in the file. You can add those macros to the unattend file. During OS deployment, the macros are replaced with actual values.

Step 3. Modify the SLES unattend file to specify dynamic values for the optional SLES packages and time zone, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

In the **<general>** section, add the time zone information, for example:

```
<timezone>
   <hwclock></hwclock>
   <timezone></timezone>
</timezone>
```

In the **<patterns>** section, add three pattern tags. These tags are used for the custom macros for the optional SLES package settings, for example:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern></pattern>
   <pattern></pattern>
   <pattern></pattern>
</patterns>
```

Notes:

- These tags are in the sample unattend file.
- When you use a custom unattend file, XClarity Administrator does not provide many of the normal convenience features that you get when you use a predefined unattend file. For example, the targets **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>**, and **<UserAccounts>** for Administrator, **<Interfaces>** for networking, and **<package>** list for installation features must be specified in the custom unattend file that is being uploaded.

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `SLES_installPackages_customUnattend.xml`).
6. Click **Import** to upload the file to the OS-images repository.

   Note: A warning that there are missing predefined macros in the unattend file is displayed. You can ignore the warning for now. You will add the predefined macros in the next step
7. Click **Close** in the warning dialog to open the Edit Unattend File dialog.

Step 4. Associate the custom unattend file with the custom configuration-settings file, and add the required predefined and custom macros (settings) from the configuration-settings file to the unattend file. For more information, see Associating an unattend file with a configuration settings file and Injecting predefined and custom macros to an unattend file.

Tip: You can optionally associate the custom unattend file with the custom configuration-settings file and add macros when importing the unattend file.

1. From the Edit Unattend File dialog, select the configuration-settings file to associate with the unattend file from the **Associate a Configuration File** drop-down list (for example, `SLES_installPackages_customConfig`).
2. Add the required predefined macros to the unattend file.
   a. Select **Predefined** from the **Available Macros** drop-down list.
   b. Place the cursor in the unattend file anywhere after line 1 (after the **<xml>** tag).
   c. Expand the **predefined → unattendSettings** list in the list of available predefined macros.
   d. Click the **preinstallConfig** and **postinstallConfig** macros to add the macros to the unattend file.

   For example:

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

3. Add the custom macro for specifying the time zone.
   a. Select **Custom** from the **Available Macros** drop-down list.
   b. Place the cursor after the **<hwclock>** tag, and click **timezone** to add the time zone macro.
   c. Place the cursor after the **<timezone>** tag, and click **timezone** to add the time zone macro.

   For example:

```
<timezone>
```

```
   <hwclock>#timezone#</hwclock>
   <timezone>#timezone#</timezone>
</timezone>
```

4. Add the custom macro for specifying the optional SLES packages.
   a. Expand the **server-settings → node** list in the list of available custom macros.
   b. Place the cursor in one of the empty **<pattern>** tags, and click **fileserver**.
   c. Place the cursor in one of the empty **<pattern>** tags, and click **lampserver**.
   d. Place the cursor in one of the empty **<pattern>** tags, and click **mailserver**.

   For example:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern>#server-settings.node.fileserver#</pattern>
   <pattern>#server-settings.node.lampserver#</pattern>
   <pattern>#server-settings.node.mailserver#</pattern>
</patterns>
```

5. Click **Save** to bind the files together and save the changes to the unattend file.

Step 5. Create a custom OS-image profile that includes the custom configuration-settings and unattend files. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom SLES with optional packages`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Associated unattend and configuration-settings files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, click **Next**.
7. On the **Unattend Files** tab, select the unattend file (for example, `SLES_installPackages_customUnattend.xml`), and click **Next**.

   The associated configuration-settings file is automatically selected.
8. On the **Installation Scripts** tab, click **Next**.
9. On the **Summary** tab, review the settings.
10. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

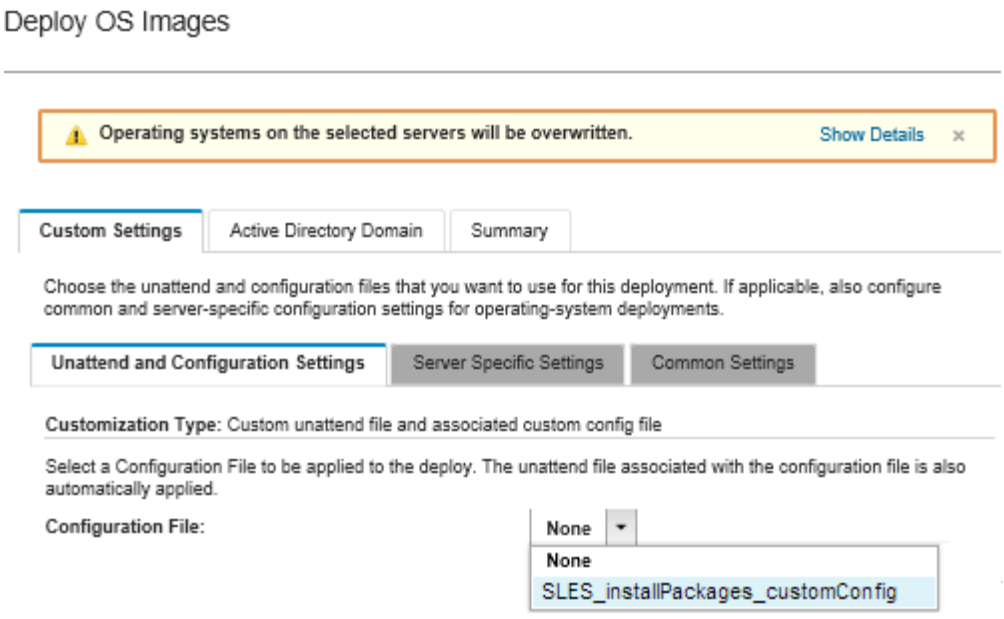
1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, *<base_OS>*|*<timestamp>*`_Custom SLES with optional packages`) from the drop-down list in the **Image to Deploy** column

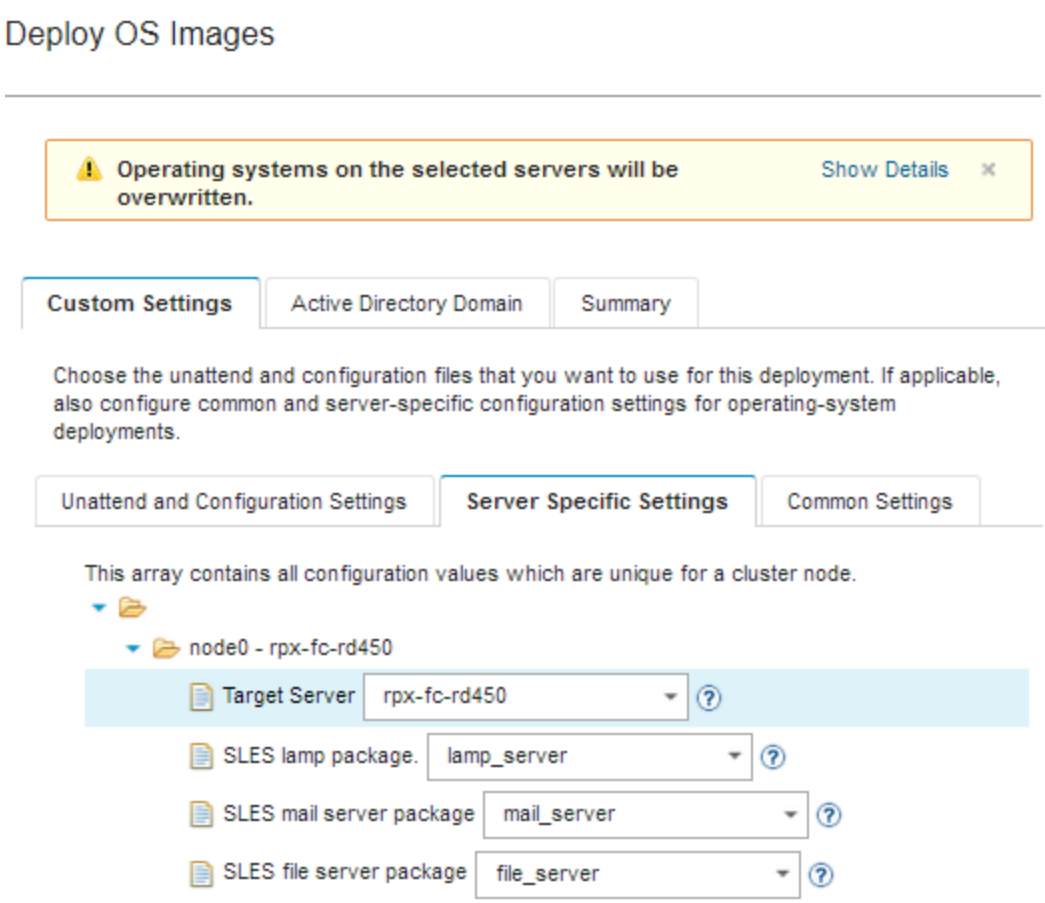
      Note: Ensure that all target servers use the same custom profile.
   d. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
   e. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom configuration-settings file (for example, `SLES_installPackages_customConfig`).

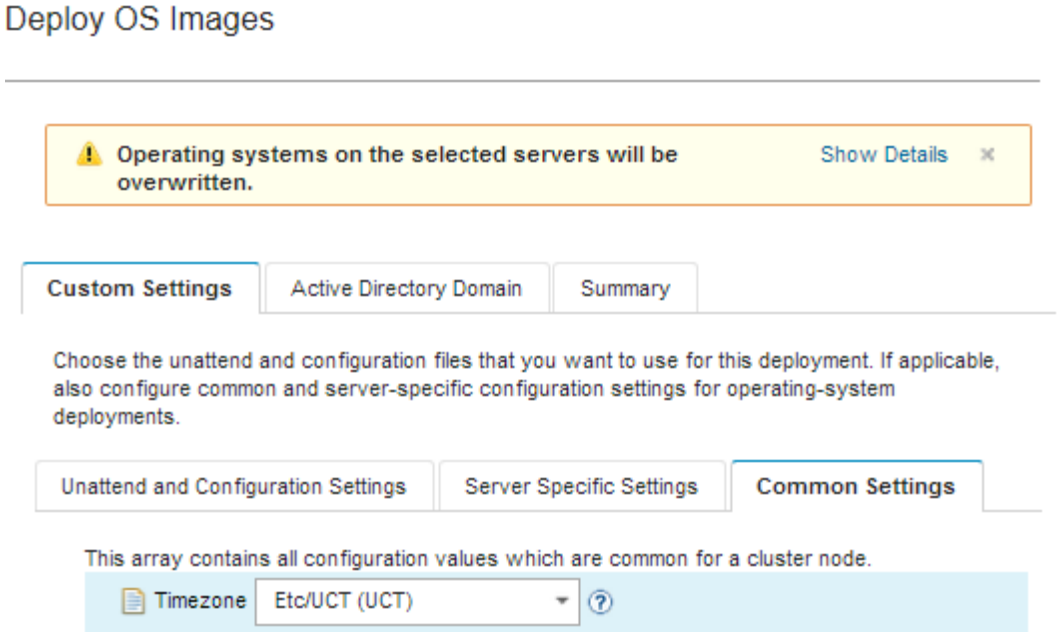
   Note: The associated custom unattend file is selected automatically.



5. On the **Server-Specific Settings** subtab, select the target server and the optional SLES packages that you want to deploy.



6. On the **Common Settings** subtab, select the time zone to set for all target servers.



7. On the **Summary** tab, review the settings.
8. Click **Deploy** to deploy the operating system.

Deploying SLES 12 SP3 with custom software

This scenario installs the SLES 12 SP3 operating system along with custom software (Java and Eclipse IDE). A custom profile is used that includes the custom software and post-installation scripts to install and configure the custom software. The custom software packages are copied to the host during the deployment and made available for the custom post-install script to use.

Before you begin

This scenario uses the following sample files.

- jre-8u151-linux-x64.tar.gz. This is the installation file for Java for Eclipse.
- eclipse-4.6.3-3.1.x86_64.tar.gz This is the installation file for Eclipse IDE.
- SLES_installSoftware_customScript.sh This post-installation script creates a user to launch Eclipse, and installs Eclipse IDE and Java.

Notes:

- SLES installation scripts can be in one of the following formats: Bash (.sh), Perl (.pm or .pl), Python (.py)
- Software files and installation scripts are installed from the custom data and files path that you specify during deployment. The default custom data and files path is `/home/lxca`.
- For SLES 12 SP3, the Eclipse IDE requires the GCC compiler, which is included in the predefined Basic profile. This scenario creates a custom OS-image profile using the predefined Basic profile as the base. If you choose to use another profile, you must ensure that the profile includes the GCC compiler.

Procedure

To deploy SLES 12 SP3 with custom software, complete the following steps.

Step 1. Download the base SLES 12 SP3 operating system from the SUSE website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the SLES 12 SP3 image to import (for example, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the custom software to the local system and import the files into the OS-images repository. For more information, see Importing custom software.

1. Click the **Software** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the software file to import (for example, `jre-8u151-linux-x64.tar.gz`).
6. Click **Import** to upload the file to the OS-images repository.

7. Click the **Import** icon ( ) again.
8. Click **Local Import**.
9. Select SLES for the operating system.
10. Click **Browse** to find and select the software- file to import (for example, eclipse-4.6.3-3.1.x86_64.tar.gz).
11. Click **Import** to upload the file to the OS-images repository.

Step 3. Create a custom post-installation script, and import the file to the OS-images repository.

Add commands to create a user to launch eclipse to this file, for example:

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "Passw0rd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] && echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Add commands to install the software, for example:

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

Note that these commands use predefined macros for the HTTPS URL that XClarity Administrator uses for reporting status (**predefined.otherSettings.statusSettings.urlStatus**), for the Folder containing the certificates that are needed to access the urlStatus web service from the host OS on first boot (**predefined.otherSettings.statusSettings.certLocation**), and for the path to the extracted data and software files (**predefined.otherSettings.deployDataAndSoftwareLocation**).

You can also add commands to send custom messages to the jobs log in XClarity Administrator, as shown in the sample file. For more information, see Adding custom status reporting to installation scripts.

To import the custom installation script, complete these steps. For more information, see Importing custom installation scripts.

1. Click the **Installation Scripts** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select SLES for the operating system.
5. Click **Browse** to find and select the post-installation script to import (for example, SLES_installSoftware_customScript.sh).
6. Click **Import** to upload the file to the OS-images repository.

Step 4. Create a custom OS-image profile that includes the custom software and post-installation script. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.

2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom SLES with software`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **None** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, select the software installation files (for example `jre-8u151-linux-x64.tar.gz` and `eclipse-4.6.3-3.1.x86_64.tar.gz`), and click **Next**.
7. On the **Installation Scripts** tab, select the installation scripts (for example, `SLES_installSoftware_customScript.sh`), and click **Next**.
8. On the **Summary** tab, review the settings.
9. Click **Customize** to create the custom OS-image profile.

Step 5. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom SLES with software`) from the drop-down list in the **Image to Deploy** column

      Note: Ensure that all target servers use the same custom profile.
   d. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
   e. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Summary** tab, review the settings.
5. Click **Deploy** to deploy the operating system.

Deploying SLES 12 SP3 with a configurable locale and NTP servers

This scenario installs the SLES 12 SP3 operating system with either English, Brazilian, or Japanese enabled for the keyboard and operating-system locales. It also configures the IP address for up to three NTP servers. A custom OS-image profile is used that includes an unattend file (with predefined and custom macros) and a configuration-settings file for selecting the locales and NTP-server settings. This custom profile can be selected on the Deploy OS Images page. Then, the locales and NTP-server settings can be selected on the **Custom Settings** tab. The specified values are substituted for the custom macros contain in the custom

unattend file, and the SLES autoyast installer uses those values in the unattend file to configure the operating system.

Before you begin

This scenario uses the following sample files.

- SLES_locale_customConfig.json. This custom configuration file prompts for the language to install for the OS local and keyboard for SLES and for the NTP server.
- SLES_locale_customUnattend.xml. This custom unattend file uses values in custom macros that are defined in the configuration file.

Procedure

To deploy SLES 12 SP3 using custom OS-image profile, complete the following steps.

Step 1. Download the base SLES operating system from the SUSE website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the SLES 12 SP3 image to import (for example, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete.

Step 2. Create a custom configuration-settings file, and import the file to the OS-images repository.

The configuration-settings file is a JSON file that describe the data that needs to be gathered dynamically during the OS deployment process. For this scenario, we want to specify the operating-system locale (en_US, ja_JP, pt_BR), the keyboard locale (english-us, Japanese, or portugese-br), and up to three NTP server IP addresses to use for each OS deployment. For more information about creating a configuration-settings file, see Custom macros.

To import the configuration-settings file, complete these steps. For more information, see Importing custom configuration settings.

1. Click the **Configuration Files** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the configuration-settings file to import (for example, `SLES_locale_customConfig.json`).
6. Click **Import** to upload the file to the OS-images repository

   Note: When you import a custom configuration-settings file, XClarity Administrator generates custom macros for each setting in the file. You can add those macros to the unattend file. During OS deployment, the macros are replaced with actual values.

Step 3. Modify the SLES unattend file to specify dynamic values for the operating-system locale, keyboard locale, and NTP server IP addresses, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

Just after the <profile> tag, add the NTP server and networking information. The following example includes tags for two NTP servers. The IP addresses will be added as macros in a later step.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

In the <general> section, add the OS and keyboard locale info, as shown in the following example. The keyboard and operating system locale settings will be added as macros in a later step.

```
<keyboard>
   <keymap></keymap>
</keyboard>
<language></language>
```

Note: When you use a custom unattend file, XClarity Administrator does not provide many of the normal convenience features that you get when you use a predefined unattend file. For example, the targets **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>**, and **<UserAccounts>** for Administrator, **<Interfaces>** for networking, and **<package>** list for installation features must be specified in the custom unattend file that is being uploaded.

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `SLES` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `SLES_locale_customUnattend.xml`).
6. Click **Import** to upload the file to the OS-images repository

Step 4. Associate the custom unattend file with the custom configuration-settings file, and add the required predefined and custom macros (settings) from the configuration-settings file to the unattend file. For more information, see Associating an unattend file with a configuration settings file and Injecting predefined and custom macros to an unattend file

Tip: You can optionally the custom unattend file with the custom configuration-settings file and add macros when importing the unattend file.

1. From the **Unattend Files** tab, select the custom attend file (for example, `SLES_locale_customUnattend.xml`).
2. Click the **Associate a Configuration File** icon ( ) to display the Associate an Unattend File dialog.
3. Select the configuration-settings file to associate with the unattend file (for example, `SLES_locale_customConfig`).
4. Add the required predefined macros to the unattend file.
   a. Select **Predefined** from the **Available Macros** drop-down list.
   b. Place the cursor in the unattend file anywhere after line 1 (after the **<xml>** tag).
   c. Expand the **predefined → unattendSettings** list in the list of available predefined macros.
   d. Click the **preinstallConfig** and **postinstallConfig** macros to add the macros.

   For example:

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

5. Add the custom macro for specifying the operating-system locale.
   a. Select **Custom** from the **Available Macros** drop-down list
   b. Place the cursor after the **<language>** tag.
   c. Expand **server-settings → node** in the list of available custom macros, and then click **locale** to add the OS-locale macro.

   For example:

```
<language>#server-settings.node.locale#</language>
```

6. Add the custom macro for specifying the keyboard locale.
   a. Place the cursor after the **<keymap>** tag.
   b. Expand **server-settings → node** in the list of available custom macros, and then click **keyboardLocale** to add the keyboard-locale macro.

   For example:

```
<keyboard>
   <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. Add the custom macro for specifying the NTP server IP addresses.

   In this scenario, the custom configuration-settings file uses a template to specify zero to three NTP servers. When using templates in the configuration-settings file, macros that are associated with template are not displayed in the Associate an Unattend File dialog. Instead, you must manually edit the unattend file and add the macros and appropriate tags.

   For example, to include three NTP servers, you would add the following tags and macros to the unattend file. These tags and macros already exist in the example unattend file for this scenario.

```
<ntp-client>
    <configure_dhcp config:type="boolean">false</configure_dhcp>
    <peers config:type="list">
      <peer>
        <address>#server-settings.ntpserver1#</address>
        <initial_sync config:type="boolean">true</initial_sync>
        <options></options>
```

```
      <type>server</type>
    </peer>
    <peer>
      <address>#server-settings.ntpserver2#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
    <peer>
      <address>#server-settings.ntpserver3#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
  </peers>
  <start_at_boot config:type="boolean">true</start_at_boot>
  <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. Click **Associate** to bind the files together and save the changes to the unattend file.

Step 5. Create a custom OS-image profile that includes the custom configuration-settings and unattend files. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Basic`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom SLES for OS and keyboard locale and NTP server`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Associated unattend and configuration-settings files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Software** tab, click **Next**.
7. On the **Unattend Files** tab, select the unattend file (for example, `SLES_locale_customUnattend.xml`), and click **Next**.

   The associated configuration-settings file is automatically selected.
8. On the **Installation Scripts** tab, click **Next**.
9. On the **Summary** tab, review the settings.
10. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target server. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.

c. Select the custom OS-image profile (for example, *<base_OS>*|*<timestamp>*_Custom SLES for OS and keyboard locale and NTP server) from the drop-down list in the **Image to Deploy** column

   Note: Ensure that all target servers use the same custom profile.

d. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

   Note: To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

e. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom configuration-settings file (for example, SLES_locale_customConfig).

   Note: The associated custom unattend file is selected automatically.

5. On the **Server-Specific Settings** subtab, select the target server, OS locale, and keyboard locale.
6. On the **Common Settings** subtab, click **Add** to specify the IP address of up to three NTP servers.
7. On the **Summary** tab, review the settings.
8. Click **Deploy** to deploy the operating system.

Deploying VMware ESXi v6.7 with Lenovo Customization to a local disk using a static IP address

This scenario installs the VMware ESXi v6.7 with Lenovo Customization operating system to the local disk using the static IP address of the host server. A custom OS-image profile is used that includes an unattend file with predefined macros. This custom profile can be selected on the Deploy OS Images page. Known values are substituted for the predefined macros in the custom unattend file, and the VMware ESXi kickstart installer uses those values in the unattend file to configure the operating system.

Before you begin

This scenario uses the following sample files.

- ESXi_staticIP_customUnattend.cfg. This custom unattend file uses values in predefined macros.

Procedure

To deploy VMware ESXi v6.7 using custom OS-image profile, complete the following steps.

Step 1. Download the VMware vSphere® Hypervisor (ESXi) with Lenovo Customization operating system from the VMware Support – Downloads webpage website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ( ).
4. Click **Local Import**.
5. Click **Browse** to find and select the ESXi image to import (for example, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete.

Step 2. Modify the ESXi unattend (kickstart) file to add the required predefined macros and other predefined macros where applicable, such as the IP address, gateway, DNS and host name settings, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

For ESXi and RHEL only, XClarity Administrator provides the **#predefined.unattendSettings.networkConfig#** macro, which adds all network settings that are defined in the UI to the unattend file. Because this example specifies a setting (**--addvmportgroup**) that is not defined in the UI, the . **#predefinedunattendSettings.storageConfig#** macro is not used in the sample unattend file. Instead, network settings are individually added to the file, and the **#predefined.hostPlatforms.networkSettings.**<*setting*>**#** macros are used.

For ESXi and RHEL only, XClarity Administrator also provides the **#predefined.unattendSettings.storageConfig#** macro, which adds all storage settings that are defined in the UI to the unattend file. Because this example specifies settings (**--novmfsondisk** and **–ignoressd**) that are not defined in the UI, the **#predefinedunattendSettings.storageConfig#** macro is not used in the sample unattend file. Instead, storage settings are individually added and **--firstdisk=local** is hardcoded in the file.

Note: XClarity Administrator provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file. The example file already contains the required macros. Note that because the %firstboot section is included, the ordering of these predefined macros matters. For more information, see Importing custom unattend files.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

The example file already contains the required macros and additional predefined macros for dynamically specifying network settings for the target server. For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file.

For more information about available predefined macros, see Predefined macros.

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `ESXi` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `ESXi_staticIP_customUnattend.cfg`).
6. Click **Import** to upload the file to the OS-images repository

Step 3. Create a custom OS-image profile that includes the custom unattend. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom ESXi using static IP`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Only unattend files** for the customization type.
   d. Click **Next**.
5. On the **Unattend Files** tab, select the unattend file (for example, `ESXi_staticIP_customUnattend.cfg`), and click **Next**.
6. On the **Summary** tab, review the settings.
7. Click **Customize** to create the custom OS-image profile.

Step 4. Deploy the custom OS-image profile to the target server. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip:

      - VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
      - The network settings that you specify on the Network Settings dialog are added to the unattend file at runtime using the **#predefined.hostPlatforms.networkSettings.** <*setting*>**#** macros.

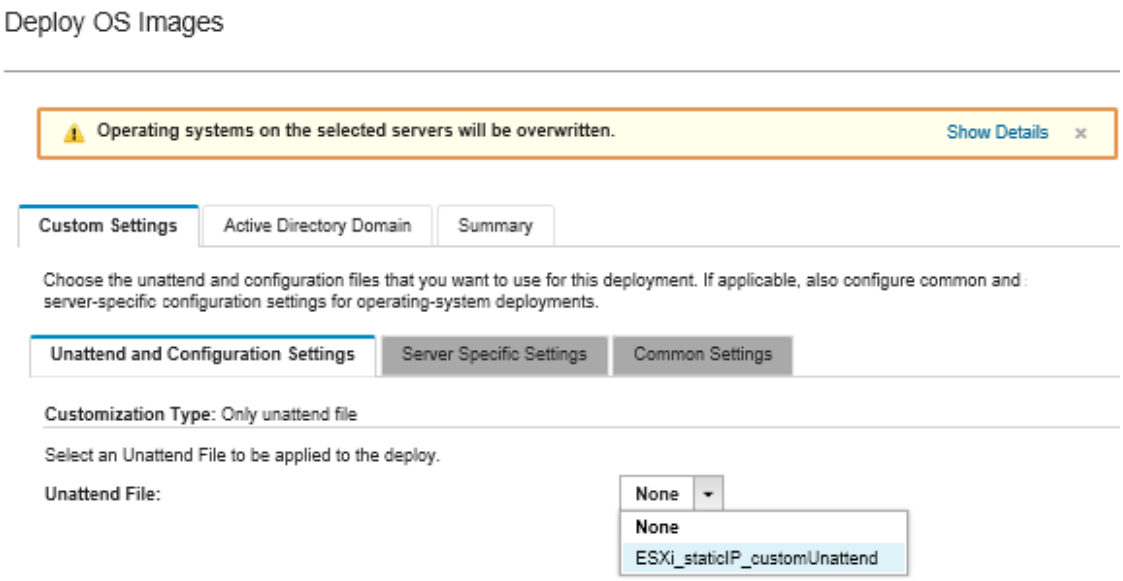
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom ESXi using static IP`) from the drop-down list in the **Image to Deploy** column

      Note: Ensure that all target servers use the same custom profile.

   d. (Optional) Click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.
   e. Verify that the deployment status for the selected server is **Ready**.

Note: Because **--firstdisk=local** is specified in the unattend file, you do not need to specify the preferred storage location in the **Storage** column. The setting in the UI is ignored.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom unattend file (for example, `ESXi_staticIP_customUnattend.cfg`).



5. On the **Summary** tab, review the settings.
6. Click **Deploy** to deploy the operating system.

Deploying VMware ESXi v6.7 with Lenovo Customization with a configurable locale and second-user credentials

This scenario installs the VMware ESXi v6.7 with Lenovo Customization operating system with a configurable language enabled for the keyboard locale and credentials for a second ESXi user. This example also uses basic network and storage settings that are defined in the UI. A custom OS-image profile is used that includes an unattend file (with predefined and custom macros) and a configuration-settings file for selecting the password. This custom profile can be selected on the Deploy OS Images page. Then, the password can be specified on the **Custom Settings** tab. The specified value is substituted for the custom macro in the custom unattend file, and the ESXi installer uses those values in the unattend file to configure the operating system.

Before you begin

This scenario uses the following sample files.

- ESXi_locale_customConfig.json. This custom configuration file prompts for the keyboard locale and credentials for the second ESXi user.
- ESXi_locale_customUnattend.cfg. This custom unattend file uses values in predefined macros and custom macros that are defined in the configuration file.

Procedure

To deploy VMware ESXi v6.7 using custom OS-image profile, complete the following steps.

Step 1. Download the VMware vSphere® Hypervisor (ESXi) with Lenovo Customization operating system from the VMware Support – Downloads webpage website to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the ESXi image to import (for example, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete.

Step 2. Create a custom configuration-settings file, and import the file to the OS-images repository.

The configuration-settings file is a JSON file that describe the data that needs to be gathered dynamically during the OS deployment process. For this scenario, we want to choose keyboard locale and the user ID and password for a second ESXi user to use for each OS deployment. For more information about creating a configuration-settings file, see Custom macros.

To import the configuration-settings file, complete these steps. For more information, see Importing custom configuration settings.

1. Click the **Configuration Files** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `ESXi` for the operating system.
5. Click **Browse** to find and select the configuration-settings file to import (for example, `ESXi_locale_customConfig.json`).
6. Click **Import** to upload the file to the OS-images repository

   Note: When you import a custom configuration-settings file, XClarity Administrator generates custom macros for each setting in the file. You can add those macros to the unattend file. During OS deployment, the macros are replaced with actual values.

Step 3. Modify the ESXi unattend (kickstart) file to specify the operating-system locale and keyboard locale and user credentials for the second ESXi user, and then import the custom file to the OS-images repository. For more information, see Importing custom unattend files.

Add commands to set the keyboard locale, for example:

```
# Set the keyboard locale
keyboard ''
```

Add commands to create a second ESXi user. In the following example, <*user_id*> and <*password*> will be replaced with custom macros in the next step.

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

To import the custom unattend file, complete these steps.

1. Click the **Unattend Files** tab.

2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `ESXi` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `ESXi_locale_customUnattend.cfg`).
6. Click **Import** to upload the file to the OS-images repository

Step 4. Associate the custom unattend file with the custom configuration-settings file, and add the required predefined and custom macros (settings) from the configuration-settings file to the unattend file. For more information, see Associating an unattend file with a configuration settings file and Injecting predefined and custom macros to an unattend file

Tip:

- You can optionally associate the custom unattend file with the custom configuration-settings file and add macros when importing the unattend file.
- XClarity Administrator provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file. The example file already contains the required macros. Note that because the %firstboot section is included, the ordering of these predefined macros matters. For more information, see Importing custom unattend files.
  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```
- XClarity Administrator also provides macros that inject all network and storage-location settings that are defined in the UI. These macros are useful when only basic settings are needed for the deployment. The example file already contains the required macros.
  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file. For more information about available predefined macros, see Predefined macros.

To associate the custom unattend file with the custom configuration-settings file, complete these steps.

1. From the **Unattend Files** tab, select the custom attend file (for example, `ESXi_locale_customUnattend.cfg`).
2. Click the **Associate a Configuration File** icon ( ) to display the Associate an Unattend File dialog.
3. Select the configuration-settings file to associate with the unattend file (for example, `ESXi_locale_customConfig`).
4. Select **Custom** from the **Available Macros** drop-down list.
5. Add the custom macro for specifying the keyboard locale by placing the cursor between the single quotes after keyboard, and then clicking **keyboard_locale**.

   For example:

   ```
   # Set the keyboard locale
   keyboard '#keyboard_locale#'
   ```
6. Add the custom macro for specifying the second user's ID by placing the cursor at each location where you want to add the user ID, and then clicking **second_user_id**. In the example file, replace each occurrence of *<user_id>* with the custom macro.

For example:

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
```

7. Add the custom macro for specifying the second user's password by placing the cursor at the location where you want to add the password, and then clicking **second_user_password**. In the example file, replace <*password*> with the custom macro.

   For example:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

8. Click **Associate** to bind the files together and save the changes to the unattend file.

Step 5. Create a custom OS-image profile that includes the custom configuration-settings and unattend files. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom ESXi using custom locale and second user credentials`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Associated unattend and configuration-settings files** for the customization type.
   d. Click **Next**.
5. On the **Unattend Files** tab, select the unattend file (for example, `ESXi_locale_customUnattend.cfg`), and click **Next**.

   The associated configuration-settings file is automatically selected.
6. On the **Summary** tab, review the settings.
7. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target server. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip:

      - VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
      - The network settings that you specify on the Network Settings dialog are added to the unattend file at runtime using the **#predefined.hostPlatforms.networkConfig#** macro.

   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom ESXi using custom locale and second user credentials`) from the drop-down list in the **Image to Deploy** column

Note: Ensure that all target servers use the same custom profile.

d. (Optional) Click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.

e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

Notes:

- To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
- The storage settings that you specify on the Storage Settings dialog are added to the unattend file at runtime using the **#predefined.hostPlatforms.storageConfig#** macro.

f. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom configuration-settings file (for example, `ESXi_locale_customConfig`).

Note: The associated custom unattend file is selected automatically.

5. On the **Server-Specific Settings** subtab, select the keyboard locale and credentials for the second ESXi user.
6. On the **Summary** tab, review the settings.
7. Click **Deploy** to deploy the operating system.

Deploying Windows 2016 with custom features

This scenario installs the Windows 2016 operating system and several additional features. A custom profile is used that includes a custom unattend file. The custom profile can then be selected on the Deploy OS Images page.

Before you begin

This scenario uses the following sample files.

- Windows_installFeatures_customUnattend.xml. This custom unattend file installs the WindowsMediaPlayer and BitLocker features, and uses predefined macros for dynamic values.

Procedure

To deploy Windows 2016 with custom features, complete the following steps.

Step 1. Download the Japanese Windows 2016 operating system to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the bundle file for Windows 2016 to the local system, and import the image to the OS-images repository. For more information, see Importing device drivers.

The bundle file contains the latest device drivers and WinPE boot files that you can add to your custom OS-images profiles. This scenario uses a custom boot file, so the boot file in the bundle will not be used.

1. Click the **Driver Files** tab.
2. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the bundle file for Windows 2016 to the local system.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `bundle_win2016_20180126130051.zip`).
6. Click **Import** to upload the file to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 3. Modify the Windows unattend file to install the additional features (such as WindowsMediaPlayer and BitLocker), and import the custom file to the OS-images repository.

In the “servicing” section of the Windows unattend file, add the Windows features to install, for example

```
<servicing>
   <package action="configure">
      <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
                        processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
                        language=""></assemblyIdentity>
      <selection name="Microsoft-Hyper-V" state="true"></selection>
      <selection name="MultipathIo" state="true"></selection>
      <selection name="FailoverCluster-PowerShell" state="true"></selection>
      <selection name="FailoverCluster-FullServer" state="true"></selection>
      <selection name="FailoverCluster-CmdInterface" state="true"></selection>
      <selection name="FailoverCluster-AutomationServer" state="true"></selection>
```

```
        <selection name="FailoverCluster-AdminPak" state="true"></selection>
        <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
        <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
        <selection name="ServerManager-Core-RSAT" state="true"></selection>
        <selection name="WindowsMediaPlayer" state="true"></selection>
        <selection name="BitLocker" state="true"></selection>
    </package>
</servicing>
```

Notes:

- These tags are in the sample unattend file.
- When you use a custom unattend file, XClarity Administrator does not provide many of the normal convenience features that you get when you use a predefined unattend file. For example, the targets `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>`, and `<UserAccounts>` for Administrator, `<Interfaces>` for networking, and `<package>` list for installation features must be specified in the custom unattend file that is being uploaded.

To import the custom unattend file, complete these steps. For more information, see Importing custom unattend files.

1. Click the **Unattend Files** tab.
2. Click **Import** icon ( ).
3. Click **Local Import**.
4. Select `Windows` for the operating system.
5. Click **Browse** to find and select the custom unattend file (for example, `Windows_installFeatures_customUnattend.xml`).
6. Click **Import** to upload the file to the OS-images repository.

XClarity Administrator provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, and custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

The example file already contains the code for installing the additional features, required macros, and other macros that are needed for dynamic input. For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file.

For more information about available predefined macros, see Predefined macros.

Step 4. Create a custom OS-image profile that includes the unattend file. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select the profile to customize (for example, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom Windows with features`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Only unattend files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.

6. On the **Boot Options** tab, and click **Next**. The predefined WinPE boot file is selected by default.
7. On the **Software** tab, click **Next**.
8. On the **Unattend Files** tab, select custom unattend file (for example, `Windows_installFeatures_customUnattend.xml`), and click **Next**.
9. On the **Installation Scripts** tab, click **Next**.
10. On the **Summary** tab, review the settings.
11. Click **Customize** to create the custom OS-image profile

Step 5. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, subnet mask, gateway, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>`_Custom Windows with features`) from the drop-down list in the **Image to Deploy** column.

      Note: Ensure that all target servers use the same custom profile.
   d. (Optional) Click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.
   e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment
   f. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom unattend file (for example, `Windows_installFeatures_customUnattend.xml`).
5. (Optional) On the **Active Directory Domain** tab, specify information to join an Active Directory domain as part of a Windows image deployment (see Integrating with Windows Active Directory).
6. On the **Summary** tab, review the settings.
7. Click **Deploy** to deploy the operating system.

Deploying Windows 2016 with custom software

This scenario installs the Windows 2016 operating system along with custom software (Java and Eclipse IDE). A custom profile is used that includes the custom software and post-installation scripts to install and configure the custom software. The custom software packages are copied to the host during the deployment and made available for the custom post-install script to use.

Before you begin

This scenario uses the following sample files.

- jre-8u151-windows-x64-with-configfile.zip. This is the installation file for Java for Eclipse.
- eclipse-java-oxygen-1a-win32-x86_64.zip This is the installation file for Eclipse IDE.
- Windows_installSoftware_customScript.ps1 This post-installation script creates a user to launch Eclipse, and installs Eclipse IDE and Java.

Notes:

- Windows installation scripts can be in one of the following formats: Command file (.cmd), PowerShell (.ps1)
- Software files and installation scripts are installed from the custom data and files path that you specify during deployment. The default custom data and files path is `C:\lxca`.

Procedure

To deploy Windows 2016 with custom software, complete the following steps.

Step 1. Download the Japanese Windows 2016 operating system to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the bundle file for Windows 2016 to the local system, and import the image to the OS-images repository. For more information, see Importing device drivers.

The bundle file contains the latest device drivers and WinPE boot files that you can add to your custom OS-images profiles. This scenario uses a custom boot file, so the boot file in the bundle will not be used.

1. Click the **Driver Files** tab.
2. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the bundle file for Windows 2016 to the local system.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `bundle_win2016_20180126130051.zip`).
6. Click **Import** to upload the file to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 3. Download the custom software to the local system and import the files into the OS-images repository. For more information, see Importing custom software.

1. Click the **Software** tab.

2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `Windows` for the operating system.
5. Click **Browse** to find and select the configuration-settings file to import (for example, `jre-8u151-windows-x64-with-configfile.zip`).
6. Click **Import** to upload the file to the OS-images repository.
7. Click the **Import** icon ( ) again.
8. Click **Local Import**.
9. Select `Windows` for the operating system.
10. Click **Browse** to find and select the configuration-settings file to import (for example, `eclipse-java-oxygen-1a-win32-x86_64.zip`).
11. Click **Import** to upload the file to the OS-images repository.

Step 4. Create a custom post-installation script, and import the file to the OS-images repository.

Add commands to install the software, for example:

```
Write-Output "Install Java...."
Invoke-Command -ScriptBlock
        {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
        [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
        /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
        "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
        -DestinationPath $eclipseDir
```

Note that these command use the predefined macro for the path to the extracted data and software files (**predefined.otherSettings.deployDataAndSoftwareLocation**).

You can also add commands to send custom messages to the jobs log in XClarity Administrator, as shown in the sample file. For more information, see Adding custom status reporting to installation scripts.

To import the custom installation script, complete these steps. For more information, see Importing custom installation scripts

1. Click the **Installation Scripts** tab.
2. Click the **Import** icon ( ).
3. Click **Local Import**.
4. Select `Windows` for the operating system.
5. Click **Browse** to find and select the unattend file to import (for example, `Windows_installSoftware_customScript.ps1`).
6. Click **Import** to upload the file to the OS-images repository.

Step 5. Create a custom OS-image profile that includes the custom unattend file. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select an OS-image profile to customize (for example, `Datacenter virtualization`).

3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom Windows with software`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **None** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Boot Options** tab, and click **Next**. The predefined WinPE boot file is selected by default.
7. On the **Software** tab, select the software installation files (for example `jre-8u151-windows-x64-with-configfile.zip` and `eclipse-java-oxygen-1a-win32-x86_64.zip`), and click **Next**.
8. On the **Installation Scripts** tab, select the installation scripts (for example, `Windows_installSoftware_customScript.ps1`), and click **Next**.
9. On the **Summary** tab, review the settings.
10. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.
   c. Select the custom OS-image profile (for example, *<base_OS>*|*<timestamp>*`_Custom Windows with software`) from the drop-down list in the **Image to Deploy** column

      Note: Ensure that all target servers use the same custom profile.
   d. (Optional) Click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.
   e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating-system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.
   f. Verify that the deployment status for the selected server is **Ready**.
3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Summary** tab, review the settings.
5. Click **Deploy** to deploy the operating system.

Deploying Windows 2016 for Japanese

This scenario installs the Windows 2016 operating system to multiple servers with Japanese enabled for the keyboard and operating-system locales. A custom profile is used that includes a custom WinPE boot file and unattend file. The custom profile can then be selected on the Deploy OS Images page.

Before you begin

This scenario uses the following sample files.

- `WinPE_64_ja.zip`. This custom Windows boot (WinPE) file installs the Japanese locale.
- Windows_locale_customUnattend.xml. This custom unattend file uses the WinPE file to install Japanese.

Notes: The sample custom unattend file assumes the following:

- The server only has one visible disk (disk 0) and does not already have a system partition on it.
- Static IPv4 mode is used and sets a static IP (which gets used in the custom unattend as a predefined macro).

Procedure

To deploy Japanese Windows 2016 to target servers using a custom OS-image profile, complete the following steps.

Step 1. Download the Japanese Windows 2016 operating system to the local system, and import the image to the OS-images repository. For more information, see Importing operating-system images.

1. From the XClarity Administrator menu bar, click **Provisioning → Manage OS Images** to display the Deploy Operating System: Manage OS Images page.
2. Click the **OS Images** tab.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Click **Import** to upload the image to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 2. Download the bundle file for Windows 2016 to the local system, and import the image to the OS-images repository. For more information, see Importing device drivers.

The bundle file contains the latest device drivers and WinPE boot files that you can add to your custom OS-images profiles. This scenario uses a custom boot file, so the boot file in the bundle will not be used.

1. Click the **Driver Files** tab.
2. Click **Downloads → Windows Bundle Files** to go to the Lenovo Support webpage, and download the bundle file for Windows 2016 to the local system.
3. Click **Import** icon ().
4. Click **Local Import**.
5. Click **Browse** to find and select the OS image that you want to import (for example, `bundle_win2016_20180126130051.zip`).
6. Click **Import** to upload the file to the OS-images repository.
7. Wait for the import to complete. This might take a while.

Step 3. Optional: Create a custom WinPE boot file that uses the Japanese locale during the WinPE install, and import the file to the OS-images repository.

XClarity Administrator uses a predefined Windows PreInstallation (WinPE) boot file to install the Windows operating system. The locale that is used with this predefined boot file is English (en-US). If you want to change the locale that is used during Windows Setup, you can create a custom WinPE boot file with the desired locale and assign that custom boot file to your custom profile.

For information about injecting locales into WinPE, see the Windows WinPE: Add packages webpage.

Important: Specifying a non-English locale in the WinPE boot file does not change the locale of the final OS being deployed. It only changes the locale that is shown during Windows install and setup.

To create a custom WinPE boot file that includes the Japanese locale, complete these steps. For more information, see Creating a boot (WinPE) file.

1. Using a user ID with administrator authority, run the Windows ADK command "Deployment and Imaging Tools Environment." A command session is displayed.
2. From the command session, change to the directory where the **genimage.cmd** and **starnet.cmd** files were downloaded (for example, `C:\customwim`).
3. Ensure that no previously mounted images are on the host by running the following command:
   `dism /get-mountedwiminfo`

   If there are mounted images, discard them by running the following command:

   `dism /unmount-wim /MountDir:C:\<mount_path> /Discard`
4. If you are adding in-box device drivers to a customized Windows profile, copy the raw device-driver files, in .inf format, to the host system in the `C:\drivers` directory.
5. Run the following command to generate the boot file, in .wim format, and then wait a few minutes for the command to complete.
   `genimage.cmd amd64 <ADK_Version>`

   Where *<ADK_Version>* is one of the following values.

   - **8.1**. For Windows 2012 R2
   - **10**. For Windows 2016

   This command creates a boot file named `C:\WinPE_64\media\Boot\WinPE_64.wim`.
6. Mount the boot file by running the following command:
   `DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount`
7. If you are adding out-of-box device drivers directly to the boot file, complete the following steps.
   a. Create the following directory structure, where *<os_release>* is `2012R2`, or `2016`
      `drivers\<os_release>\`
   b. Copy the device drivers, in .inf format, to a directory inside that path, for example:
      `drivers\<os_release>\<driver1>\<driver1_files>`
   c. Copy the `drivers` directory to the mount directory, for example:
      `C:\WinPE_64\mount\drivers`
8. **Optional:** Make additional customizations to the boot file, such as adding folders, files, startup scripts, language packs, and apps. For more information about customizing boot files, see the WinPE: Mount and Customize website.
9. Add the Japanese packages, for example.

10. View installed packages to ensure that the Japanese-specific packages are installed.

```
Dism /Add-Package /Image:"C:\WinPE_64\mount"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
```

11. Review the International Settings in the image.

```
Dism /Get-Packages /Image:"C:\WinPE_64\mount"
```

12. Unmount the image by running the following command.

```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```

13. Compress the contents of the `C:\WinPE_64\media` directory into a zip file called `WinPE_64_ja.zip`.
14. Import the .zip file into XClarity Administrator (see Importing boot files).
    a. Click the **Boot Files** tab.
    b. Click **Import** icon ().
    c. Click **Local Import**.
    d. Select `Windows` for the operating system.
    e. Click **Browse** to find and select the custom boot file (for example, `WinPE_64_ja.zip`).
    f. Click **Import** to upload the file to the OS-images repository.

Step 4. Modify the Windows unattend file to specify that Japanese is included in the OS image, and import the custom file to the OS-images repository.

In the “windowsPE” pass of the Windows install, add the Japanese as the operating-system language and the locale, for example:

```
<settings pass="windowsPE">
   <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
              publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
              xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
         <UILanguage>ja-JP</UILanguage>
      </SetupUILanguage>
      <SystemLocale>ja-JP</SystemLocale>
      <UILanguage>ja-JP</UILanguage>
      <UserLocale>ja-JP</UserLocale>
      <InputLocale>0411:00000411</InputLocale>
   </component>
</settings>
```

Note: When you use a custom unattend file, XClarity Administrator does not provide many of the normal convenience features that you get when you use a predefined unattend file. For example, the targets `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>`, and `<UserAccounts>` for Administrator, `<Interfaces>` for networking, and `<package>` list for installation features must be specified in the custom unattend file that is being uploaded.

XClarity Administrator provides some basic convenience macros, such as OOB driver injection, status reporting, post-install scripts, custom software. However, to take advantage of these predefine macros, you must specify the following macros in the custom unattend file.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

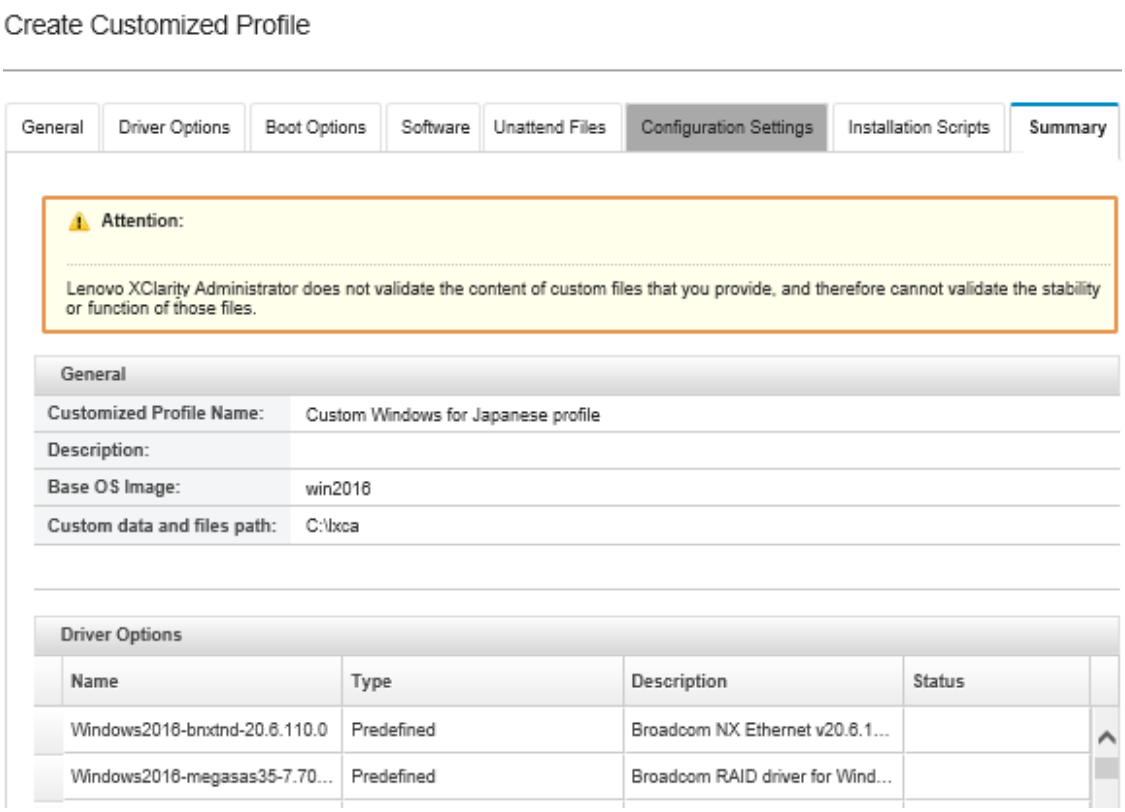
The example file already contains the required macros. For more information about adding macros to unattend files, see Injecting predefined and custom macros to an unattend file. For more information about available predefined macros, see Predefined macros.

To import the custom unattend file, complete these steps. For more information, see Importing custom unattend files.

1. Click the **Unattend Files** tab.
2. Click **Import** icon ( ).
3. Click **Local Import**.
4. Select `Windows` for the operating system.
5. Click **Browse** to find and select the custom unattend file (for example, `Windows_locale_customUnattend.xml`).
6. Click **Import** to upload the file to the OS-images repository.

Step 5. Create a custom OS-image profile that includes the custom boot (WinPE) file and unattend file. For more information, see Creating a custom OS-image profile.

1. Click the **OS Images** tab.
2. Select the profile to customize (for example, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Click **Create** icon ( ) to display the Create Customized Profile dialog.
4. On the **General** tab:
   a. Enter a name for the profile (for example, `Custom Windows for Japanese profile`).
   b. Use the default value for the **Custom data and file path** field.
   c. Select **Only unattend files** for the customization type.
   d. Click **Next**.
5. On the **Driver Options** tab, click **Next**. The inbox device drivers are included by default.
6. On the **Boot Files** tab, select custom boot file (for example, `WinPE_64_ja`), and click **Next**.
7. On the **Software** tab, click **Next**.
8. On the **Unattend Files** tab, select custom unattend file (for example, `Windows_locale_customUnattend.xml`), and click **Next**.
9. On the **Installation Scripts** tab, click **Next**.
10. On the **Summary** tab, review the settings.



11. Click **Customize** to create the custom OS-image profile.

Step 6. Deploy the custom OS-image profile to the target servers. For more information, see Deploying an operating-system image.

1. From the XClarity Administrator menu bar, click **Provisioning → Deploy OS Images** to display the Deploy Operating System: Deploy OS Images page.
2. For each target server:
   a. Select the server.
   b. Click **Change Selected → Network Settings**, and specify the hostname, IP address, subnet mask, gateway, DNS, MTU and VLAN settings for the server.

      Tip: VLAN settings are available only when VLAN mode is set in **Global Settings → IP Assignment → Use VLANs**.

   c. Select the custom OS-image profile (for example, <*base_OS*>|<*timestamp*>_`Custom Windows for Japanese profile`) from the drop-down list in the **Image to Deploy** column.

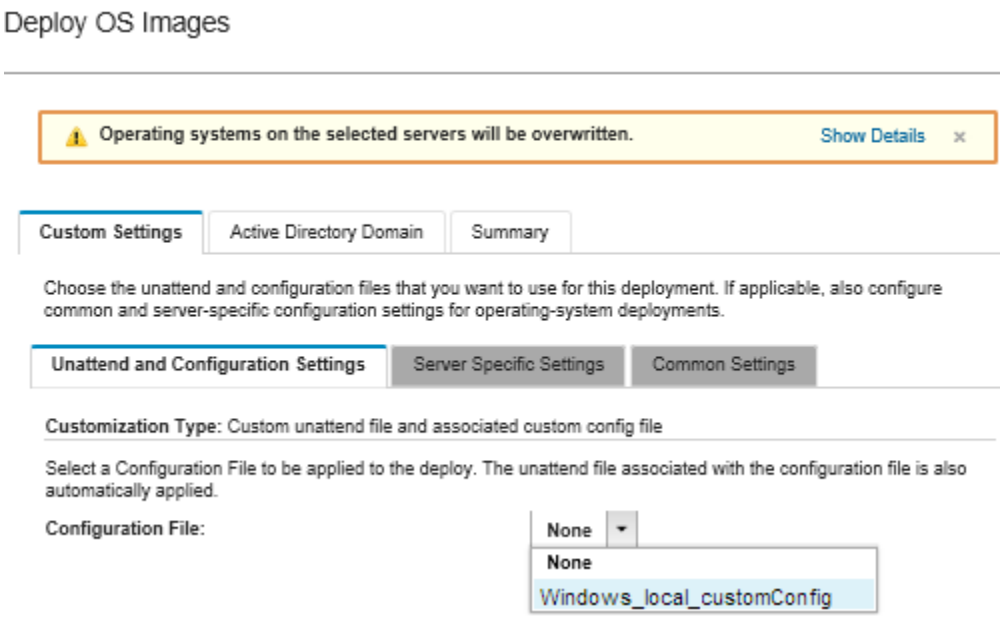
      Note: Ensure that all target servers use the same custom profile.

   d. (Optional) Click the **License Key** icon ( ) and specify the license key to use to activate the operating system after it is installed.
   e. Select the preferred storage location where you want to deploy the operating system image from the **Storage** column.

      Note: To ensure that operating system deployments are successful, detach all storage from the managed server except the storage that is chosen for the operating-system deployment.

   f. Verify that the deployment status for the selected server is **Ready**.

3. Select all target servers, and click the **Deploy image** icon ( ) to initiate the operating-system deployment.
4. On the **Custom Settings** tab, click the **Unattend and Configuration Settings** subtab, and select the custom unattend file (for example, `Windows_locale_customUnattend.xml`).



5. (Optional) On the **Active Directory Domain** tab, specify information to join an Active Directory domain as part of a Windows image deployment (see Integrating with Windows Active Directory).
6. On the **Summary** tab, review the settings.
7. Click **Deploy** to deploy the operating system.

   The Windows installation dialog is displayed in Japanese.

   After installation is complete, the Windows login page also displayed in Japanese.

Administrator
パスワード
パスワードのリセット

Chapter 16. End-to-end scenarios for setting up new devices

Use these end-to-end scenarios describe how to help you use Lenovo XClarity Administrator to set up new devices in a way that is consistent and easily repeatable.

Deploying ESXi to a local hard drive

Use these procedures to deploy VMware ESXi 5.5 to a locally installed hard drive on a Flex System x240 Compute Node. It illustrates how to learn a server pattern from an existing server, modify the extended UEFI-settings category pattern for that server pattern, and how to install VMware ESXi.

VMware ESXi 5.5 requires memory-mapped I/O (MMIO) space to be configured within the initial 4 GB of the system. Depending on the configuration, certain systems attempt to use memory higher than 4 GB, which might cause a failure. To resolve the issue, you can increase the value of the MM Config option to 3 GB through the Setup utility for each server on which VMware ESXi 5.5 is going to be installed.

An alternative is to deploy a server pattern that contains one of the predefined extended UEFI category patterns that is related to virtualization, which sets the MM Config option and disables the PCI 64-bit resource allocation.

Deploying a predefined virtualization pattern

A category pattern defines specific firmware settings that can be reused by multiple server patterns. To deploy a predefined virtualization pattern, you create a server pattern and then apply a predefined extended UEFI pattern to that server pattern. That server pattern can then be applied to multiple servers of the same type, such as the Flex System x240 Compute Node or the Flex System x880 X6 Compute Node.

About this task

When creating a server pattern, you can choose to complete the configuration yourself or learn the pattern attributes from an existing server that has already been set up. When you learn a new pattern from an existing server, most of the pattern attributes are already defined.

For more information about server patterns and category patterns, see Working with server patterns.

Procedure

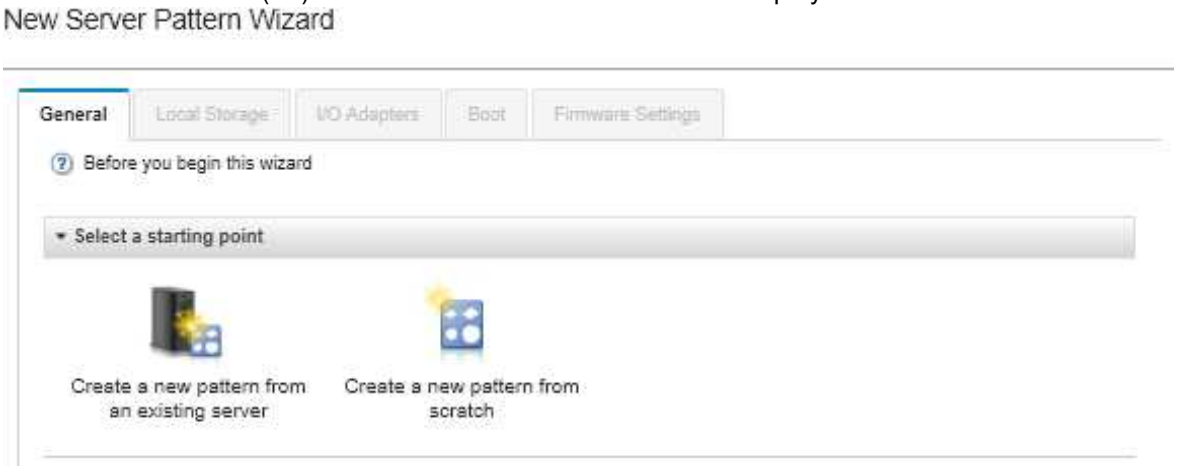
To learn a new pattern from an existing server, complete the following steps.

Step 1. From the XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

Step 2. Click the **Server Patterns** tab.

© Copyright Lenovo 2015, 2022

Step 3. Click the **Create** icon ( ). The New Server Patterns Wizard is displayed.



Step 4. Click **Create a new pattern from an existing server**. You can choose to create a pattern from scratch, but it is typically more efficient to create a pattern from an existing server that has the desired configuration.

When you create a server pattern from an existing server, XClarity Administrator learns the settings from a managed server (including the extended port, UEFI, and baseboard management controller settings) and dynamically creates category patterns for those settings. If the server is brand new, XClarity Administrator learns the manufacturing settings. If the server is in use, XClarity Administrator learns the customized settings. You can then modify the settings specifically for the server to which this pattern is to be deployed.

Step 5. Select the server to use as a base configuration when creating the pattern.

Note: Remember that the server that you choose must be the same model as the servers to which you intend to deploy the server pattern. This scenario is based on choosing a Flex System x240 Compute Node.

Step 6. Enter the name of the new pattern, and provide a description.

For example:

- Name: **x240_ESXi_deployment**
- Description: **Pattern with extended UEFI settings that are appropriate for the deployment of VMware ESXi**

Step 7. Click **Next** to load the information from the selected server.

Step 8. On the **Local Storage** tab, select **Specify storage configuration**, and choose one of the storage types. Then click **Next**.

For more information about the local-storage settings, see Defining local storage.

Step 9. On the **I/O adapters** tab, enter information about the adapters that are in the servers on which you intend to install VMware ESXi.

Any adapters that were present in the server used as a base are displayed.

If all Flex System x240 Compute Nodes in your installation have the same adapters, you do not need to modify any settings on this tab.

For more information about the I/O adapters settings, see Defining I/O adapters.

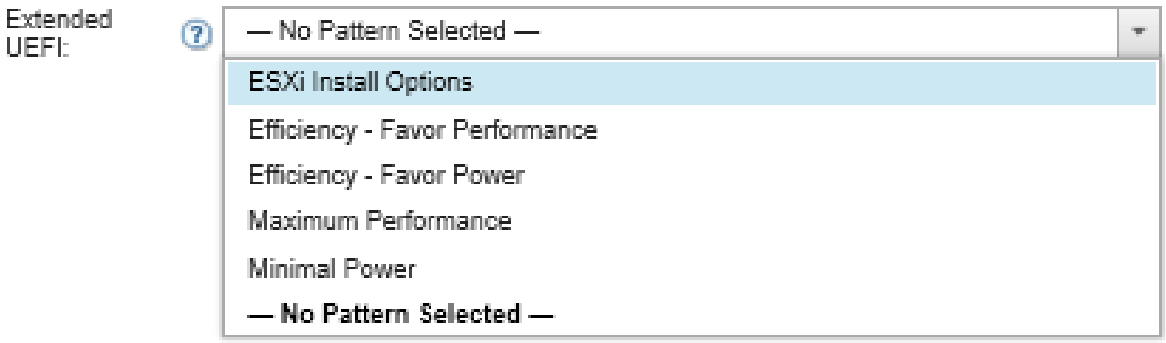
Step 10. Click **Next** to continue.

Step 11. On the **Boot** tab, configure settings for legacy-only boot environment and SAN boot environments. Unless you are using one of these environments, accept the default, which is **UEFI Only Boot**, and click **Next**.

For more information about the boot settings, see Defining boot options.

Step 12. On the **Firmware Settings** tab, specify the management controller and UEFI firmware settings that are to be used for target servers when this pattern is deployed (for example, select **x240 Virtualization**).

On this tab, you can choose one of the predefined extended UEFI patterns:



For more information about the firmware settings, see Defining firmware settings.

Step 13. Click **Save and Deploy** to save the pattern to XClarity Administrator and deploy it to the servers on which you intend to install VMware ESXi.

After you finish

After the server pattern has been deployed to all servers, you can install the operating system on those servers.

Deploying VMware ESXi to a Flex System x240 Compute Node

Use this procedure as an example flow to illustrate the process for deploying the ESXi operating system to a Flex System x240 Compute Node.

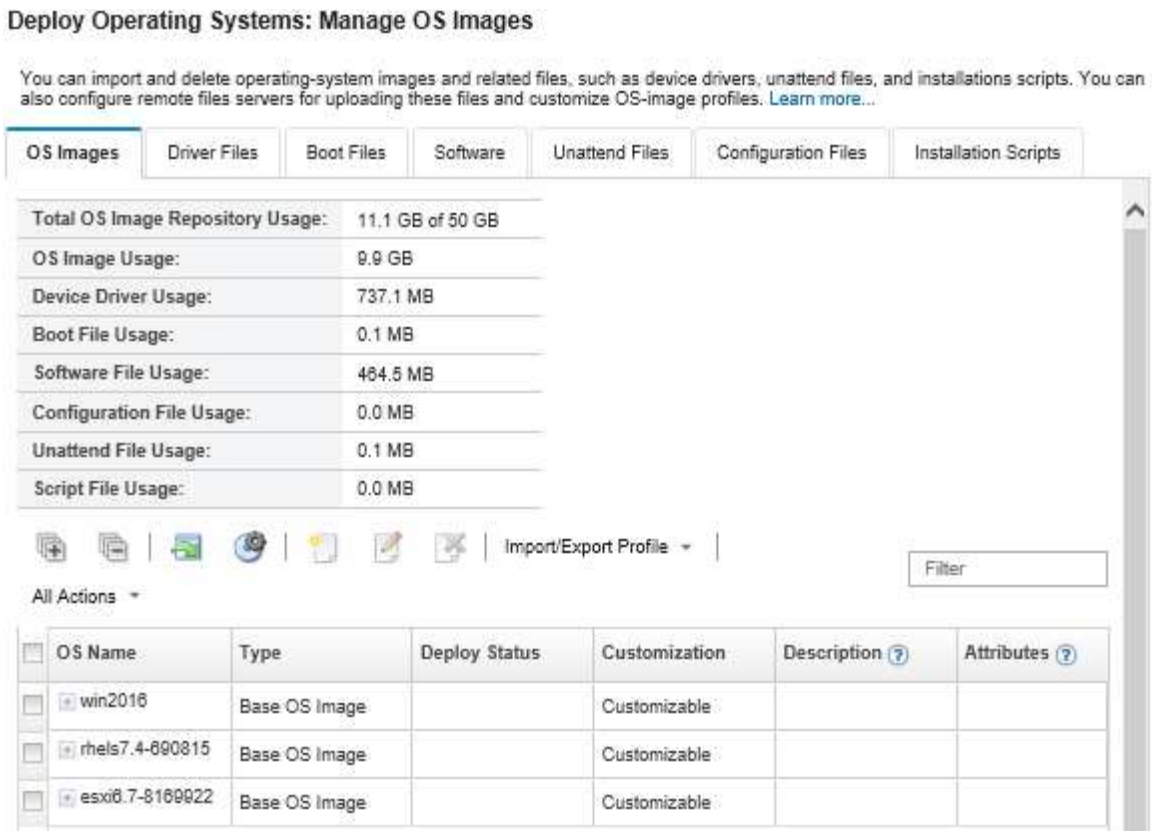
Before you begin

Before you begin this procedure, ensure that Lenovo XClarity Administrator is managing the chassis in which the Flex System x240 Compute Node is installed.

Procedure

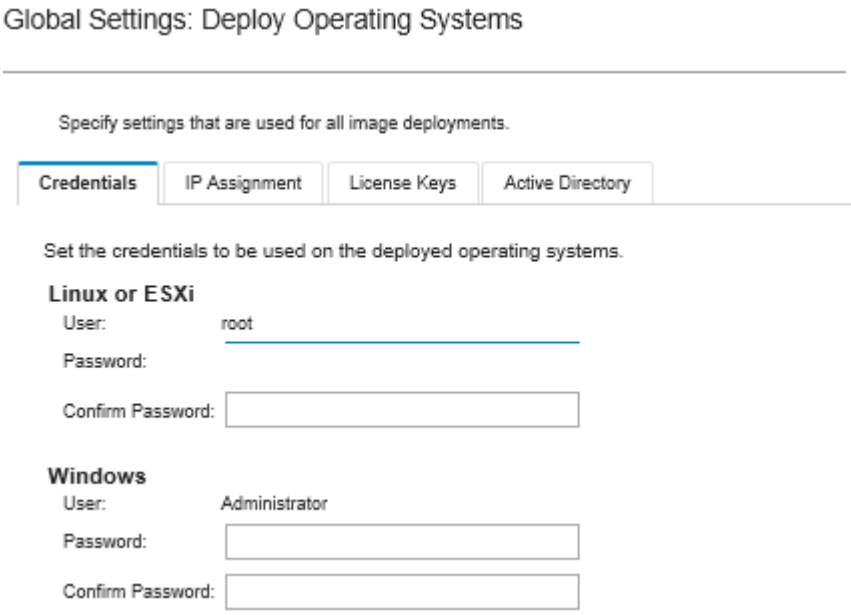
Complete the following steps to deploy the ESXi operating system to an Flex System x240 Compute Node.

Step 1. Ensure that the image to be deployed is already loaded into the OS images repository by click **All actions → Manage OS images** to display a list of all available images.



Step 2. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Deploy OS images**. The Deploy OS Images page is displayed.

Step 3. Set global settings that are to be used as defaults for all image deployments by clicking **All actions → Global Settings** to display the Global Settings dialog.



a. On the **Credentials** tab, enter the password that is to be used by the administrator account to log in to the operating system.

b. On the **IP Assignment** tab, specify how the IP address for the operating system will be assigned to the server.

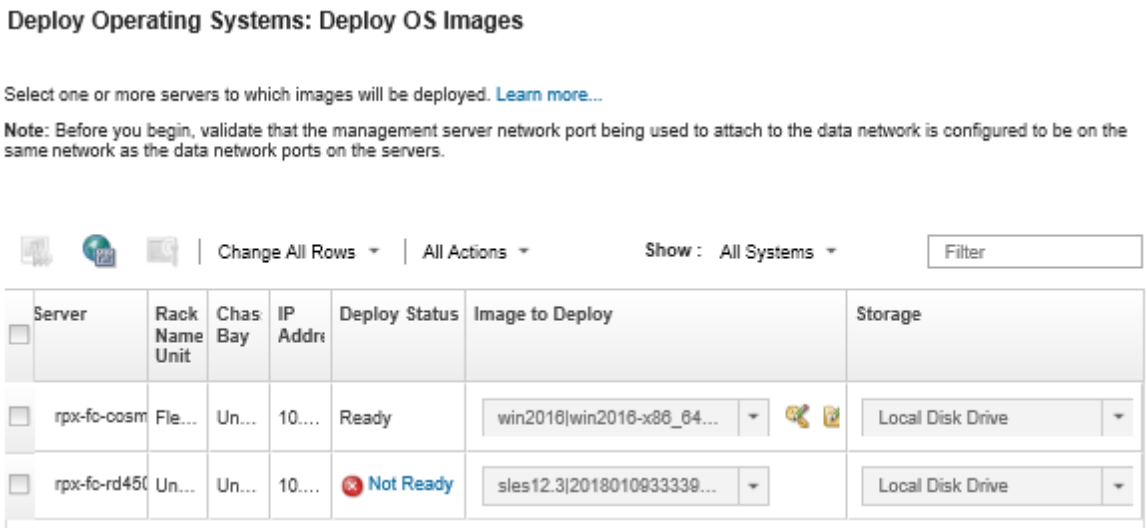
   If you choose **Use Dynamic Host Configuration Protocol (DHCP)** to assign IP addresses, the IP address information is not displayed on the Edit Network Settings dialog (see step Step 8 9 on page 579). If you choose **Assign static IP address (IPv4)**, you can specify an IP address, subnet, and gateway for each deployment.

c. On the **License Keys** tab, enter a mass-activation license key, if desired.

d. Click **OK** to close the dialog.

Step 4. Ensure that the server is ready for operating system deployment. by selecting the server to which the operating system is to be deployed. Initially, the deployment status might be shown as Not Ready. The deployment status must be Ready before you can deploy an operating system to a server.

Tip: You can choose multiple servers in multiple Flex System chassis if you intend to deploy the same operating system to all servers. You can choose up to 28 server.



Step 5. Click in the **Image to Deploy** column, and select VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Step 6. In that same column, click the **License Key** icon ( ) to enter the license key for this deployment.

Tip: You can also choose to use a mass-activation key that you entered in the Global Settings dialog.

Step 7. Ensure that **Local Disk** is selected in the Storage column.

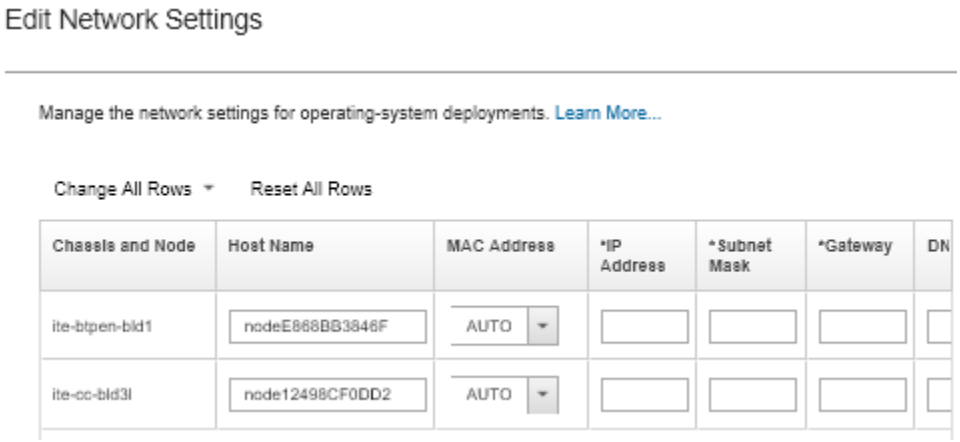
Step 8. Click **Edit** in the **Network Settings** column of the server row to configure the network settings that are to be used for this deployment. The Edit Network Settings page is displayed.

Fill in the following fields:

- Hostname
- MAC address of the port on the host where the operating system is to be installed
- Domain name system (DNS) servers, if required
- maximum transmission unit (MTU) speed

Notes: If you chose **Assign static IP address (IPv4)** from the Global Settings dialog (see step Step 3 4 on page 578), also enter the following information:

- IPv4 address
- Subnet mask
- Gateway



Step 9. Click **OK** to close the dialog.

From the Deploy OS images page, ensure that the server shows a Deploy Status of Ready.

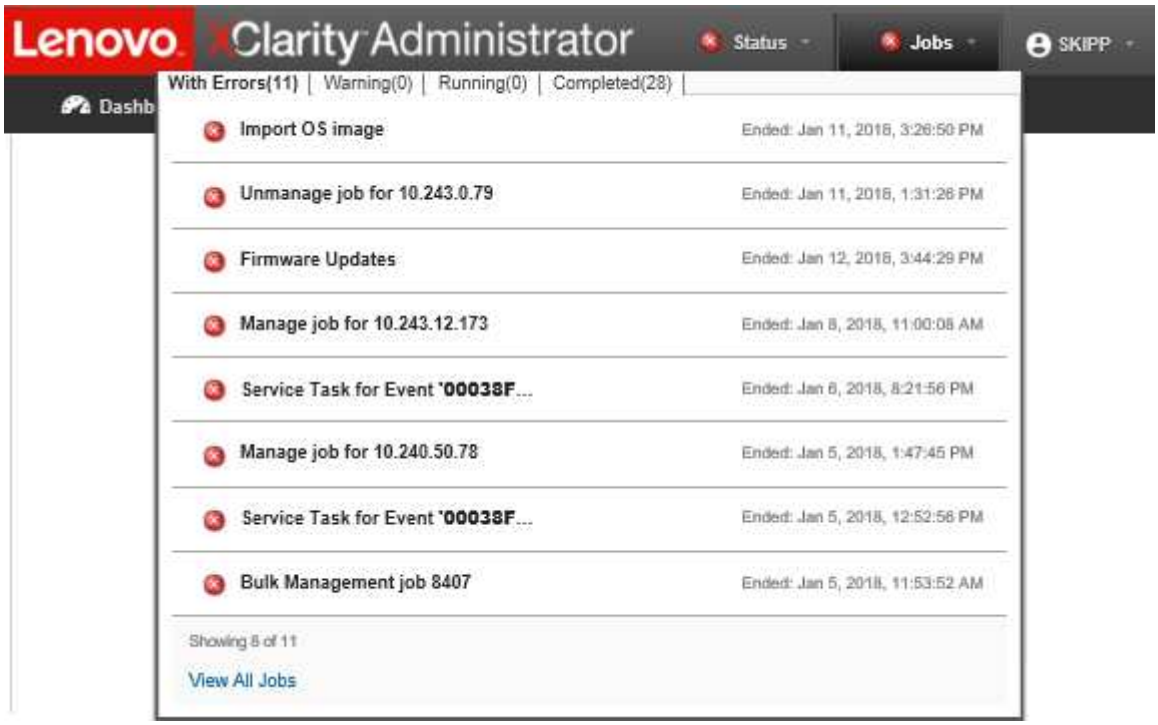
Step 10. Deploy the operating system by clicking **All actions → Deploy images**.

Step 11. From the confirmation page, click **Deploy** to deploy the image.

If the server currently has an operating system installed, you are warned about the fact that deploying the image will overwrite the current operating system.

Tip: You can set up a Remote Control session to watch the installation as it progresses. Click **All actions → Remote Control** to start a Remote Control session with the server.

When you deploy the operating system, Lenovo XClarity Administrator starts a job to track the deployment. To view the status of the deployment job, click **Jobs** from the Lenovo XClarity Administrator menu bar. Then, click the **Running** tab.

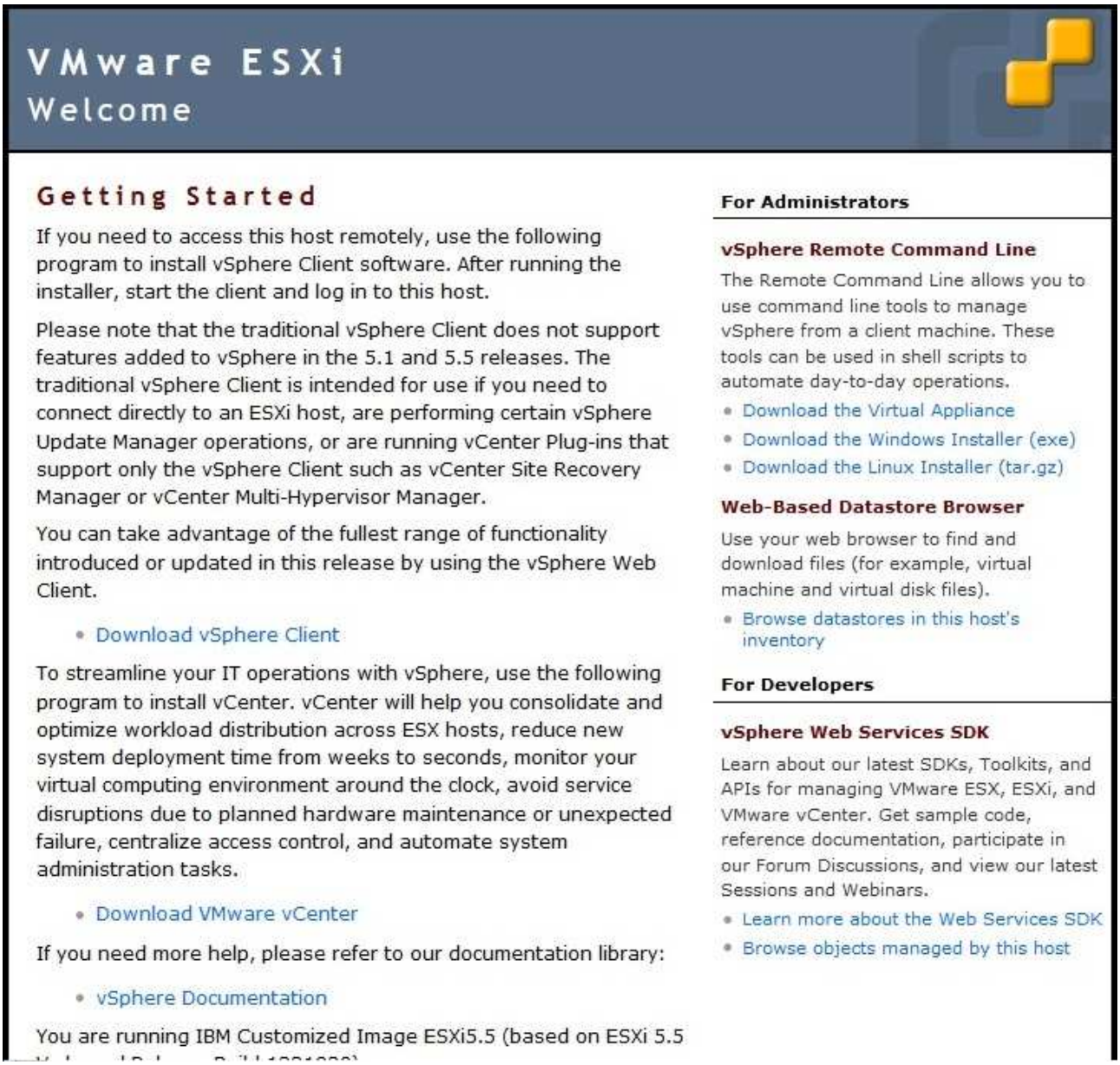


Hover over the running job to see the details, such as the percentage of the job that is complete.

Results

After the operating system deployment has completed, log in to the IP address that you specified on the Edit Network Settings page to continue with the configuration process.

Note: The license provided with the image is a 60-day free trial. You are responsible for meeting all VMware licensing requirements.



Deploying ESXi to SAN storage

Use these procedures to deploy VMware ESXi 5.5 to SAN volumes that are attached to servers.

When you deploy an operating system to a SAN, the operating system is deployed to the first SAN boot target that is configured through a server pattern. In addition, a local hard drive cannot be enabled in the server that will be booting from SAN. It must be disabled or removed if a hard drive is present.

Deploying a server pattern to support SAN boot

When you create and deploy a server pattern to support booting a system from SAN, ensure that you identify the SAN boot target and the adapters that are part of the server.

Procedure

To create and deploy a server pattern that supports the deployment of the operating system on SAN storage, complete the following steps.

Step 1. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Patterns**. The Configuration Patterns: Patterns page is displayed.

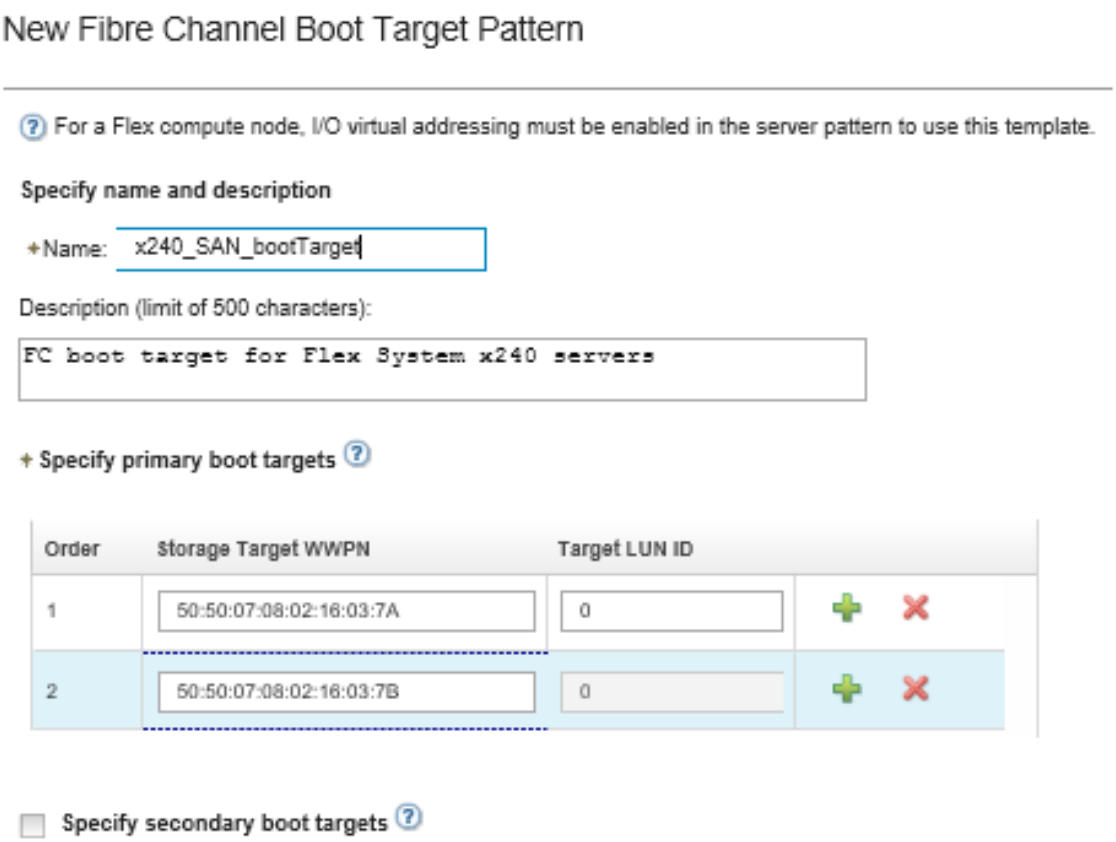
Step 2. To identify the WWPN and LUN IDs of the storage volumes where the operating system is to be deployed, create a category pattern.

a. Click the **Category Patterns** tab.

b. Click **Fibre Channel Boot Target Patterns**, and then click the **Create** icon ( ).

c. Enter the WWPN of the storage target.

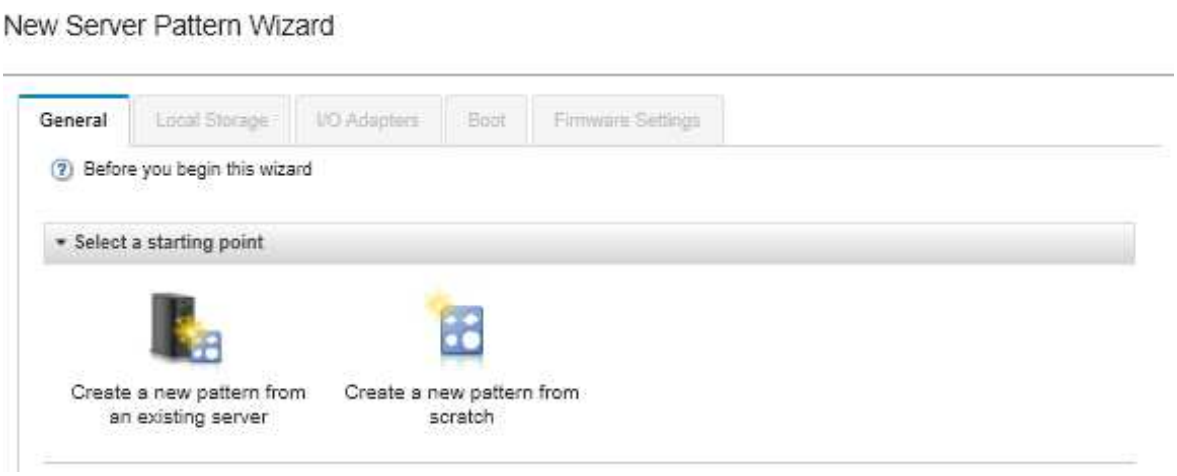
Note: Click **Allow Multiple LUN Identifiers** to assign multiple target LUN identifiers to the same storage volumes.



d. Click **Create** to create the pattern. The target is displayed in the list of Fibre Channel boot target patterns.

Step 3. Click the **Server Patterns** tab to create a pattern.

Step 4. Click the **Create** icon ( ). The New Server Patterns Wizard is displayed.



Step 5. Click **Create a new pattern from scratch**.

Step 6. On the **General** tab:

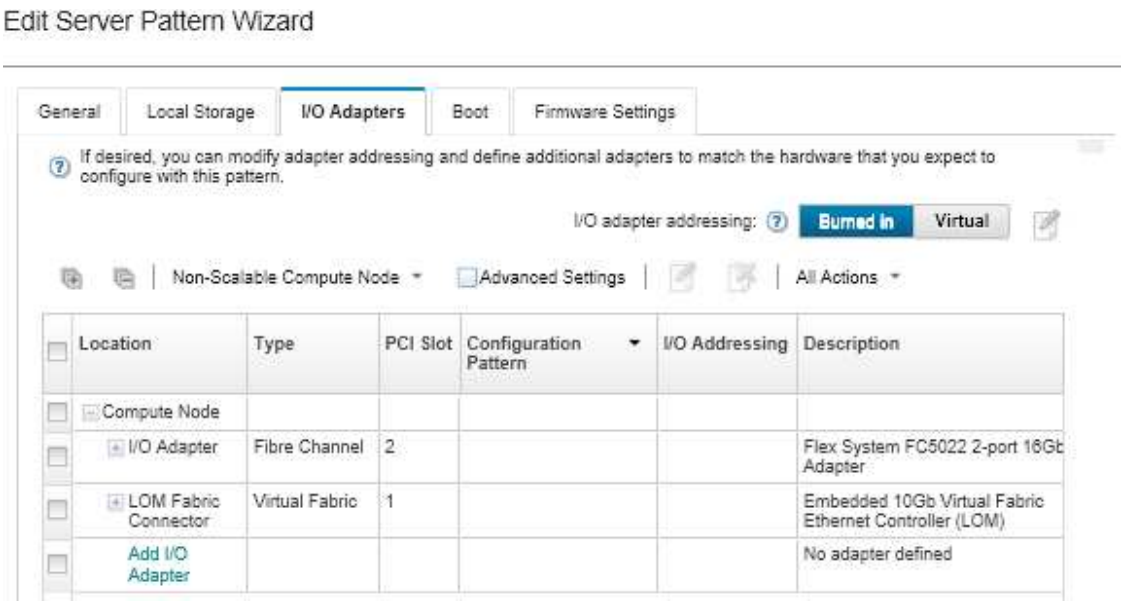
- Select **Flex Compute Node** for the form factor.
- Specify a pattern name (**x240_san_boot**) and description.
- Click **Next**.

Step 7. On the **Local Storage** tab, consider disabling the local storage adapter if you are using a diskless system to improve boot times that are related to scanning for local drives. Then, click **Next**.

Step 8. On the **I/O Adapters** tab, add the Ethernet and Fibre Channel cards. Ensure that they are in the appropriate PCI slots.

a. For each card, click **Add I/O Adapter**, choose the PCI slot where the card is located, and select the card.

Note: Ensure that you specify an Ethernet card and a Fibre Channel card.



b. Ensure that I/O adapter addressing is set to **Virtual**. Then click the **Edit** icon to specify the configuration to be used for Ethernet (MAC) virtual addressing and Fibre Channel (WWN) virtual addressing.

Note: From the Edit Virtual Addressing page, you can choose to use the burned-in MAC address for the Ethernet card by disabling the virtual addressing. However, to select and use a Fibre Channel boot-target pattern, you must use virtual addressing for the Fibre Channel adapter.

c. Click **Next**.

Step 9. On the **Boot** tab, add the SAN boot target pattern that you created earlier.

a. On the **SAN Boot** tab, choose the boot target pattern that you defined.

b. Click **Next**.

Step 10. On the **Firmware Settings** tab, define any additional category patterns that are to be included in this server pattern. You can define the following category patterns.

- **System information** (see Defining system-information settings)
- **Management interface** (see Defining management-interface settings
- **Device and I/O ports** (see Defining devices and I/O ports settings
- **Extended BMC**. You can choose from baseboard management controller settings that have been learned previously (see Defining extended management-controller settings).
- **Extended UEFI**. You can choose from predefined settings or from UEFI settings that have been learned previously (see Defining extended UEFI settings).

Step 11. Click **Save and Deploy** to save the pattern to Lenovo XClarity Administrator, and deploy it to the servers on which you intend to install VMware ESXi.

After you finish

Consider the following steps after the server pattern has been deployed to all servers.

1. Take the virtualized WWPN addresses that were created, and add them to the storage zone so that the server can reach the defined storage LUNs.

   Tip: After you deploy the server profile, you can find the virtualized WWPN addresses by viewing the server profile.

   a. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Server profiles**.

   b. Click the deployed server profile (for example, **x240_SAN_boot**). The **Virtual Address Mapping** tab displays the list of addresses.

2. Deploy the operating system to the server.

Deploying VMware ESXi to SAN storage

Use this procedure as an example flow to illustrate the process for deploying the ESXi operating system to SAN storage that is connected to a server.

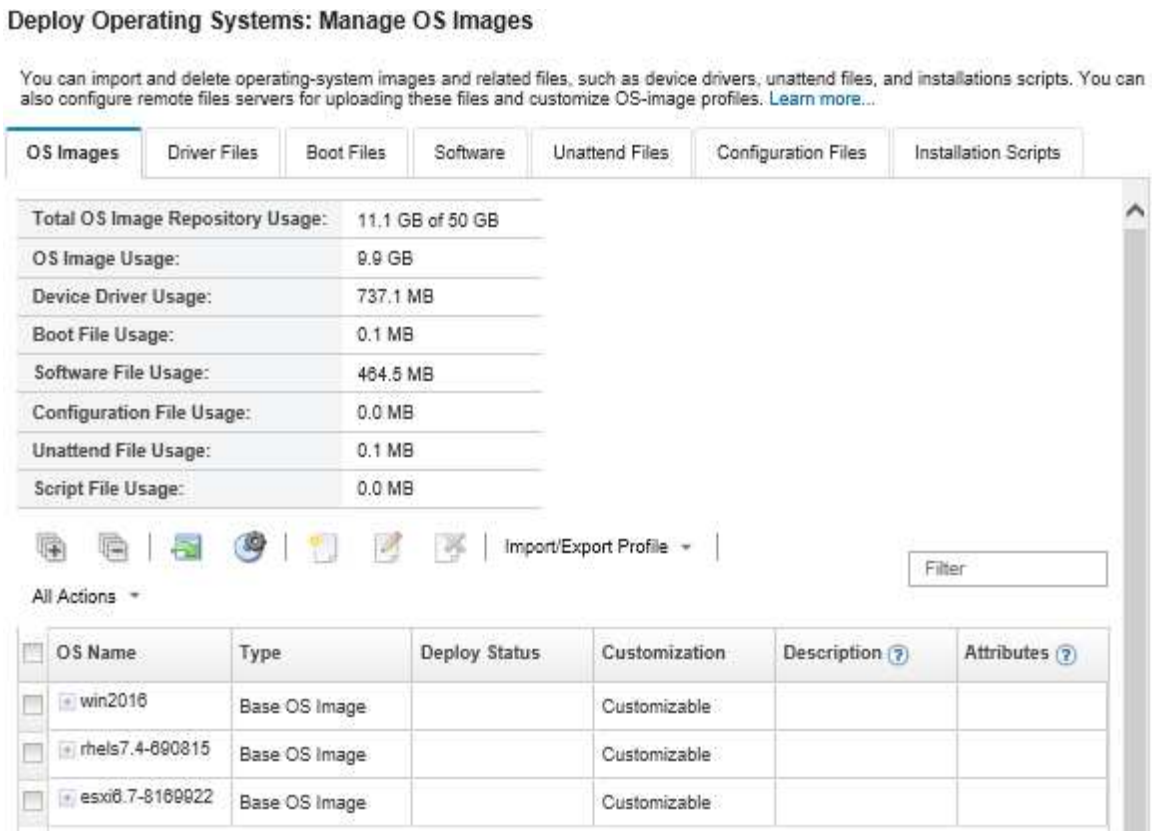
Before you begin

Before you begin this procedure, ensure that Lenovo XClarity Administrator is managing the chassis in which the Flex System x220 Compute Node is installed.

Procedure

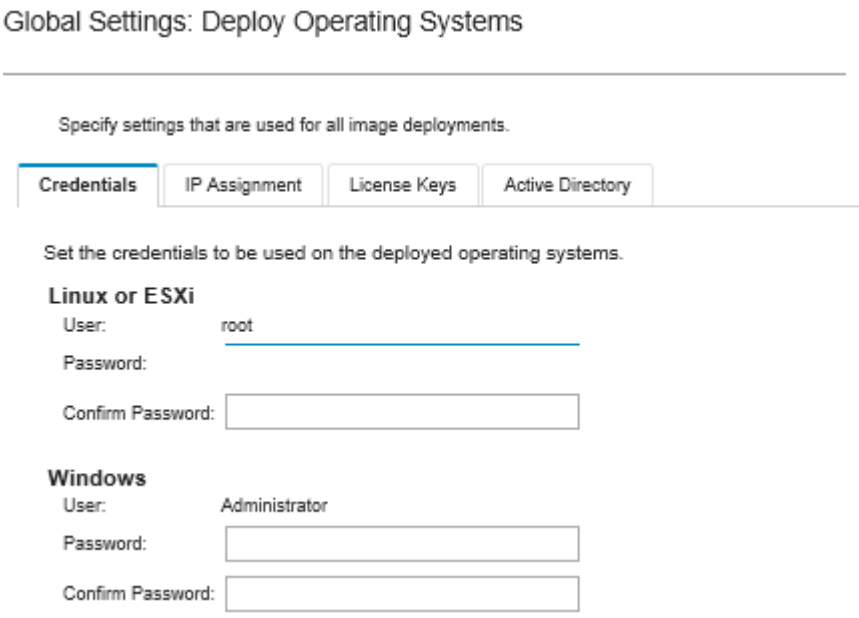
Complete the following steps to deploy the ESXi operating system to an Flex System x222 Compute Node.

Step 1. Ensure that the image to be deployed is already loaded into the OS images repository by clicking **All actions → Manage OS images**.



Step 2. From the Lenovo XClarity Administrator menu bar, click **Provisioning → Deploy OS images**

Step 3. Set global settings that are to be used as a default for all image deployments by clicking **All actions → Global Settings** to display the Global Settings: Deploy Operating Systems dialog.



a. On the **Credentials** tab, enter the password that is to be used by the administrator account to log in to the operating system.

b. On the IP **Assignment** tab, specify how the IP address for the operating system is to be assigned to the server.

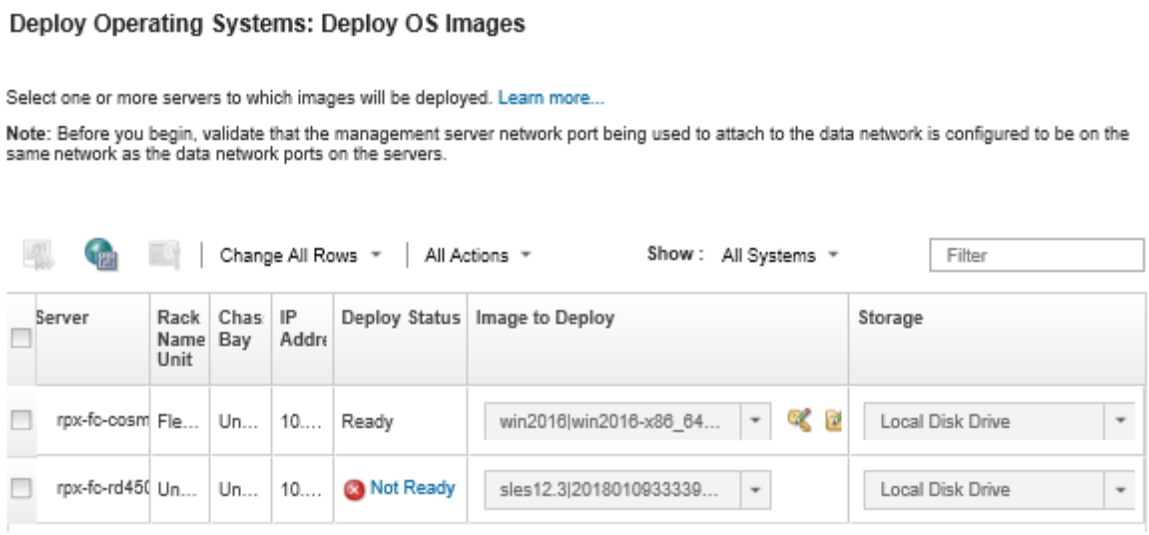
If you choose **Use Dynamic Host Configuration Protocol (DHCP)** to assign IP addresses, the IP address information will not be displayed on the Edit Network Settings dialog (see step Step 8 9 on page 587). If you choose **Assign static IP address (IPv4)**, you can specify an IP address, subnet, and gateway for each deployment.

c. On the **License Keys** tab, enter a mass-activation license key, if desired.

d. Click **OK** to close the dialog.

Step 4. Ensure that the server is ready for operating-system deployment by selecting server to which the operating system is to be deployed. Initially, the deployment status might be shown as Not Ready. The deployment status must be Ready before you can deploy an operating system to a server.

Tip: You can choose multiple servers from multiple Flex System chassis if you intend to deploy the same operating system to all servers. You can choose up to 28 servers.



Step 5. Click in the **Image to Deploy** column, and select VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Step 6. In that same column, click the **License Key** icon ( ) to enter the license key for this deployment.

Tip: You can also choose to use a mass-activation key that you entered in the Global Settings: Deploy Operating Systems dialog.

Step 7. In the **Storage** column, select the SAN storage to which the operating system is to be deployed.

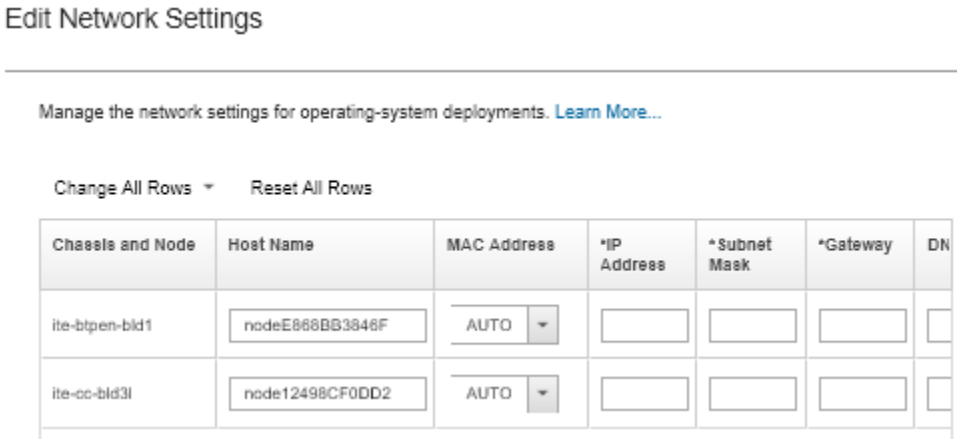
The storage is listed as:
`LUN: <LUN VALUE>  WWPN: <WWPN_VALUE>`

Step 8. Click **Edit** in the **Network Settings** column of the server row to configure the network settings that is to be used for this deployment. The Edit Network Settings page is displayed.

Fill in the following fields:
- Hostname
- MAC address of the port on the host where the operating system will be installed
- Domain name system (DNS) serveres, if required
- Maximum transmission unit (MTU) speed

Notes: If you chose **Assign static IP address (IPv4)** from the Global Settings: Deploy Operating Systems dialog (step Step 3 4 on page 586), also enter the following information:
- IPv4 address
- Subnet mask

- Gateway



Step 9. Click **OK** to close the dialog.

From the Deploy OS images page, the server now shows a deployment status of Ready.

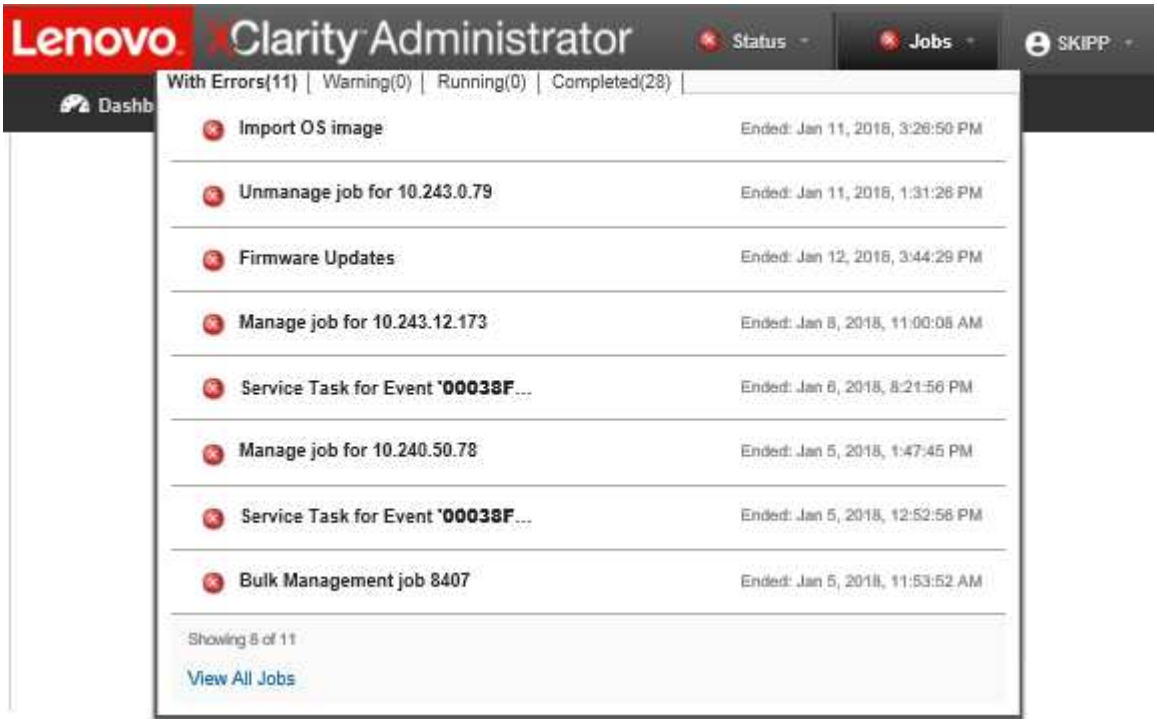
Step 10. Deploy the operating system by clicking **All actions → Deploy images**.

Step 11. From the confirmation page, click **Deploy** to deploy the image.

If the server currently has an operating system installed, you are warned about the fact that deploying the image will overwrite the current operating system.

Tip: You can set up a remote-control session to watch the installation as it progresses. Click **All actions → Remote Control** to start a remote-control session with the server.

When you deploy the operating system, Lenovo XClarity Administrator starts a job to track the deployment. To view the status of the deployment job, click **Jobs** from the Lenovo XClarity Administrator menu bar. Then, click the **Running** tab.

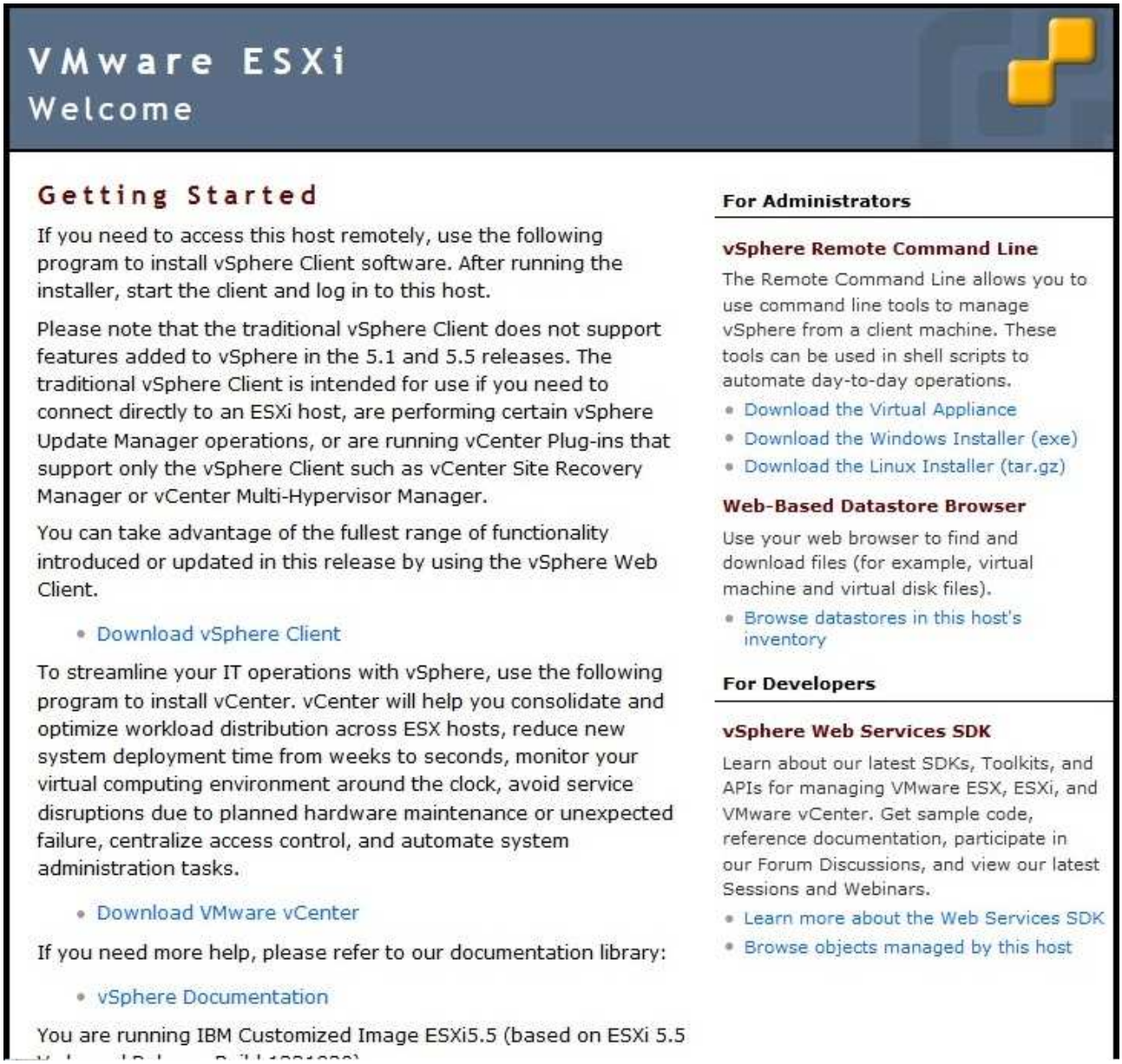


Hover over the running job to see the details, such as the percentage of the job that is complete.

Results

After the operating-system deployment has completed, log in to the IP address that you specified on the Edit Network Settings page to continue with the configuration process.

Note: The license provided with the image is a 60-day free trial. You are responsible for meeting all VMware licensing requirements.



Notices

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

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

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

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

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, SYSTEM, NEXTSCALE, SYSTEM X, THINKSERVER, THINKSYSTEM, and XCLARITY are trademarks of Lenovo.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, Windows Server, Windows PowerShell, Hyper-V, Internet Explorer, and Active Directory are registered trademarks of the Microsoft group of companies.

Mozilla and Firefox are registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Nutanix is a trademark and brand of Nutanix, Inc. in the United States, other countries, or both.

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.

SUSE is atrademark of SUSE IP Development Limited or its subsidiaries or affiliates.

VMware vSphere is a registered trademark of VMware in the United States, other countries, or both.

All other trademarks are the property of their respective owners.

Lenovo