Lenovo XClarity Administrator Planning and Installation Guide for Nutanix AHV Environments

Version 4.0.0

First Edition (February 2023)

© Copyright Lenovo 2017, 2023.
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

Contents i

Figures iii

Tables v

Summary of changes vii

Chapter 1. Lenovo XClarity Administrator Overview 1

Chapter 2. Planning for XClarity Administrator 7

Licenses and the free 90-day trial 7
Hardware and software prerequisites 8
Firewalls and proxy servers 10
Port availability 11
Management considerations 16
Network considerations. 16
IP configuration limitations 17
Network types 17
Network configurations 17
Security considerations 27
Encapsulation management 27
Cryptographic management 28
Security certificates 30
Authentication 30
User accounts and role groups 33
User-account security 33
High availability considerations 34
Features on Demand 35

Chapter 3. Installing Lenovo XClarity Administrator in a Nutanix AHV environment 37

Single data and management network (Nutanix AHV) 37
Step 1: Cable the rack servers and Lenovo XClarity Administrator host to the top-of-rack switches 38
Step 2: Configure top-of-rack switches 39
Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance 39
Physically separate data and management networks (Nutanix AHV) 43
Step 1: Cable the rack servers and Lenovo XClarity Administrator host to the top-of-rack switches 44
Step 2: Configure top-of-rack switches 45
Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance 45
Virtually separate data and management network topology (Nutanix AHV) 49
Step 1: Cable rack servers to the top-of-rack switches 51
Step 2: Configure top-of-rack switches 51
Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance 52

Chapter 4. Configuring Lenovo XClarity Administrator 57

Accessing the Lenovo XClarity Administrator web interface for the first time 57
Creating user accounts 60
Configuring network access 61
Configuring the date and time 67
Configuring service and support 69
Configuring security 71
Managing devices 72

Chapter 5. Registering XClarity Administrator 85

Chapter 6. Installing the full-function enablement license 87

Installing full-function enablement licenses using the XClarity Administrator web interface 88
Installing full-function enablement licenses using the Features on Demand web portal 92

Chapter 7. Updating XClarity Administrator 95

Chapter 8. Uninstalling XClarity Administrator 101

Notices ciii
Trademarks civ

© Copyright Lenovo 2017, 2023

Figures

1. Example implementation of a single network for management, data, and operating system deployment 21
2. Example implementation of physically separate data and management networks with the operating-system network as part of the data network. 22
3. Example implementation of physically separate data and management networks with the operating-system network as part of the management network 23
4. Example implementation of virtually separate data and management networks with the operating-system network as part of the data network. 24
5. Example implementation of virtually separate management and data networks with the operating-system network as part of the management network 25
6. Example implementation of a management-only network with no support for operating-system deployment 26
7. Example implementation of a management-only network with support for operating-system deployment 27
8. Sample single data and management network topology (Nutanix AHV) 38
9. Example cabling for a single data and management network 39
10. Sample Network topology - Physically separate data and management network (Nutanix AHV) 44
11. Example cabling for physically separate data and management networks (VMware ESXi) 45
12. Sample Network topology - Virtually separate data and management network (Nutanix AHV) 50
13. Example cabling for virtually separate data and management networks 51
14. Example configuration for Flex switches on virtually separate data and management networks (KVM) in which VLAN tagging is enabled on the management network 52

© Copyright Lenovo 2017, 2023

Tables

1. Role of each network interface based on network topology 19
2. Role of each network interface based on network topology 62

© Copyright Lenovo 2017, 2023

Summary of changes

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

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

For information about all supported hardware (including servers, chassis, and Flex switches), see Hardware and software prerequisites.

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

This version supports the following planning or installation enhancements to the management software.

Function	Description
Planning and installation	Removed ssh-rsa and added ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521 to the list of supported host key algorithms (see Cryptographic management).

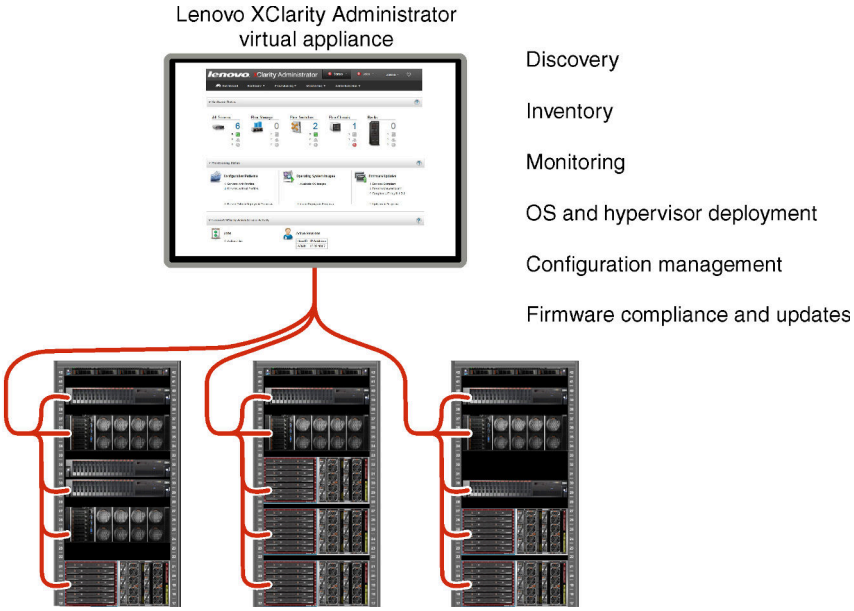
© Copyright Lenovo 2017, 2023

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 in the XClarity Administrator online documentation.

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 in the XClarity Administrator online documentation.

Learn more:

- XClarity Administrator: Discovery

© Copyright Lenovo 2017, 2023

- 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 in the XClarity Administrator online documentation.

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 the XClarity Administrator in the XClarity Administrator online documentation.

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 in the XClarity Administrator online documentation.

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 Deploying an operating system image in the XClarity Administrator online documentation.

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 in the XClarity Administrator online documentation.

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 in the XClarity Administrator online documentation.

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 role group in the XClarity Administrator online documentation.

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 in the XClarity Administrator online documentation.

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 in the XClarity Administrator online documentation .

- **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 in the XClarity Administrator online documentation.

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 in the XClarity Administrator online documentation.

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

For additional considerations, see Management considerations.

Learn more:

- Lenovo XClarity Integrator for Microsoft System Center overview
- 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**

Chapter 2. Planning for XClarity Administrator

Before installing Lenovo XClarity Administrator, review the following considerations to help you plan for installation and day-to-day management.

Licenses and the free 90-day trial

Lenovo XClarity Administrator offers a free, 90-day trial license that enables full use of all available features for a limited time.

You can determine the license status, including the number of days are left in the trial license, by clicking the user-actions menu (

) on the XClarity Administrator title bar, and then clicking **About**.

XClarity Administrator supports the following license.

- **Lenovo XClarity Pro**. Each license provides the following entitlements for a single device.
  - Service and support for Lenovo XClarity Integrator
  - Service and support for XClarity Administrator
  - Advanced functions within XClarity Administrator:
    - Configuring servers using Configuration Patterns
    - Deploying operating systems
    - Reporting XClarity Administrator problems using Call Home (Call Home for hardware alerts is not affected.)

You must purchase a license for each managed device that supports the advanced functions. A license is not tied to a specific device.

License compliance is determined based on the number of managed devices that support the advanced functions. The number of managed devices must not exceed the total number of licenses in all active license keys. If XClarity Administrator is not in compliance with the installed licenses (for example, if licenses expire or if managing additional devices exceeds the total number of active licenses), you have a grace period of 90 days to install appropriate licenses. Each time XClarity Administrator becomes non-compliant, the grace period resets to 90 days. If the grace period (including the free trial) ends before licenses are compliant, advanced functions are disabled for all devices.

Notes:

- Server configuration and operating-system deployment features are disabled when the grace period expires.
- Call Home for XClarity Administrator issues (software Call Home feature) is disabled when licenses are out of compliance. There is no grace period for this feature. However, Call Home for hardware alerts is not affected.

If licenses are already installed, new licenses are *not* required when upgrading to a new release of XClarity Administrator.

For information about purchasing Lenovo XClarity Pro licenses, contact your Lenovo representative or authorized business partner.

For information about installing the license, see Installing the full-function enablement license in the XClarity Administrator online documentation.

© Copyright Lenovo 2017, 2023

Hardware and software prerequisites

The Lenovo XClarity Administrator management appliance runs in a virtual machine on a host system.

Hypervisor requirements

Container environments

The following container environment are supported for running XClarity Administrator as a container.

- Docker v20.10.9
- Docker-compose v1.29.2

Hypervisors

The following hypervisors are supported for running XClarity Administrator as a virtual appliance.

- Citrix Hypervisor v8.2
- Citrix XenServer v7.6
- CentOS 7 and 8[1]
- Microsoft Windows Server 2022 with Hyper-V installed
- Microsoft Windows Server 2019 with Hyper-V installed
- Microsoft Windows Server 2016 with Hyper-V installed
- Microsoft Windows Server 2012 R2 with Hyper-V installed
- Microsoft Windows Server 2012 with Hyper-V installed
- Nutanix Acropolis Hypervisor (AHV)
- Red Hat Enterprise Linux v9.x with Kernel-based Virtual Machine (KVM) v6.2.0 installed
- RedHat Enterprise Linux v8.x with KVM v2.12.0 installed
- RedHat Enterprise Linux v7.x with KVM v1.2.17 installed
- Rocky Linux 8.x and 9.x with KVM v7.0.0 installed
- Ubuntu Server 22.04.x LTS with KVM v6.2.0 installed
- Ubuntu Server 20.04.2 LTS with KVM v4.2.3 installed
- VMware ESXi 8.0
- VMware ESXi 7.0, U1, U2, and U3
- VMware ESXi 6.7, U1, U2[2], and U3

Notes:

1. CentOS Linux is no longer updated by Red Hat. Consider migrating to Red Hat Enterprise Linux instead (see the Red Hat: How to convert from CentOS or Oracle Linux to RHEL webpage).
2. For VMware ESXi 6.7 U2, you must use the ISO image VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso or later).

For VMware and Citrix, the virtual machine is available as an OVF template. For Hyper-V and Nutanix AHV, the virtual machine is a virtual-disk image (VHD). For CentOS and KVM, the virtual machine is available as qcow2 format.

Important: For Hyper-V environments that run on Linux guests with a 2.6 kernel base and that use large amounts of memory for the virtual appliance, you must disable the use of non-uniform memory access (NUMA) on the Hyper-V Settings Panel from Hyper-V Manager. Changing this setting requires you to restart the Hyper-V service, which also restarts all running virtual machines. If this setting is not disabled, XClarity Administrator virtual appliance might experience problems during initial startup.

Hardware requirements

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 in the XClarity Administrator online documentation.

Software requirements

- **Orchestrator server**

  If you manage a large number of devices using multiple XClarity Administrator instances, you can centralize monitoring, management, provisioning, and analytics using Lenovo XClarity Orchestrator. XClarity Orchestrator can support an unlimited number of XClarity Administrator instances that collectively manage a maximum of **10,000** non-ThinkEdge-Client devices.

  To manage XClarity Administrator v4.0 or later instances using Lenovo XClarity Orchestrator, XClarity Orchestrator v2.0 or later is required.

- **Authentication server**

  If you choose to use an external authentication server, only Microsoft Active Directory running on Windows Server 2008 or later is supported.

  If you choose to use an SAML identify provider, only Microsoft Active Directory Federation Services (AD FS) versions 2.0 or later running on Windows Server 2012 is supported.

- **NTP server**

A Network Time Protocol (NTP) server is required to ensure that timestamps for all events and alerts that are received from managed devices are synchronized with XClarity Administrator. Ensure that the NTP server is accessible over the management network (typically the Eth0 interface).

Tip: Consider using the host system on which XClarity Administrator is installed as the NTP server. If you do, ensure that the host system is accessible over the management network.

Manageable resources

A single XClarity Administrator instance can manage, monitor, and provision a maximum of **1,000** physical devices.

You can find a complete list of supported devices and options (such as I/O, DIMM, and storage adapters), minimum required firmware levels, and limitations considerations from the following Lenovo XClarity Support webpages.

- ThinkAgile, ThinkEdge, ThinkSystem, System x, Converged HX, and NeXtScale rack and tower servers
- Flex System devices and ThinkSystem compute nodes
- ThinkServer rack and tower servers
- RackSwitch devices
- Storage devices

For general information about hardware configuration and options for a specific device, see the Lenovo Server Proven webpage.

Restriction: If the host system on which XClarity Administrator is installed is a managed rack server or compute node, you cannot use XClarity Administrator to apply firmware updates to that host system or to the entire chassis at one time. When firmware updates are applied to the host system, the host system must be restarted. Restarting the host system also restarts XClarity Administrator, making XClarity Administrator unavailable to complete the updates on the host system.

Supported web browsers

The XClarity Administrator web interface works with the following 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)

Firewalls and proxy servers

Some functions of Lenovo XClarity Administrator, including management server updates, firmware updates, service and support, require access to the Internet. If you have firewalls in your network, configure the firewalls to enable XClarity Administrator management server to perform these operations. If the management server does not have direct access to the Internet, configure XClarity Administrator to use a proxy server.

Firewalls

Ensure that the following DNS names and ports are open on the firewall. Each DNS represents a geographically distributed system with a dynamic IP address.

DNS name	Ports	Protocols
Download license activation keys		
fod.lenovo.com	443	https

DNS name	Ports	Protocols
Retrieve service bulletins		
download.lenovo.com/servers/LXCA_Bulletin_Service.json	443	https
Download updates (management-server updates, firmware updates, UpdateXpress System Packs (OS device drivers), and repository packs)		
download.lenovo.com	443	https
support.lenovo.com	443 and 80	https and http
Send service data to Lenovo Support (Call Home)		
soaus.lenovo.com	443	https
logupload.lenovo.com/BLL/Logupload.ashx	443 and 80	https
Send service data to the Lenovo Update Facility		
logupload.lenovo.com/BLL/Logupload.ashx	443 and 80	https
Retrieve warranty information		
csapi.lenovo.com.cn (China only)	443	https
supportapi.lenovo.com (worldwide)	443 and 80	https and http

Proxy server

If the management server does not have direct access to the Internet, ensure that the management server is configured to use an HTTP proxy server (see “Configuring network access” on page 61).

- 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.

Port availability

Several ports must be available, depending on how the firewalls are implemented in your environment. If the required ports are blocked or used by another process, some Lenovo XClarity Administrator functions might not work.

To determine which ports must be opened based on your environment, review the following sections. The tables in these sections include information about how each port is used in XClarity Administrator, the managed device that is affected, the protocol (TCP or UDP), and the direction of traffic flow. *Inbound* traffic identifies flows from the managed device or external systems to XClarity Administrator, so ports need to open on the XClarity Administrator appliance. *Outbound* traffic flows from XClarity Administrator to the managed device.

- Access to the XClarity Administrator server
- Access between XClarity Administrator and managed devices
- Access between XClarity Administrator and data network for OS deployment and device-driver updates

Access to the XClarity Administrator server

If the XClarity Administrator server and all managed devices are behind a firewall, and you intend to access those devices from a browser that is outside of the firewall, you must ensure that the XClarity Administrator ports are open. If you are using SNMP and SMTP for event management, you might also need to ensure that the ports that are used by the XClarity Administrator server for event forwarding are open.

The XClarity Administrator server listens on and responds through the ports that are listed in the following table.

Notes:

- XClarity Administrator is a RESTful application that communicates securely over TCP on port 443.
- XClarity Administrator can be optionally configured to make outbound connections to external services, such as LDAP, SMTP, or syslog. These connections might require additional ports that are generally user configurable and not included in this list. These connections might also require access to a domain name service (DNS) server on TCP or UDP port 53 to resolve external server names.

Service	Outbound (ports open on external systems)	Inbound (ports open on XClarity Administrator appliance)
XClarity Administrator appliance	• DNS – TCP/UDP on port **53**	• HTTPS – TCP on port **443**
External authentication servers	• LDAP– TCP on port **389**[1] • LDAPS – TCP on port **636** • SAML authentication – TCP on ports **3268, 3269**	Not applicable
Event forwarding services	• FTP server – TCP on port **21**[1] • Email server (SMTP) – UDP on port **25**[1] • REST Web Service (HTTP) – TCP on port **80**[1] • SNMP manager – UDP on port **161**[2], **162**[1] • MS Azure – UDP on port **443**[1] • Syslog – UDP on port **514**[1] • Apple push[3] – TCP on ports **443, 2195, 5223** • Google push[4] – TCP on ports **443, 5288, 5299, 5230**	• SNMP – UDP on port **161**
Lenovo services (including Call Home)	• Warranty (China only) – TCP on port **83**[5] • HTTPS (Call Home) – TCP on port **443**	Not applicable

1. This is the default port. You can configure this port from the user interface.
2. This port is used when SNMP event forwarding with user authentication is configured.
3. Open this port when Wi-Fi is behind a firewall or private Access Point Name (APN) for cellular data. A direct, unproxied connection is required to the APN servers on this port. This port is used as a failback on Wi-Fi only, when devices cannot reach the Apple Push Notifications service on port 5223. The IP address range is 17.0.0.0/8.
4. For the IP address range, see Google ASN 15169. The domain is android.googleapis.com.
5. Though not required outside of China, XClarity Administrator might attempt to connect to this service in other countries.

Access between XClarity Administrator and managed devices

If managed devices (such as compute nodes or rack servers) are behind a firewall and if you intend to manage those devices from a XClarity Administrator server that is outside of that firewall, you must ensure that all ports involved with communications between XClarity Administrator and the baseboard management controller in each managed device are open.

If you intend to install operating systems on managed devices using XClarity Administrator, ensure that you review the list of ports in Access between XClarity Administrator and data network for OS deployment and device-driver updates.

- **Flex chassis CMM**

Device type	Outbound (ports open on external systems)	Inbound (ports open on XClarity Administrator appliance)
Flex Chassis CMMs	– SLP – UDP/TCP on port **427** – CIM HTTP – TCP on port **5988**[2] – CIM HTTPS – TCP on port **5989** – TCP command – TCP on port **6090**[2] – Secure TCP command – TCP on port **6091**	– SFTP – TCP on port **22**[1] – CIM indications HTTPS – TCP **9090** – LDAPS – TCP on ports **50637**

1. This port is used to transfer firmware-updates using SFTP.
2. By default, management is performed over secure ports. The non-secure ports are optional.

- **Servers and compute nodes**

Device type	Outbound (ports open on external systems)	Inbound (ports open on XClarity Administrator appliance)
ThinkSystem and ThinkAgile	– SSDP discovery – UDP on port **1900** – SFTP – TCP on port **115**[4] – HTTPS – TCP on port **443** – Remote control – TCP on port **3888**[3] – CIM HTTPS – TCP on port **5989**[8] – Firmware updates - TCP on port **6990**[4, 7] – SLP – UDP/TCP on port **427**[6]	– SFTP – TCP on port **22**[1] – HTTPS – TCP on port **443** – Firmware updates - TCP on port **6990**[4] – CIM indications HTTPS – TCP **9090** – LDAPS – TCP on ports **50636**[5] – LDAPS – TCP on ports **50637**[9]
System x	– SLP – UDP/TCP on port **427** – HTTPS – TCP on port **443** – IPMI – TCP on port **623** – Remote control – TCP on port **3888**[3] – CIM HTTP – TCP on port **5988**[2] – CIM HTTPS – TCP on port **5989**[2] – Firmware updates - TCP on port **6990**[4, 7]	– SFTP – TCP on port **22**[1] – HTTPS – TCP on port **443** – Firmware updates - TCP on port **6990**[4] – CIM indications HTTPS – TCP **9090**[8] – LDAPS – TCP on ports **50636**[5] – LDAPS – TCP on ports **50637**[9]

Device type	Outbound (ports open on external systems)	Inbound (ports open on XClarity Administrator appliance)
Flex System	– SLP – UDP/TCP on port **427** – Remote control – TCP on port **3888**[3] – CIM HTTP – TCP on port **5988**[2] – CIM HTTPS – TCP on port **5989**[2] – Firmware updates - TCP on port **6990**[4, 7]	– SFTP – TCP on port **22**[1] – HTTPS – TCP on port **443** – Firmware updates - TCP on port **6990**[4] – CIM indications HTTPS – TCP **9090** – LDAPS – TCP on ports **50636**[5] – LDAPS – TCP on ports **50637**[9]
ThinkServer	– SNMP traps – UDP on port **162** – IPMI – UDP on port **623**	– SNMP traps – UDP on port **162**

1. This port is used to transfer firmware-updates using SFTP, to download service data files, and to store drive erase tool that is fetched by the BMU OS when securely erasing drive data.
2. By default, management is performed over secure ports. The non-secure ports are optional.
3. Remote control and remote KVM is launched from the web browser, not the XClarity Administrator server.
4. This port is required to for BMU firmware updates to upload firmware update package to the management controller.
5. This port is required to configure servers using configuration patterns.
6. This port is required only for ThinkSystem SR635 and SR655 servers.
7. This port is required to mount the BMU image when securely erasing drive data.
8. This port is required for only ThinkSystem V1 servers.
9. This port is required to use managed authentication.

- **Rack and Flex switches**

Device type	Outbound (ports open on external systems)	Inbound (ports open on XClarity Administrator appliance)
Rack switches	– SSH – TCP on port **22**[1,3] – SNMP - UDP on port **161**[2] – SLP – UDP/TCP on port **427**[6] – HTTPS – TCP on port **443**[7]	– SFTP – TCP on port **22**[4] – SNMP traps – TCP on ports **162**[2]
Flex switches	– SSH – TCP on port **22**[3] – SNMP - UDP on port **161**[5]	– SFTP – TCP on port **22**[4] – SNMP traps- TCP on port **162**[2]

1. For ENOS rack switches, this port is used to configure Head of Stack (HoS) credentials used between CMM and Flex switches, activate the firmware slot, and clear SSH host keys before SFTP file transfer operations.
2. This port must be open on the XClarity Administrator appliance (inbound) when switches are on a different network than XClarity Administrator, so that XClarity Administrator can receive events for those devices.
3. This port is used for management (SSH).
4. This port is used to transfer firmware-updates using SFTP.

5. For ENOS rack switches, this port is used to transfer inventory data.
6. This port is used for discovery.
7. This port is used to apply firmware updates.

- **Storage devices**

Device type	Outbound (ports open on external systems)	Inbound (ports open on XClarity Administrator appliance)
Storage devices	– FTP – TCP on port **21** – SFTP- TCP on port **22**[2] – SLP – UDP/TCP on port **427** – HTTPS – TCP on port **443**[1] – HTTPS – TCP on port **3031**[3]	– HTTPS – TCP on port **443**[2] – SNMP traps- UDP on port **115**

1. This port is used to transfer firmware-updates.
2. This port is used to transfer and apply firmware-updates.
3. This port is used for discovery of Tape Library Storage devices.

Access between XClarity Administrator and data network for OS deployment and device-driver updates

Device type	Outbound (ports open on external systems)	Inbound (ports open on XClarity Administrator appliance)
OS deployment[1, 2, 3]		• SMB communication – TCP on port **445**[4] • HTTPS (Except ThinkServer) – TCP on port **8443**[6]
OS device driver updates[2]	• WinRM over HTTP – TCP on port **5985**[5] • WinRM over HTTPS – TCP on port **5986**[6]	• SMB communication – TCP on port **445**[4]

1. If you configured XClarity Administrator to use an operating-system deployment network, ports must be open on that network.
2. For a list of ports that must be available for the deploying operating systems, see Port availability for deployed operating systems in the XClarity Administrator online documentation. For example, if operating-system deployment is configured to use the data network (eth1), then these ports must be open on that network.
3. Each XClarity Administrator instance has a unique Certificate Authority (CA) that is used for only OS deployment. That CA signs a certificate that is used for the target server on port 8443. When OS deployment is initiated, the CA certificate is included in the OS image that is pushed to the target server. As part of the deployment process, that server connects back to port 8443, and verifies the certificate that port 8443 provide during the handshake because they have the CA certificate.
4. This port is used to transfer Windows driver files.
5. This port is used to connect to the target server WinRM.
6. This port is used to exchange data between the target OS and XClarity Administrator, including OS images and status.

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.

Network considerations

When planning the Lenovo XClarity Administrator installation, consider the network topology that is implemented in your environment and how XClarity Administrator fits into that topology.

Important: Configure the devices and components in ways that minimize IP address changes. Consider using static IP addresses instead of Dynamic Host Configuration Protocol (DHCP). If DHCP is used, ensure that IP address changes are minimized.

IP configuration limitations

For the following functions and managed devices, network interfaces must be configured with an IPv4 address. IPv6 addresses are not supported.
- Firmware updates for Lenovo Storage devices
- ThinkServer servers
- Lenovo Storage devices

Managing RackSwitch devices using IPv6 link local through a data port or management port is not supported.

Network address translation (NAT), which remaps one IP address space into another, is not supported.

Network types

In general, most environments implement the following types of networks. Based on your requirements, you might implement only one of these networks or you might implement all three.

- **Management network**

  The management network is typically reserved for communications between Lenovo XClarity Administrator and the management processors for managed devices. For example, the management network might be configured to include XClarity Administrator, the CMMs for each managed chassis, and the baseboard management controller of each server that XClarity Administrator manages.
- **Data network**

  The data network is typically used for communications between the operating systems that are installed on the servers and the company intranet, the Internet, or both.
- **Operating-system deployment network**

  In some cases, an operating-system deployment network is set up to separate out the communications that are required to deploy operating systems on servers. If implemented, this network typically includes XClarity Administrator and all server hosts.

  Instead of implementing a separate operating-system deployment network, you might choose to combine this functionality in either the management network or the data network.

Network configurations

You can configure Lenovo XClarity Administrator to use one or two network interfaces.

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.

  Note: When enabled, XClarity Administrator runs an ARP scan to find active IPv4 devices on the same subnet. To prevent the ARP scan, disable **Duplicate IP address checking**.
- 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, ensure that a macvlan network is set up on the host system..

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, at least one of the network interfaces 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 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, at least one of the network interfaces 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 OS 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.

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 1. 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 • None
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 • OS deployment • OS device-driver updates

Table 1. Role of each network interface based on network topology (continued)

Network topology	Role of interface 1 (eth0)	Role of interface 2 (eth1)
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 • None
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

Single data and management network

In this network topology, management communications, data communications, and operating-system deployment occur over the same network. This topology is referred to as a *converged* network.

Important: Implementing a shared data and management network can cause disruptions in traffic, such as packets being dropped or management-network connectivity issues, depending on your network configuration (for example, if traffic from servers have a high priority and traffic from the management controllers have a low priority). The management network uses UDP traffic in addition TCP. UDP traffic can have a lower priority when the network traffic is high.

When you install Lenovo XClarity Administrator, define the eth0 network interface using the following considerations:

- 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, at least one of the network interfaces 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 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.
- You can set up XClarity Administrator on any system that meets the requirements for XClarity Administrator, including a managed server only when you implement either a single data and management

network topology or a virtually separate data and management network topology; however, you cannot use XClarity Administrator to apply firmware updates to that managed server. Even then, only some of the firmware is applied with immediate activation, and XClarity Administrator forces the target server to restart, which would restart XClarity Administrator as well. When applied with deferred activation, only some firmware is applied when XClarity Administrator host is restarted.

You can also configure a second network interface to connect to the same network from XClarity Administrator to support redundancy.

The following figure shows an example implementation for a converged network topology.

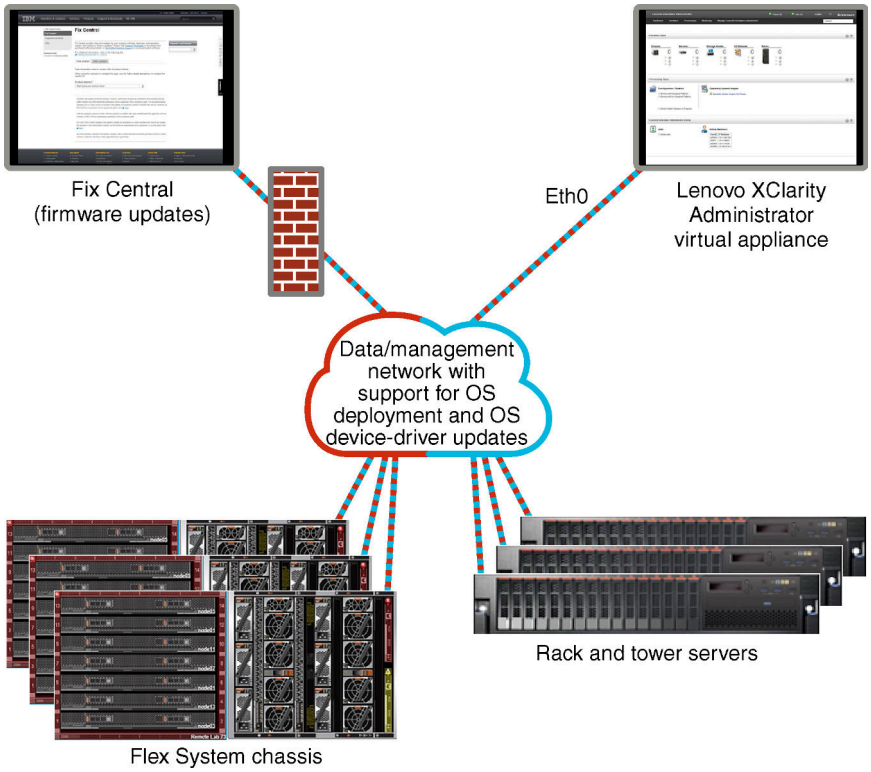


Figure 1. Example implementation of a single network for management, data, and operating system deployment

Physically separate data and management network

In this network topology, the management network and the data network are physically separate networks, and the operating-system deployment network is configured as part of either the management network or the data network.

When you install Lenovo XClarity Administrator, define network settings using the following considerations:

- 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, at least one of the network interfaces 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 OS 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.

Figure 2 “Example implementation of physically separate data and management networks with the operating-system network as part of the data network” on page 22 shows an example implementation of separate management and data networks in which the operating-system deployment network is configured as part of the data network.

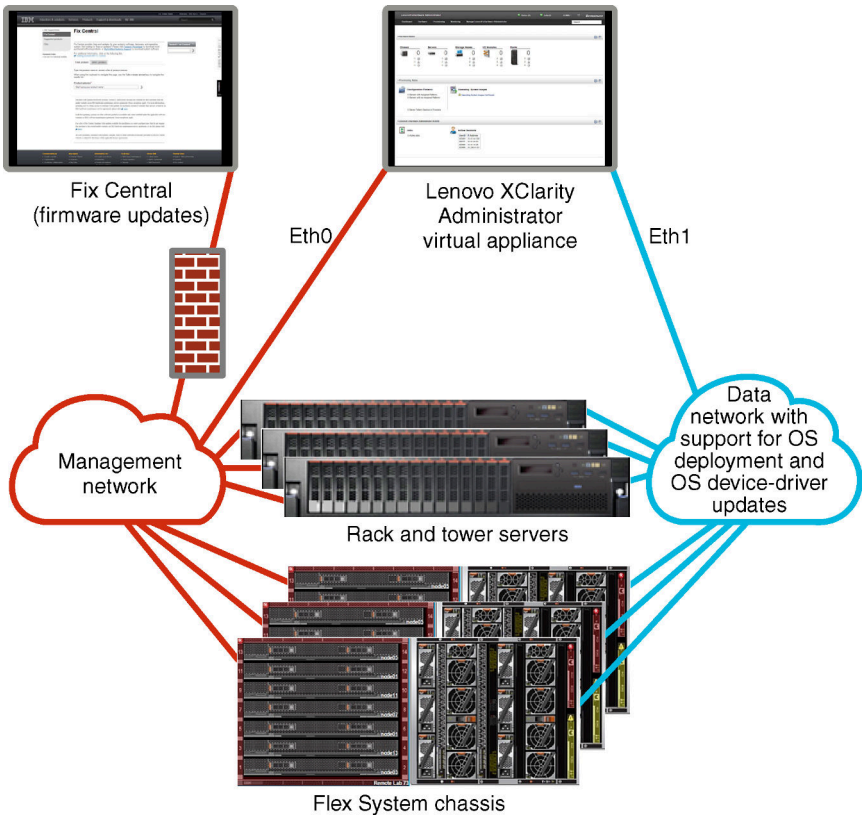


Figure 2. Example implementation of physically separate data and management networks with the operating-system network as part of the data network

Figure 3 “Example implementation of physically separate data and management networks with the operating-system network as part of the management network” on page 23 shows another example implementation of separate management and data networks in which the operating-system deployment network is configured as part of the management network. In this implementation, XClarity Administrator does not need connectivity to the data network.

Note: If the operating-system deployment network does not have access to the data network, configure an additional interface on the servers to provide connectivity from the host operating system on the server to the data network, if needed.

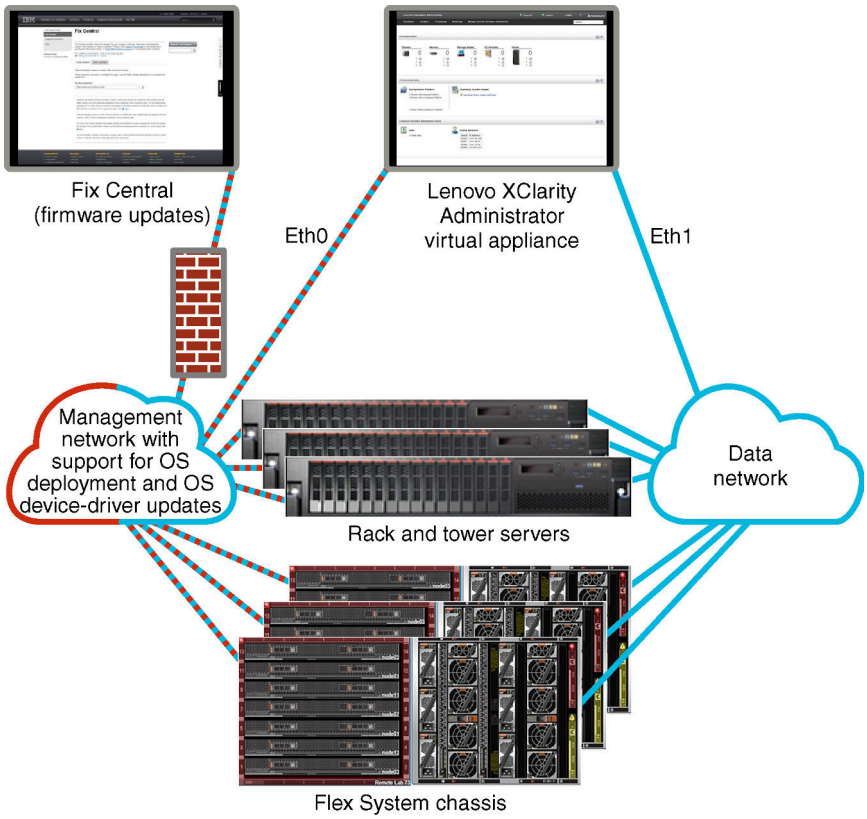


Figure 3. Example implementation of physically separate data and management networks with the operating-system network as part of the management network

Virtually separate data and management network

In this topology, the data network and management network are virtually separate. Packets from the data network and packets from the management network are sent over the same physical connection. VLAN tagging is used on all management-network data packets to keep the traffic between the two networks separated.

Note: If Lenovo XClarity Administrator is installed on a host running on a managed server in a chassis, you cannot use XClarity Administrator to apply firmware updates to that entire chassis at one time. When firmware updates are applied, the host system must be restarted.

When you install XClarity Administrator, define network settings using the following considerations:

- 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, at least one of the network interfaces 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 OS 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.
- You can set up XClarity Administrator on any system that meets the requirements for XClarity Administrator, including a managed server only when you implement either a single data and management network topology or a virtually separate data and management network topology; however, you cannot use XClarity Administrator to apply firmware updates to that managed server. Even then, only some of the firmware is applied with immediate activation, and XClarity Administrator forces the target server to restart, which would restart XClarity Administrator as well. When applied with deferred activation, only some firmware is applied when XClarity Administrator host is restarted.

Figure 4 “Example implementation of virtually separate data and management networks with the operating-system network as part of the data network” on page 24 shows an example implementation of virtually separate management and data networks in which the operating-system deployment network is configured as part of the data network. In this example, XClarity Administrator is installed on a managed server in a chassis.

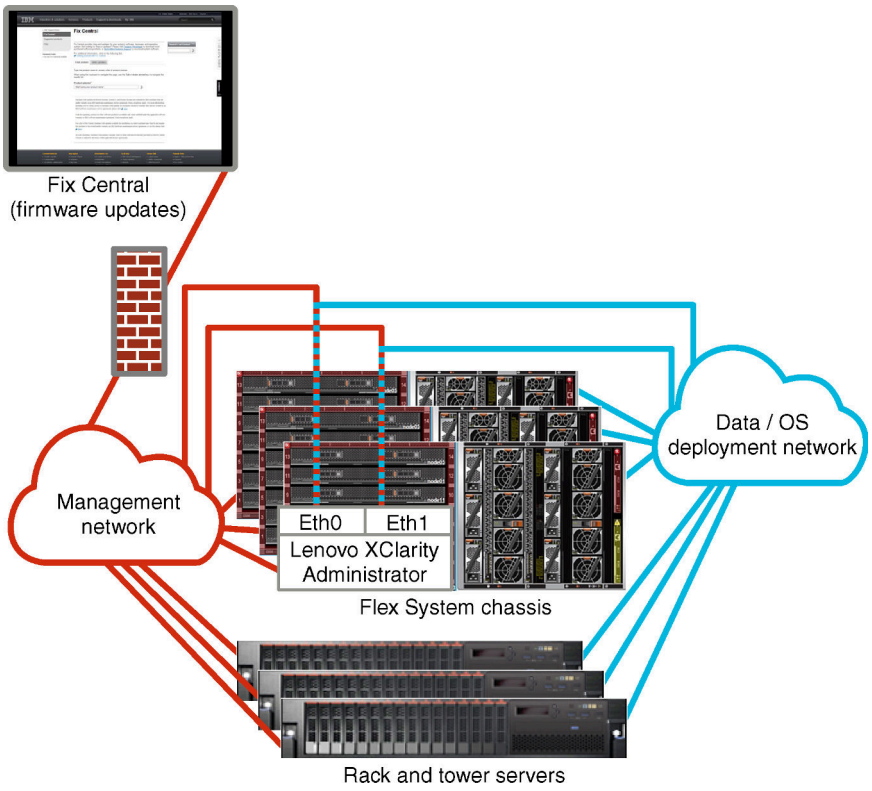


Figure 4. Example implementation of virtually separate data and management networks with the operating-system network as part of the data network

Figure 5 “Example implementation of virtually separate management and data networks with the operating-system network as part of the management network” on page 25 shows an example implementation of virtually separate management and data networks in which the operating-system deployment network is configured as part of the management network, and XClarity Administrator is installed on a managed server in a chassis. In this implementation, XClarity Administrator does not need connectivity to the data network.

Note: If the operating-system deployment network does not have access to the data network, configure an additional interface on the servers to provide connectivity from the host operating system on the server to the data network, if needed.

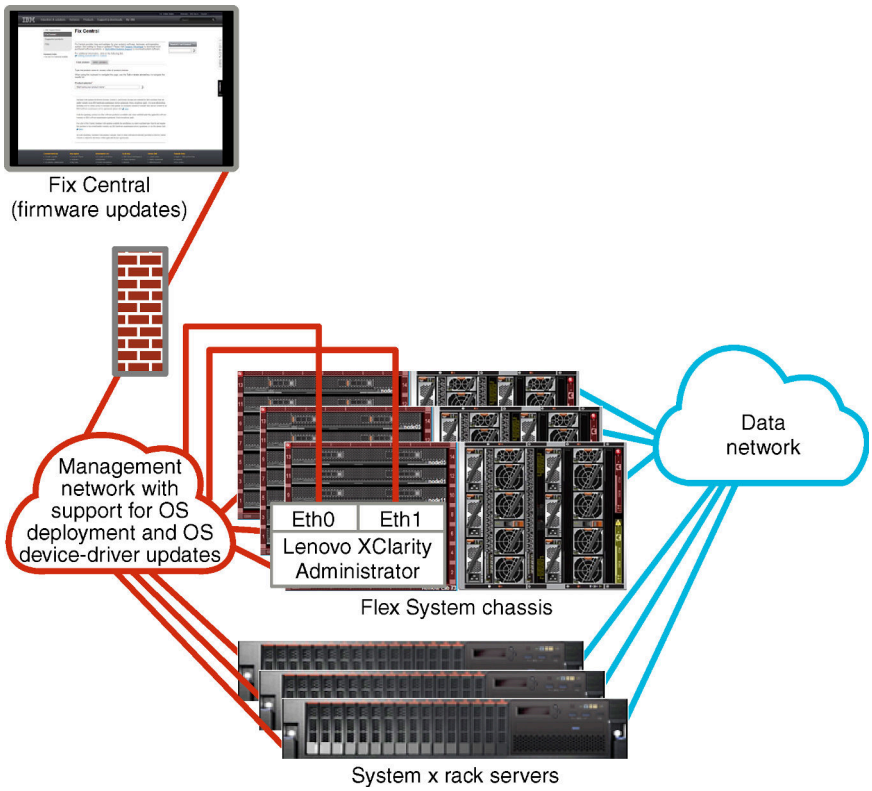


Figure 5. Example implementation of virtually separate management and data networks with the operating-system network as part of the management network

Management-only network

In this topology, Lenovo XClarity Administrator has access to only the management network. It does not have access to the data network. However, XClarity Administrator must have access to the operating-system deployment network if you intend to deploy operating-system images from XClarity Administrator to managed servers.

When you install XClarity Administrator and define network settings, the eth0 network interface must be configured to:

- 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, at least one of the network interfaces 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 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.

You can also configure a second network interface to connect to the same network from XClarity Administrator to support redundancy.

Figure 6 “Example implementation of a management-only network with no support for operating-system deployment” on page 26 shows an example implementation for a management-only network in which operating-system deployment from XClarity Administrator is not supported.

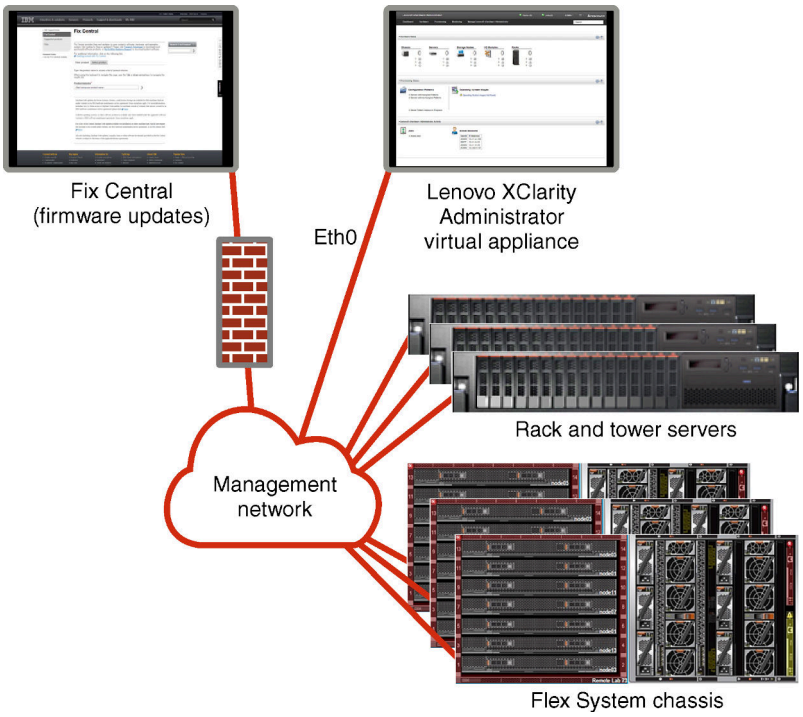


Figure 6. Example implementation of a management-only network with no support for operating-system deployment

Figure 6 “Example implementation of a management-only network with no support for operating-system deployment” on page 26 shows an example implementation for a management-only network in which operating-system deployment from XClarity Administrator is supported.

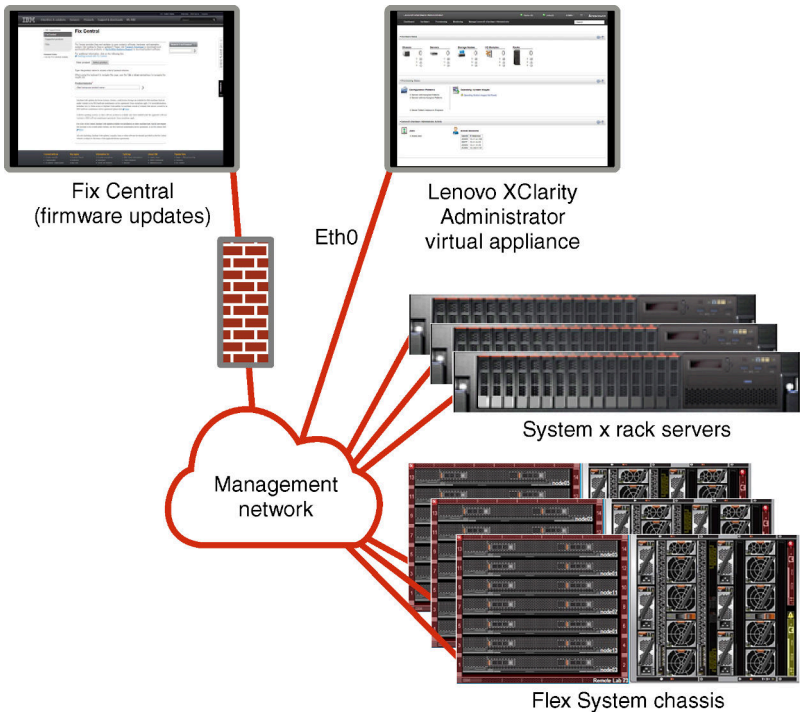


Figure 7. Example implementation of a management-only network with support for operating-system deployment

Security considerations

Plan for the security of Lenovo XClarity Administrator and all managed devices.

Encapsulation management

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.

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 Recovering chassis management with a CMM after a management server failure and Recovering rack or tower server management after a management server failure in the XClarity Administrator online documentation.

Notes:

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

For more information about encapsulation, see Enabling encapsulation in the XClarity Administrator online documentation.

Cryptographic management

Cryptographic management is composed of communication modes and protocols that control the way that secure communication is handled between Lenovo XClarity Administrator and the managed devices (such as chassis, servers, and Flex switches).

Cryptography algorithms

XClarity Administrator supports TLS 1.2 and stronger cryptographic algorithms for secure network connections.

For increased security, only high-strength ciphers are supported. The client operating systems and web browsers must support one of the following cipher suites.

- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

Cryptographic modes for the management server

This setting determines the mode to use for secure communications from the management server.

- **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 in the XClarity Administrator online documentation). 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 800-131A compliance in the XClarity Administrator online documentation.

For more information about setting the security modes on the management server, see Setting the cryptography mode and communication protocols in the XClarity Administrator online documentation.

Security modes for the managed servers

This setting determines the mode to use for secure communications from the managed servers.

- **Compatibility Security**. Select this mode when services and clients require cryptography that is not CNSA/FIPS compliant. This mode supports a wide range of cryptography algorithms and allows all services to be enabled.
- **NIST SP 800-131A**. Select this mode to ensure compliance with the NIST SP 800-131A standard. This includes restricting RSA keys to 2048 bits or greater, restricting hashes used for digital signatures to SHA-256 or longer, and ensuring only NIST-approved symmetric encryptions algorithms are used. This mode requires setting SSL/TLS mode to **TLS 1.2 Server Client**.

  This mode *is not* supported for servers with XCC2.
- **Standard Security**. (Servers with XCC2 only) This is the default security mode for servers with XCC2. Select this mode to ensure compliance with the FIPS 140-3 standard. For XCC to operate in FIPS 140-3 validated mode, only services that support FIPS 140-3 level cryptography can be enabled. Services that do not support FIPS 140-2/140-3 level cryptography are disabled by default but can be enabled if required. If any service that uses non FIPS 140-3 level cryptography is enabled, the XCC cannot operate in FIPS 140-3 validated mode. This mode requires FIPs-level certificates.
- **Enterprise Strict Security**. (servers with XCC2 only) This is the most secure mode. Select this mode to ensure compliance with the CNSA standard. Only services that support CNSA level cryptography are allowed. Nonsecure services are disabled by default and cannot be enabled. This mode requires CNSA-level certificates.

  XClarity Administrator uses RSA-3072/SHA-384 certificate signatures for servers in **Enterprise Strict Security** mode.

  Important:

  - The XCC2 Feature On Demand key must be installed on each selected servers with XCC2 to use this mode.
  - In this mode, if XClarity Administrator uses self-signed certificate, XClarity Administrator must use RSA3072/SHA384 based root certificate and server certificate. If XClarity Administrator uses an external signed certificate, XClarity Administrator must generate an RSA3072/SHA384 based CSR and contact the external CA to sign a new server certificate based on RSA3072/SHA384.
  - When XClarity Administrator uses an RSA3072/SHA384 based certificate, XClarity Administrator might disconnect devices other than Flex System chassis (CMMS) and servers, ThinkSystem servers, ThinkServer servers, System x M4 and M5 servers, Lenovo ThinkSystem DB series switches, Lenovo RackSwitch, Flex System switches, Mellanox switches, ThinkSystem DE/DM storage devices, IBM tape library storage, and ThinkSystem SR635/SR655 servers flashed with firmware earlier than 22C. To continue managing the disconnected devices, set up another XClarity Administrator instance with an RSA2048/SHA384 based certificate.

Consider the following implications of changing the cryptographic mode.

- Changing from **Compatibility Security** mode or **Standard Security** mode to **Enterprise Strict Security** mode is not supported.
- If you upgrade from **Compatibility Security** mode to **Standard Security** mode, you are warned if imported certificates or SSH public keys are not compliant, but you are still able to upgrade to **Standard Security** mode.
- If you downgrade from **Enterprise Strict Security** mode to **Compatibility Security** mode or **Standard Security** mode:
  - The server is automatically restarted for the security mode to take effect.
  - If the strict mode FoD key is missing or expired on the XCC2, and if XCC2 uses a self-signed TLS certificate, XCC2 regenerates the self-signed TLS certificate based on the Standard Strict compliant

algorithm. XClarity Administrator shows a connection failure due to a certificate error. To resolve the untrusted certificate error, see Resolving an untrusted server certificate in the XClarity Administrator online documentation. If XCC2 uses a custom TLS certificate, XCC2 allows the downgrade, and warns you that you need to import a server certificate that is based on **Standard Security** mode cryptography

- **NIST SP 800-131A** mode is not supported for servers with XCC2.
- You cannot use *managed authentication* to manage a ThinkSystem or ThinkAgile server when the XCC's security mode set to **TLS v1.3**.
- For a ThinkSystem or ThinkAgile server that is managed using *managed authentication*, changing the XCC's security mode to **TLS v1.3** using either XClarity Administrator or XCC will cause the server to go offline.

You can change the security settings for the following devices.
- Lenovo ThinkSystem servers with Intel or AMD processors (except SR635 / SR655)
- Lenovo ThinkSystem V2 servers
- Lenovo ThinkSystem V3 servers with Intel or AMD processors
- Lenovo ThinkEdge SE350 / SE450 servers
- Lenovo System x servers

For more information about setting the security modes on the managed server, see Configuring the security settings for a server in the XClarity Administrator online documentation.

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.

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.

For more information about certificates, see Working with security certificates in the XClarity Administrator online documentation.

Authentication

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.

For more information about authentication servers, see Managing the authentication server in the XClarity Administrator online documentation.

Device 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).

  Note: 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.

  Note: For Think Edge SE450, SE350 V2, and SE360 V2 servers, the default local user account remains enabled and all other local 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. 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 in the XClarity Administrator online documentation).

  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.

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

For information about recovering a device management, see Recovering chassis management with a CMM after a management server failure and Recovering rack or tower server management after a management server failure in the XClarity Administrator online documentation.

User accounts and role groups

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

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.

For more information about the user accounts and role groups, see Managing user accounts in the XClarity Administrator online documentation.

User-account security

User-account settings control the password complexity, account lockout, and web-session inactivity time-out. You can change the values of the account-security settings.

For more information about the account-security settings, see Changing the user-account security settings in the Lenovo XClarity Administrator online documentation.

High availability considerations

To set up high availability for Lenovo XClarity Administrator, use the high availability features that are part of the host operating system or container environment.

Docker

You can use Docker Datacenter to set up a high-availability environment for XClarity Administrator containers running in Docker Engine. For more information about Docker Datacenter high availability, see High Availability Architecture and Apps with Docker Datacenter webpage.

Citrix

Use the high-availability function that is provided for the Citrix environment. For more information, see Implementing high availability (Citrix) in the XClarity Administrator online documentation..

KVM (CentOS, RedHat, Rocky and Ubuntu)

You can use OpenStack, or if you already have a high-availability environment, continue to use your internal processes. For more information about OpenStack high availability, see Implementing high availability (KVM) in the XClarity Administrator online documentation..

Microsoft Hyper-V

Use the high-availability function that is provided for the ESXi environment. For information, see Implementing high availability (Microsoft Hyper-V) in the XClarity Administrator online documentation..

Nutanix AHV

use the Virtual Machine High Availability function that is provided for the Nutanix AHV environment. For more information, see Implementing high availability (Nutanix) in the XClarity Administrator online documentation..

VMware ESXi

In a VMware high-availability environment, multiple hosts are configured as a cluster. Shared storage is used to make the disk image of a virtual machine (VM) available to the hosts in the cluster. The VM runs on only one host at a time. When there is an issue with the VM, another instance of that VM is started on a backup host.

VMware high availability requires the following components:

- A minimum of two hosts on which ESXi is installed. These hosts become part of the VMware cluster.
- A third host on which VMware vCenter is installed.

  Tip: Ensure that you install a version of VMware vCenter that is compatible with the versions of ESXi that are installed on the hosts to be used in the cluster.

  VMware vCenter can be installed on one of the hosts that is used in the cluster. However, if that host is powered off or not usable, you lose access to the VMware vCenter interface as well.
- Shared storage (datastores) that can be accessed by all hosts in the cluster. You can use any type of shared storage that VMware supports. The datastore is used by VMware to determine if a VM should fail over to a different host (heartbeating).

For details about setting up a VMware high availability cluster, see Implementing high availability (VMware ESXi) in the XClarity Administrator online documentation..

Features on Demand

Features on Demand activates features without requiring the installation of hardware or the purchase of new equipment. This activation is done by acquiring and installing the corresponding Features on Demand key.

To use the remote-control and operating-system deployment operations in Lenovo XClarity Administrator, you must enable XClarity Controller Enterprise level or MM Advanced Upgrade for servers that do not come with these features already activated by default. These operations also require that a Features on Demand key for remote presence is installed on ThinkSystem, Converged, and System x 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 in the XClarity Administrator online documentation).

Some advanced server functions are activated using Features on Demand keys. If features have configurable settings that are exposed during UEFI setup, you can configure the setting using Configuration Patterns; however, the resulting configuration is not activated until the corresponding Features on Demand key is installed.

Note: You cannot install or managed Features on Demand keys from XClarity Administrator; however, you can view the list of Features on Demand keys that are currently installed on managed servers. For more information about viewing installed Features on Demand keys, see Viewing Feature on Demand keys in theXClarity Administrator online documentation.

To acquire and install Features on Demand keys:

1. Purchase the Features on Demand upgrade using the appropriate part number.

   You can purchase keys from the Features on Demand web portal. When your purchase is complete, you will receive an authorization code by e-mail.
2. On the Features on Demand web portal, enter the authorization code that you received, along with the unique system identifier of the server that you intend to upgrade.
3. Download the activation key in the form of a .KEY file.
4. Upload the activation key to the management controller for the server.
5. Restart the server. When the restart is complete, the feature is activated.

For more information about Features on Demand keys, see Using Lenovo Features on Demand.

Chapter 3. Installing Lenovo XClarity Administrator in a Nutanix AHV environment

There are a number of different ways to connect manageable devices to the network and to set up the Lenovo XClarity Administrator virtual appliance to manage those devices. Use the information in this section as a guide to setting up manageable devices and installing the XClarity Administrator virtual appliance in a Nutanix Acropolis Hypervisor (AHV) based environment.

This section describes how to set up several common topologies. This section does not cover every possible network topology.

Attention: To manage devices, XClarity Administrator must have access to the management network.

Single data and management network (Nutanix AHV)

In this topology, both the data network and management network are the same network. All communications between Lenovo XClarity Administrator and the network occurs over the Eth0 network interface on the host. The XClarity Administrator Eth1 network interface is not enabled.

Before you begin

Ensure that all appropriate ports are enabled, including ports that XClarity Administrator requires (see Port availability).

Ensure that the minimum required firmware is installed on each device that you intend to manage using XClarity Administrator. You can find minimum required firmware levels from the XClarity Administrator Support – Compatibility webpage by clicking the **Compatibility** tab and then clicking the link for the appropriate device types..

Important: Configure the servers in ways that minimize IP address changes. Consider using static IP addresses instead of Dynamic Host Configuration Protocol (DHCP). If DHCP is used, ensure that IP address changes are minimized.

About this task

Important: Implementing a shared data and management network can cause disruptions in traffic, such as packets being dropped or management-network connectivity issues, depending on your network configuration (for example, if traffic from servers have a high priority and traffic from the management controllers have a low priority). The management network uses UDP traffic in addition TCP. UDP traffic can have a lower priority when the network traffic is high.

The following figure illustrates one way to set up your environment if the data network and management network are the same network. The numbers in the figure correspond to the numbered steps in the following sections.

Note: This figure does not depict all cabling options that might be required for your environment,. Instead, this figure shows only the cabling-option requirements as they relate to setting up a single data/management network.

© Copyright Lenovo 2017, 2023

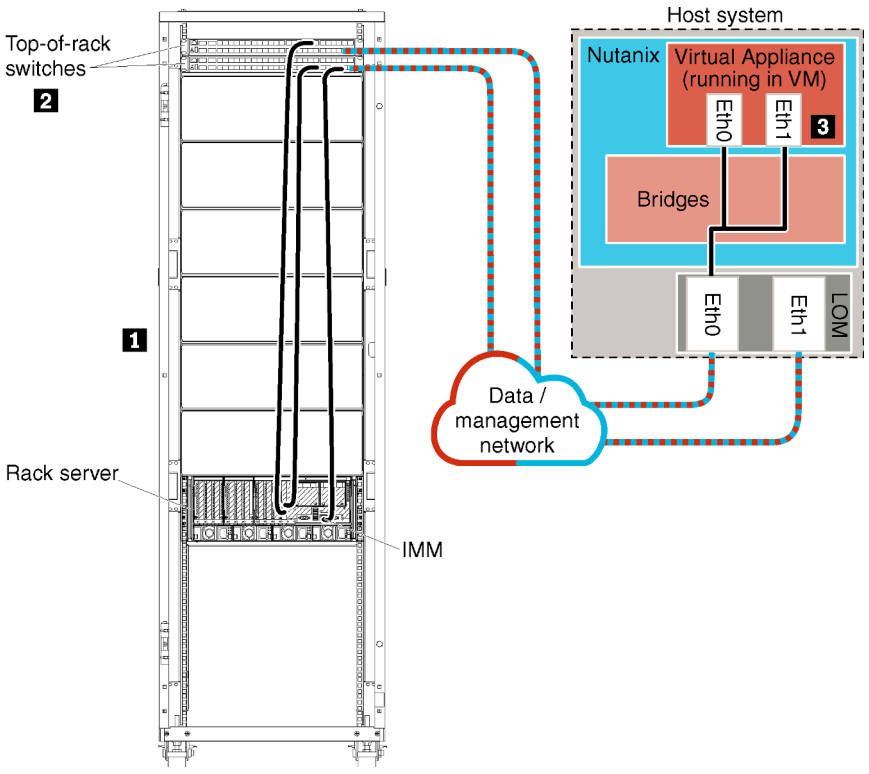


Figure 8. Sample single data and management network topology (Nutanix AHV)

Important: You can setup XClarity Administrator on any system that meets the requirements for XClarity Administrator, including a managed server. If you use a managed server for the XClarity Administrator host:

- You must implement either a virtually separate data and management network topology or a single data and management network topology.
- You cannot use XClarity Administrator to apply firmware updates to that managed server. Even when only some of the firmware is applied with immediate activation, XClarity Administrator forces the target server to restart, which would restart XClarity Administrator as well. When applied with deferred activation, only some firmware is applied when the XClarity Administrator host is restarted.

If you intend to install XClarity Administrator to manage an existing rack server that has already been configured, proceed to Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance.

For additional information about planning for this topology, including information about network settings and Eth1 and Eth0 configuration, see Single data and management network.

Step 1: Cable the rack servers and Lenovo XClarity Administrator host to the top-of-rack switches

Cable rack servers and Lenovo XClarity Administrator host to the top-of-rack switches to enable communications between the devices and your network.

Procedure

Cable each rack server and the XClarity Administrator host to both top-of-rack switches. You can choose any ports in the top-of-rack switches.

The following figure is an example that illustrates cabling from the rack servers and XClarity Administrator host to the top-of-rack switches.

Note: This figure does not depict all cabling options that might be required for your environment,. Instead, this figure shows only the cabling-option requirements as they relate to setting up a single data/management network.

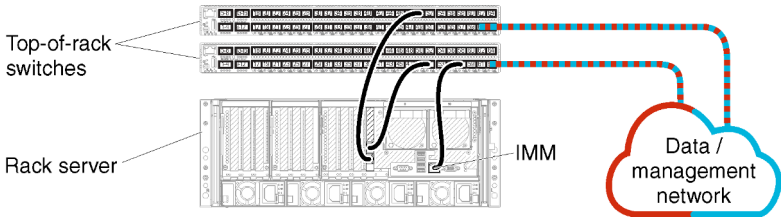


Figure 9. Example cabling for a single data and management network

Step 2: Configure top-of-rack switches

Configure the top-of-rack switches.

Before you begin

In addition to typical configuration requirements for top-of-rack switches, ensure that all appropriate ports are enabled, including the external ports to the rack servers and network.

Procedure

The configuration steps might vary, depending on the type of rack switches that are installed.

For information about configuring Lenovo top-of-rack switches, see Rack switches in the System x online documentation. If another top-of-rack switch is installed, see the documentation that came with that switch.

Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance

Install and configure the XClarity Administrator virtual appliance on the Nutanix AHV host.

Before you begin

You must be logged in to Nutanix AHV as a user with admin authority to install the virtual appliance.

Ensure that the network is configured before installing XClarity Administrator.

Procedure

To install the XClarity Administrator virtual appliance, complete the following steps.

Step 1. Download the XClarity Administrator virtual-appliance image from the XClarity Administrator download webpage to a client workstation. Log on to the Web site, and then use the access key that was given to you to download the image.

For Nutanix AHV, download the image in QCOW2 format.

Step 2. Install and configure the virtual appliance on the host.

a. Log in to the Nutanix AHV cluster.

b. If you are not using a DHCP server, upload the virtual disk image and `eth0_config.iso` image to the Nutanix AHV cluster.
    1. Click the **Settings** menu (), and then click **Image configuration** to display the Image Configuration dialog.
    2. Click **Upload Image** to display the Create Image dialog.
        a. Specify a name for the virtual disk image, such as XClarity Administrator.
        b. Select DISK for the image type.
        c. Select **Upload a file**, click **Choose File**, and select the virtual disk image.
        d. Click **Save** to upload the file.
    3. Click **Close** to close the Image Configuration dialog.
c. Wait until the upload processes are completed before continuing. The status circle in the menu indicates when the processes are complete.
d. Create the virtual machine.
    1. Click **Home → VM**.
    2. Click **+Create VM** in the upper-right corner to display the Create VM dialog.
    3. Specify a name for the virtual machine.
    4. Specify at least `2` for the number of VCPUs.
    5. Specify least **8192** MB or the memory.
    6. Scroll down to the Disk section.
    7. Add a disk for the virtual disk image:
        a. Click the **Add New Disk** to display the Add Disk dialog.
        b. Select **Clone from Image Service** for the operations.
        c. Select the virtual disk image in the image list.
        d. Click **Add**.
    8. Scroll down to the Network Adapters NIC section and add the data/management network:
        a. Click **Add New NIC** to display the Create NIC dialog.
        b. Select the appropriate VLAN for the network.
        c. Click **Add**.
    9. Click **Save** in the Create VM dialog.
    10. Wait until the virtual machine is created before continuing. The status circle in the menu indicates when the process is complete.
    11. Start the virtual machine.
        a. Select the **Table** view in the upper left corner.
        b. Select the virtual machine that you just created.
        c. Click **Power On Actions**.
        d. Click **Launch Console**.

    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 build xxx
----------------------------------------

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     Disabled


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

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
  … …
```

(Optional) Using a configuration file to set the IP settings

If you are not using a DHCP server, you can optionally use a configuration file to specify the IP settings that you want to use to access the XClarity Administrator web interface using the Eth0 network interface.

The configuration file (`eth0_config`) is contained in an ISO file that you create and mount to the virtual machine before XClarity Administrator is started for the first time. When XClarity Administrator starts the first time, it configures the IP address for the Eth0 network using the static IP address that is defined in the `eth0_config` file and displays the web interface to set up initially and configure the appropriate settings (see Configuring Lenovo XClarity Administrator).

Restriction: Only the Eth0 network can be configured using this method. Creating a configuration file named `eth1_config` does not configure the Eth1 network.

To use a configuration file, perform the following steps before powering on the virtual appliance

1. Create a file named `eth0_config` (with no file extension) that contains the following IPv4 parameters that you want the virtual machine to use at startup.
   - IPV4_ADDR=
   - IPV4_NETMASK=
   - IPV4_GATEWAY=
   - IPV6_ADDR=
   - IPV6_GATEWAY=

   You can use the echo command to create the file, for example:

   ```
   ECHO IPV4_ADDR=1.1.1.1 > ./eth0_config
   ECHO IPV4_NETMASK=255.255.255.05 >> ./eth0_config
   ECHO IPV4_GATEWAY=1.1.1.5 >> ./eth0_config
   ECHO IPV6_ADDR=1001:1002:1003:1004::2 >> ./eth0_config
   ECHO IPV6_GATEWAY=1001:1002:1003:1004::1 >> ./eth0_config
   ```

   Note: The IPV6_ADDR and IPV6_GATEWAY parameters are supported in XClarity Administrator v1.1.1 and later.
2. Create an ISO image that contains the `eth0_config` file.

   To create an ISO image on Windows, use your favorite ISO software. On Linux, use the `mkisofs` command, for example:

   ```
   mkisofs -V IP4ADDR -J -o ./boot.iso ./eth0_config
   ```

   where -V is the volume label, -J is for Joliet format, -o is the output file name, and ./eth0_config is the file to be included in the ISO image.
3. Upload the ISO image to a suitable location using the Datastore Browser.
4. Mount the .ISO image to the virtual machine.
   a. Click the **Settings** menu (), and then click **Image configuration** to display the Image Configuration dialog.
   b. Upload the `eth0_config.iso` image.
      1) From the Image Configuration dialog, click **Upload Image** to display the Create Image dialog again.
      2) Specify a name for the ISO image.
      3) Select ISO for the image type.
      4) Select **Upload a file**, click **Choose File**, and select the `eth0_config.iso` image.
      5) Click **Save** to upload the file.
      6) Click **Close** to close the Image Configuration dialog.
   c. Wait until the upload processes are completed before continuing with the setup steps. The status circle in the menu indicates when the processes are complete.
   d. Add a disk for the `eth0_config.iso` image.
      1) From the VM, click **Update** from the bottom menu bar.
      2) Click the **Edit** icon for the CDROM disk to display the Edit Disk dialog.
      3) Select **Clone** from Image Service for the operations.
      4) Select the ISO image that you created earlier from the image list.
      5) Click **Update**.

6) Click **Save**.

Note: You can unmount the drive and delete the ISO image after you log in to the XClarity Administrator web interface and finish configuring the appropriate settings.

After you finish

Log in and configure XClarity Administrator (see Accessing the Lenovo XClarity Administrator web interface for the first time and Configuring Lenovo XClarity Administrator).

Physically separate data and management networks (Nutanix AHV)

In this topology, the data network and management network are physically separate networks. Management communications between Lenovo XClarity Administrator and the network occurs over the Eth0 network interface on the host. Data communications occurs over the Eth1 network interface.

Before you begin

Ensure that all appropriate ports are enabled, including ports that XClarity Administrator requires (see Port availability).

Ensure that the minimum required firmware is installed on each device that you intend to manage using XClarity Administrator. You can find minimum required firmware levels from the XClarity Administrator Support – Compatibility webpage by clicking the **Compatibility** tab and then clicking the link for the appropriate device types..

Important: Configure the servers in ways that minimize IP address changes. Consider using static IP addresses instead of Dynamic Host Configuration Protocol (DHCP). If DHCP is used, ensure that IP address changes are minimized.

About this task

The following figure illustrates one way to set up your environment when the data and management networks are physically different networks. The numbers in the figure correspond to the numbered steps in the following sections.

Note: This figure does not depict all cabling options that might be required for your environment. Instead, this figure shows only the cabling-option requirements as they relate to setting up physically separate data and management networks.

Tip: Instead of setting up two physical switches that are connected to each network for redundancy (for a total of four switches), you can set up a single physical switch that is connected to each network (for a total of two switches). In that case, each switch would be connected to both networks, and you would implement two VLANs: one for the data network and one for the management network, to segregate data traffic.

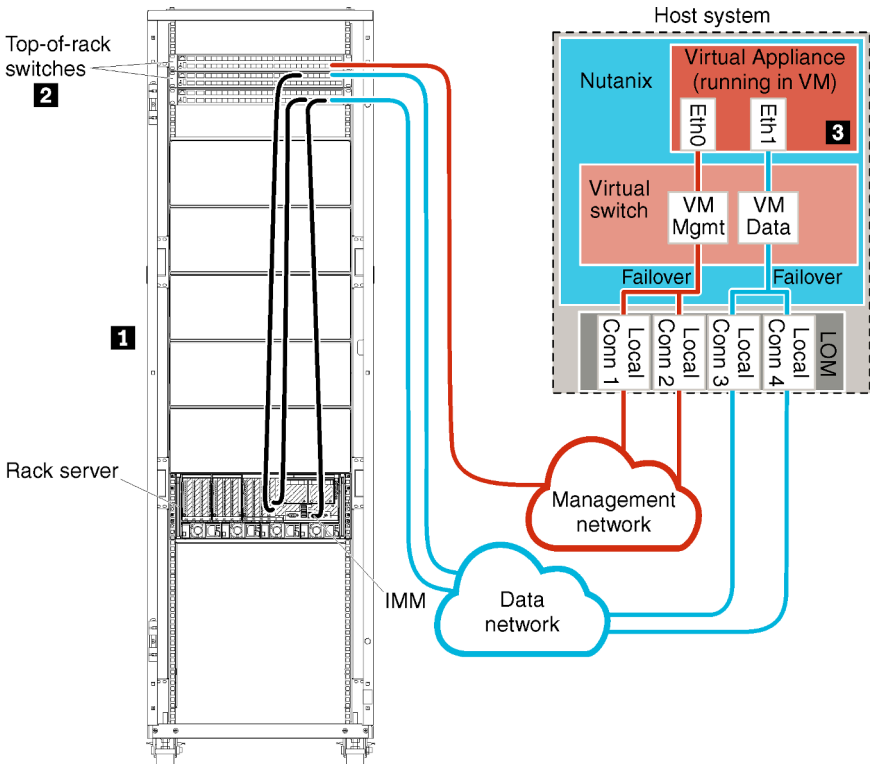


Figure 10. Sample Network topology - Physically separate data and management network (Nutanix AHV)

If you intend to install XClarity Administrator to manage an existing rack server that has already been configured, proceed to Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance.

For additional information about planning for this topology, including information about network settings and Eth1 and Eth0 configuration, see Physically separate data and management network.

Step 1: Cable the rack servers and Lenovo XClarity Administrator host to the top-of-rack switches

Cable rack servers and XClarity Administrator host to the top-of-rack switches to enable communications between the devices and your networks.

Procedure

Cable each rack server, and the XClarity Administrator host to both top-of-rack switches. You can choose any ports in the top-of-rack switches.

The following figure is an example that illustrates cabling from the rack servers and XClarity Administrator host to the top-of-rack switches.

Note: This figure does not depict all cabling options that might be required for your environment,. Instead, this figure shows only the cabling-option requirements as they relate to setting up physically separate data and management networks.

Tip: Instead of setting up two physical switches that are connected to each network for redundancy (for a total of four switches), you can set up a single physical switch that is connected to each network (for a total of two switches). In that case, each switch would be connected to both networks, and you would implement two VLANs: one for the data network and one for the management network, to segregate data traffic.

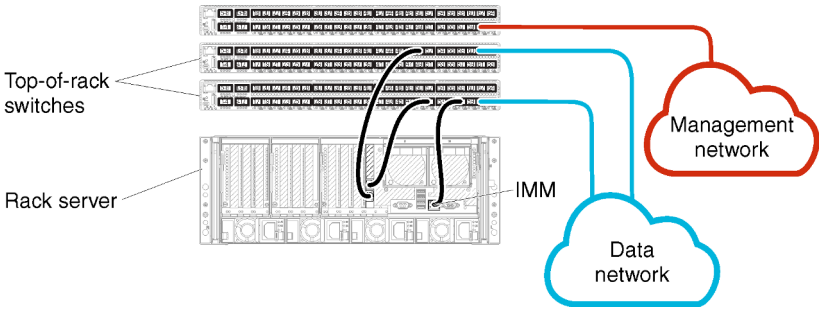


Figure 11. Example cabling for physically separate data and management networks (VMware ESXi)

Step 2: Configure top-of-rack switches

Configure the top-of-rack switches.

Before you begin

In addition to typical configuration requirements for top-of-rack switches, ensure that all appropriate ports are enabled, including the external ports to the rack servers and network.

Procedure

The configuration steps might vary, depending on the type of rack switches that are installed.

For information about configuring Lenovo top-of-rack switches, see Rack switches in the System x online documentation. If another top-of-rack switch is installed, see the documentation that came with that switch.

Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance

Install and configure the XClarity Administrator virtual appliance on the Nutanix AHV host.

Before you begin

You must be logged in to Nutanix AHV as a user with admin authority to install the virtual appliance.

Ensure that the network is configured before installing XClarity Administrator.

Procedure

To install the XClarity Administrator virtual appliance, complete the following steps.

Step 1. Download the XClarity Administrator virtual-appliance image from the XClarity Administrator download webpage to a client workstation. Log on to the Web site, and then use the access key that was given to you to download the image.

For Nutanix AHV, download the image in QCOW2 format.

Step 2. Install and configure the virtual appliance on the host.

a. Log in to the Nutanix AHV cluster.

b. If you are not using a DHCP server, upload the virtual disk image and `eth0_config.iso` image to the Nutanix AHV cluster.

1. Click the **Settings** menu (), and then click **Image configuration** to display the Image Configuration dialog.
2. Click **Upload Image** to display the Create Image dialog.
   a. Specify a name for the virtual disk image, such as XClarity Administrator.
   b. Select DISK for the image type.
   c. Select **Upload a file**, click **Choose File**, and select the virtual disk image.
   d. Click **Save** to upload the file.
3. Click **Close** to close the Image Configuration dialog.

c. Wait until the upload processes are completed before continuing. The status circle in the menu indicates when the processes are complete.

d. Create the virtual machine.
   1. Click **Home → VM**.
   2. Click **+Create VM** in the upper-right corner to display the Create VM dialog.
   3. Specify a name for the virtual machine.
   4. Specify at least 2 for the number of VCPUs.
   5. Specify least **8192** MB or the memory.
   6. Scroll down to the Disk section.
   7. Add a disk for the virtual disk image:
      a. Click the **Add New Disk** to display the Add Disk dialog.
      b. Select **Clone from Image Service** for the operations.
      c. Select the virtual disk image in the image list.
      d. Click **Add**.
   8. Scroll down to the Network Adapters NIC section and add the data/management network:
      a. Click **Add New NIC** to display the Create NIC dialog.
      b. Select the appropriate VLAN for the network.
      c. Click **Add**.
   9. Click **Save** in the Create VM dialog.
   10. Wait until the virtual machine is created before continuing. The status circle in the menu indicates when the process is complete.
   11. Start the virtual machine.
      a. Select the **Table** view in the upper left corner.
      b. Select the virtual machine that you just created.
      c. Click **Power On Actions**.
      d. Click **Launch Console**.

   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 build xxx
----------------------------------------

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     Disabled


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

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
  … …
```

(Optional) Using a configuration file to set the IP settings

If you are not using a DHCP server, you can optionally use a configuration file to specify the IP settings that you want to use to access the XClarity Administrator web interface using the Eth0 network interface.

The configuration file (`eth0_config`) is contained in an ISO file that you create and mount to the virtual machine before XClarity Administrator is started for the first time. When XClarity Administrator starts the first time, it configures the IP address for the Eth0 network using the static IP address that is defined in the `eth0_config` file and displays the web interface to set up initially and configure the appropriate settings (see Configuring Lenovo XClarity Administrator).

Restriction: Only the Eth0 network can be configured using this method. Creating a configuration file named `eth1_config` does not configure the Eth1 network.

To use a configuration file, perform the following steps before powering on the virtual appliance

1. Create a file named `eth0_config` (with no file extension) that contains the following IPv4 parameters that you want the virtual machine to use at startup.
   - IPV4_ADDR=
   - IPV4_NETMASK=
   - IPV4_GATEWAY=
   - IPV6_ADDR=
   - IPV6_GATEWAY=

   You can use the echo command to create the file, for example:
   ```
   ECHO IPV4_ADDR=1.1.1.1 > ./eth0_config
   ECHO IPV4_NETMASK=255.255.255.05 >> ./eth0_config
   ECHO IPV4_GATEWAY=1.1.1.5 >> ./eth0_config
   ECHO IPV6_ADDR=1001:1002:1003:1004::2 >> ./eth0_config
   ECHO IPV6_GATEWAY=1001:1002:1003:1004::1 >> ./eth0_config
   ```

   Note: The IPV6_ADDR and IPV6_GATEWAY parameters are supported in XClarity Administrator v1.1.1 and later.
2. Create an ISO image that contains the `eth0_config` file.

   To create an ISO image on Windows, use your favorite ISO software. On Linux, use the `mkisofs` command, for example:
   ```
   mkisofs -V IP4ADDR -J -o ./boot.iso ./eth0_config
   ```

   where -V is the volume label, -J is for Joliet format, -o is the output file name, and ./eth0_config is the file to be included in the ISO image.
3. Upload the ISO image to a suitable location using the Datastore Browser.
4. Mount the .ISO image to the virtual machine.
   a. Click the **Settings** menu (), and then click **Image configuration** to display the Image Configuration dialog.
   b. Upload the `eth0_config.iso` image.
      1) From the Image Configuration dialog, click **Upload Image** to display the Create Image dialog again.
      2) Specify a name for the ISO image.
      3) Select ISO for the image type.
      4) Select **Upload a file**, click **Choose File**, and select the `eth0_config.iso` image.
      5) Click **Save** to upload the file.
      6) Click **Close** to close the Image Configuration dialog.
   c. Wait until the upload processes are completed before continuing with the setup steps. The status circle in the menu indicates when the processes are complete.
   d. Add a disk for the `eth0_config.iso` image.
      1) From the VM, click **Update** from the bottom menu bar.
      2) Click the **Edit** icon for the CDROM disk to display the Edit Disk dialog.
      3) Select **Clone** from Image Service for the operations.
      4) Select the ISO image that you created earlier from the image list.
      5) Click **Update**.
      6) Click **Save**.

   Note: You can unmount the drive and delete the ISO image after you log in to the XClarity Administrator web interface and finish configuring the appropriate settings.

After you finish

Log in and configure XClarity Administrator (see Accessing the Lenovo XClarity Administrator web interface for the first time and Configuring Lenovo XClarity Administrator).

Virtually separate data and management network topology (Nutanix AHV)

In this topology, the data network and management network are virtually separate. Packets from the data network and packets from the management network are sent over the same physical connection. VLAN tagging on all management-network data packets is used to keep the traffic between the two networks separate.

Ensure that all appropriate ports are enabled, including ports that XClarity Administrator requires (see Port availability).

Ensure that the minimum required firmware is installed on each device that you intend to manage using XClarity Administrator. You can find minimum required firmware levels from the XClarity Administrator Support – Compatibility webpage by clicking the **Compatibility** tab and then clicking the link for the appropriate device types..

Ensure that VLAN IDs are set up for the data network and management network. Optionally, enable VLAN tagging the top-of-rack switches if you implement tagging from the top-of-rack switches.

Important: Configure the servers in ways that minimize IP address changes. Consider using static IP addresses instead of Dynamic Host Configuration Protocol (DHCP). If DHCP is used, ensure that IP address changes are minimized.

About this task

The following figure illustrates one way to set up your environment so that the management network is separated from the virtual network. The numbers in the figure correspond to the numbered steps in the following sections.

Note: This figure does not depict all cabling options that might be required for your environment. Instead, this figure shows only the cabling-option requirements as they relate to setting up virtually separate data and management networks.

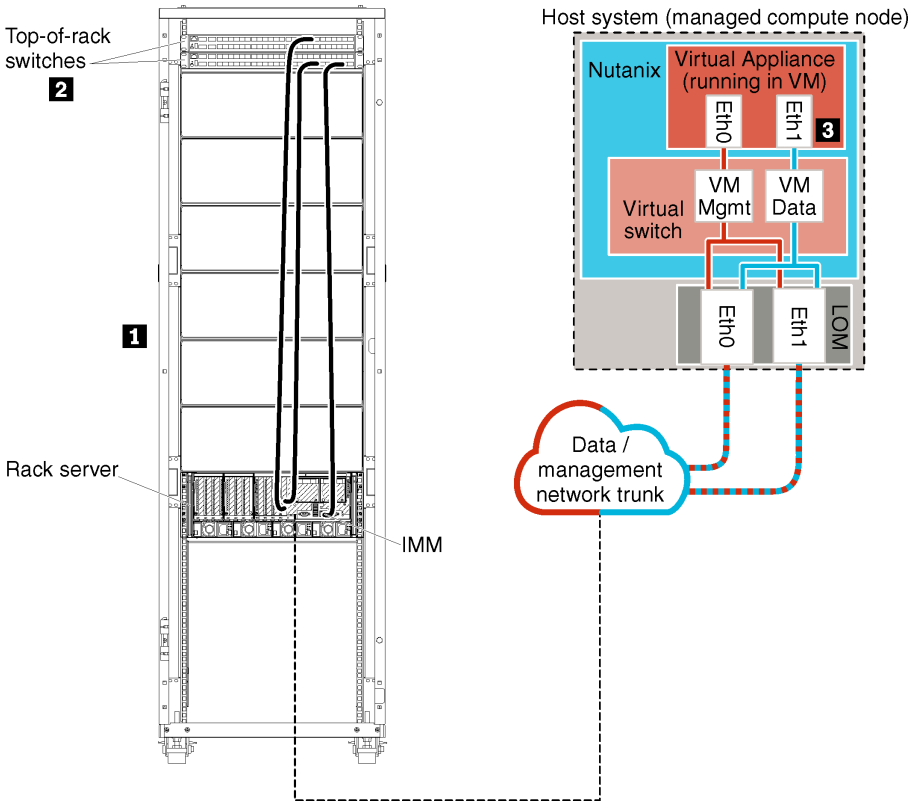


Figure 12. Sample Network topology - Virtually separate data and management network (Nutanix AHV)

In this scenario, Lenovo XClarity Administrator is installed on a server in a Flex System chassis that is being managed by XClarity Administrator.

Important: You can setup XClarity Administrator on any system that meets the requirements for XClarity Administrator, including a managed server. If you use a managed server for the XClarity Administrator host:

- You must implement either a virtually separate data and management network topology or a single data and management network topology.
- You cannot use XClarity Administrator to apply firmware updates to that managed server. Even when only some of the firmware is applied with immediate activation, XClarity Administrator forces the target server to restart, which would restart XClarity Administrator as well. When applied with deferred activation, only some firmware is applied when the XClarity Administrator host is restarted.

Also in this scenario, all data is sent over the same physical connections. The separation of the management network from the data network is accomplished through VLAN tagging, in which specific tags corresponding to the management network are appended to incoming data packets to ensure that they are routed to the appropriate interfaces. The tags are removed from outgoing data packets.

VLAN tagging can be enabled on the top-of-rack switches. VLAN tags corresponding to the management network are added to packets as they enter the top-of-rack switch and are passed through the Flex switches and on to the servers in the Flex System chassis. On the return route, VLAN tags are removed as they are sent from the top-of-rack switch to the management controllers.

The choice of whether to implement VLAN tagging is based on the needs and complexity of your environment.

If you intend to install XClarity Administrator to manage an existing rack server that has already been configured, proceed to Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance.

For additional information about planning for this topology, including information about network settings and Eth1 and Eth0 configuration, see Virtually separate data and management network.

Step 1: Cable rack servers to the top-of-rack switches

Cable rack servers to the same top-of-rack switch to enable communications between the devices.

Procedure

Cable each rack server to both top-of-rack switches. You can choose any ports in that top-of-rack switch.

The following figure is an example that illustrates cabling from the rack servers to the top-of-rack switches when Lenovo XClarity Administrator is installed on a server that will be managed by Lenovo XClarity Administrator.

Note: This figure does not depict all cabling options that might be required for your environment,. Instead, this figure shows only the cabling-option requirements as they relate to setting up a virtually separate data and management networks.

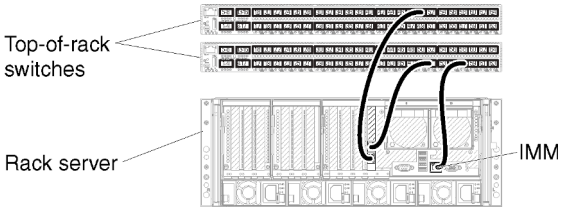


Figure 13. Example cabling for virtually separate data and management networks

Step 2: Configure top-of-rack switches

Configure the top-of-rack switches.

Before you begin

In addition to typical configuration requirements for top-of-rack switches, ensure that all appropriate ports are enabled, including the external ports to the rack servers and network.

You can implement VLAN tagging in the Flex switches or top-of-rack switches, depending on the needs and complexity of your environment. If you implement tagging from the top-of-rack switches, enable VLAN tagging from the top-of-rack switches.

Ensure that VLAN IDs are set up for the management and data networks.

Procedure

The configuration steps might vary, depending on the type of rack switches that are installed.

The following figure is an example scenario that illustrates VLAN tagging that is implemented in the top-of-rack switches and enabled on only the management network. The management VLAN is set up as VLAN 10.

In this scenario, you must define the ports to which the CMMs are connected as belonging to the management VLAN.

Note: You can also enable VLAN tagging on the data network to configure a data VLAN.

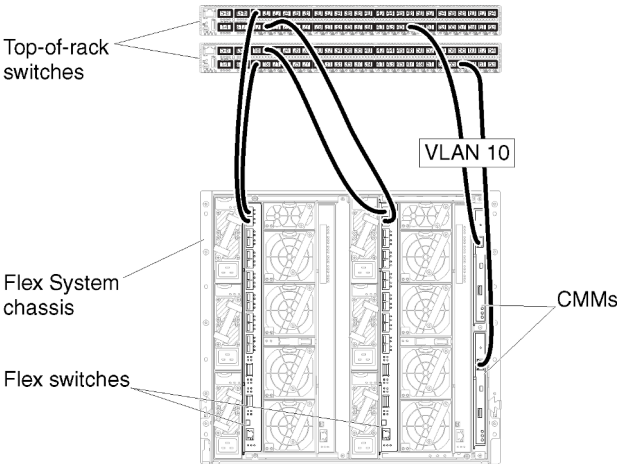


Figure 14. Example configuration for Flex switches on virtually separate data and management networks (KVM) in which VLAN tagging is enabled on the management network

For information about configuring Lenovo top-of-rack switches, see Rack switches in the System x online documentation. If another top-of-rack switch is installed, see the documentation that came with that switch.

Step 3. Install and configure the Lenovo XClarity Administrator virtual appliance

Install the XClarity Administrator virtual appliance on the host, and configure XClarity Administrator.

Before you begin

You must be logged in to Nutanix AHV as a user with admin authority to install the virtual appliance.

Ensure that the network is configured before installing XClarity Administrator.

Procedure

To install the XClarity Administrator virtual appliance, complete the following steps.

Step 1. Download the XClarity Administrator virtual-appliance image from the XClarity Administrator download webpage to a client workstation. Log on to the Web site, and then use the access key that was given to you to download the image.

For Nutanix AHV, download the image in QCOW2 format.

Step 2. Install and configure the virtual appliance on the host.

a. Log in to the Nutanix AHV cluster.

b. If you are not using a DHCP server, upload the virtual disk image and `eth0_config.iso` image to the Nutanix AHV cluster.

1. Click the **Settings** menu ( ), and then click **Image configuration** to display the Image Configuration dialog.
2. Click **Upload Image** to display the Create Image dialog.

a. Specify a name for the virtual disk image, such as XClarity Administrator.
b. Select DISK for the image type.
c. Select **Upload a file**, click **Choose File**, and select the virtual disk image.
d. Click **Save** to upload the file.

3. Click **Close** to close the Image Configuration dialog.

c. Wait until the upload processes are completed before continuing. The status circle in the menu indicates when the processes are complete.

d. Create the virtual machine.

1. Click **Home → VM**.
2. Click **+Create VM** in the upper-right corner to display the Create VM dialog.
3. Specify a name for the virtual machine.
4. Specify at least 2 for the number of VCPUs.
5. Specify least **8192** MB or the memory.
6. Scroll down to the Disk section.
7. Add a disk for the virtual disk image:
   a. Click the **Add New Disk** to display the Add Disk dialog.
   b. Select **Clone from Image Service** for the operations.
   c. Select the virtual disk image in the image list.
   d. Click **Add**.
8. Scroll down to the Network Adapters NIC section and add the data/management network:
   a. Click **Add New NIC** to display the Create NIC dialog.
   b. Select the appropriate VLAN for the network.
   c. Click **Add**.
9. Click **Save** in the Create VM dialog.
10. Wait until the virtual machine is created before continuing. The status circle in the menu indicates when the process is complete.
11. Start the virtual machine.
    a. Select the **Table** view in the upper left corner.
    b. Select the virtual machine that you just created.
    c. Click **Power On Actions**.
    d. Click **Launch Console**.

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 build xxx
----------------------------------------

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     Disabled


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

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
  … …
```

(Optional) Using a configuration file to set the IP settings

If you are not using a DHCP server, you can optionally use a configuration file to specify the IP settings that you want to use to access the XClarity Administrator web interface using the Eth0 network interface.

The configuration file (`eth0_config`) is contained in an ISO file that you create and mount to the virtual machine before XClarity Administrator is started for the first time. When XClarity Administrator starts the first time, it configures the IP address for the Eth0 network using the static IP address that is defined in the `eth0_config` file and displays the web interface to set up initially and configure the appropriate settings (see Configuring Lenovo XClarity Administrator).

Restriction: Only the Eth0 network can be configured using this method. Creating a configuration file named `eth1_config` does not configure the Eth1 network.

To use a configuration file, perform the following steps before powering on the virtual appliance

1. Create a file named `eth0_config` (with no file extension) that contains the following IPv4 parameters that you want the virtual machine to use at startup.
   - IPV4_ADDR=
   - IPV4_NETMASK=

- IPV4_GATEWAY=
- IPV6_ADDR=
- IPV6_GATEWAY=

You can use the echo command to create the file, for example:

```
ECHO IPV4_ADDR=1.1.1.1 > ./eth0_config
ECHO IPV4_NETMASK=255.255.255.05 >> ./eth0_config
ECHO IPV4_GATEWAY=1.1.1.5 >> ./eth0_config
ECHO IPV6_ADDR=1001:1002:1003:1004::2 >> ./eth0_config
ECHO IPV6_GATEWAY=1001:1002:1003:1004::1 >> ./eth0_config
```

Note: The IPV6_ADDR and IPV6_GATEWAY parameters are supported in XClarity Administrator v1.1.1 and later.

2. Create an ISO image that contains the `eth0_config` file.

   To create an ISO image on Windows, use your favorite ISO software. On Linux, use the `mkisofs` command, for example:

   ```
   mkisofs -V IP4ADDR -J -o ./boot.iso ./eth0_config
   ```

   where -V is the volume label, -J is for Joliet format, -o is the output file name, and ./eth0_config is the file to be included in the ISO image.

3. Upload the ISO image to a suitable location using the Datastore Browser.
4. Mount the .ISO image to the virtual machine. The ISO file must reside in the datastore of the ESXi host so that it can be mounted as a CD/DVD drive on the XClarity Administrator virtual machine.
   a. Right click the virtual machine, and click **Edit Settings**.
   b. Click **Add** to display the Add Hardware wizard.
   c. Click **CD/DVD Drive**, and click **Next**.
   d. Select **Use ISO image**, and click **Next**.
   e. Select the ISO image, and click **Next**.
   f. Select the virtual device node, and click **Next**.
   g. Click **Finish**.

   Note: You can unmount the drive and delete the ISO image after you log in to the XClarity Administrator web interface and finish configuring the appropriate settings.

After you finish

Log in and configure XClarity Administrator (see Accessing the Lenovo XClarity Administrator web interface for the first time and Configuring Lenovo XClarity Administrator).

Chapter 4. Configuring Lenovo XClarity Administrator

When you access Lenovo XClarity Administrator for the first time, there are several steps that you must complete to initially set up XClarity Administrator.

Learn more: XClarity Administrator: Configuring for the first time

Procedure

Complete the following steps to set up XClarity Administrator for the first time.

Read and accept license agreement | Create user accounts | Configure network access | Configure date and time | Configure service and support | Configure security | Manage devices

Step 1. Access the XClarity Administrator web interface.

Step 2. Read and accept the license agreement.

Step 3. Create user accounts that have supervisor authority.

Tip: Consider creating at least two user accounts with supervisor authority so that you have a backup, if needed.

Step 4. Configure network access, including IP addresses for the data and management networks.

Step 5. Configure the date and time.

Step 6. Configure service and support settings, including the privacy statement, usage and hardware data, Lenovo Support (Call Home), Lenovo Upload Facility, and product warranty.

Step 7. Configure security settings, including authentication server, user groups, server certificates, and cryptography mode.

Step 8. Manage your chassis, servers, switches, and storage devices.

Step 9. We appreciate your feedback. Please take a minute to comment on your experience setting up XClarity Administrator.

Accessing the Lenovo XClarity Administrator web interface for the first time

You can launch the XClarity Administrator web interface from any computer that has network connectivity to the XClarity Administrator virtual machine.

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)

© Copyright Lenovo 2017, 2023

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 access the XClarity Administrator web interface for the first time.

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.

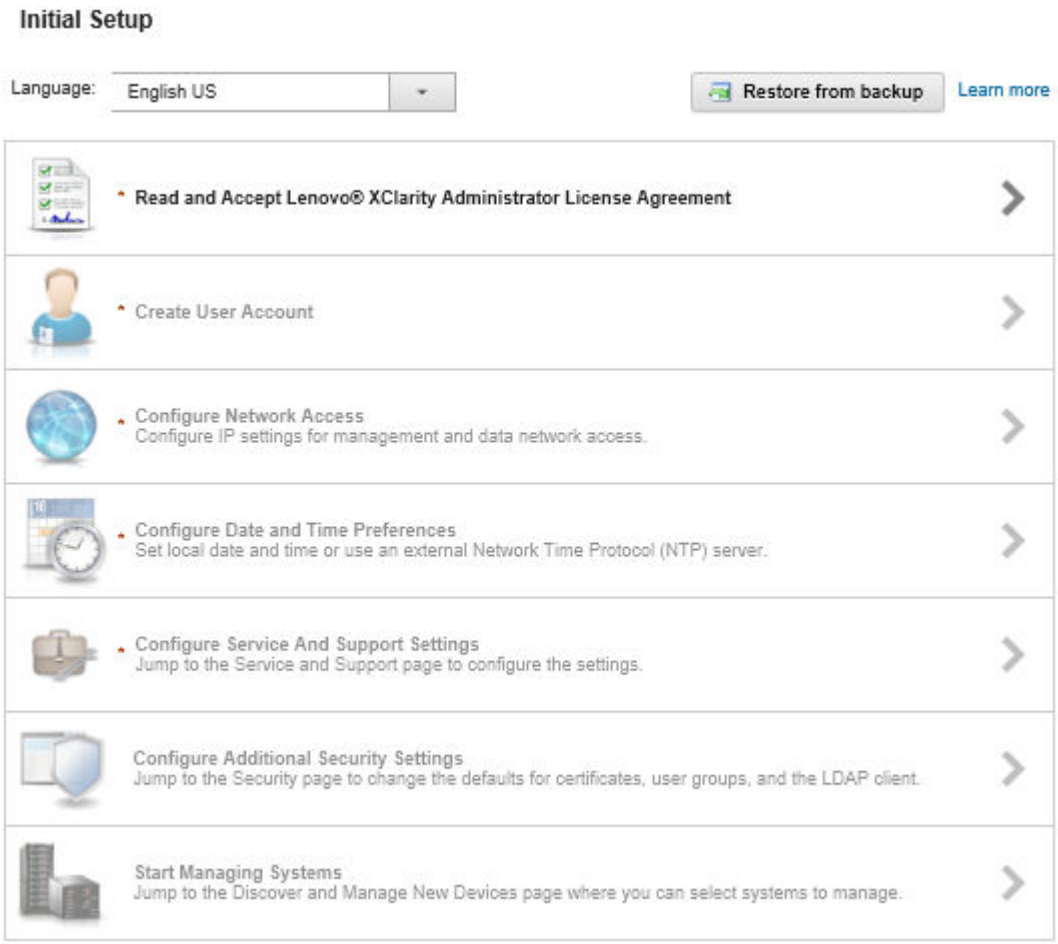
  For example, based on the examples shown for Eth0 and the zone index, enter the following URL in your web browser:

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

Step 2. You might receive security or certificate warnings the first time that you access Lenovo XClarity Administrator. You can ignore the warnings.

Results

The Initial Setup page is displayed.



After you finish

Complete the initial setup steps to configure the XClarity Administrator (see Configuring Lenovo XClarity Administrator).

Creating user accounts

User accounts are used to manage authorization and access to Lenovo XClarity Administrator and to devices that are under managed authentication.

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 create user accounts, complete the following steps.

Step 1. Fill in the following information in the Create New Supervisor User 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 role group in the XClarity Administrator online documentation.
- (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 2. Click **Create**.

Step 3. Click the **Create** icon ( ) and repeat the previous steps to create additional users.

Step 4. Click **Return to Initial Setup**.

Configuring network access

To configure network access, you can configure up to two network interfaces, the hostname for Lenovo XClarity Administrator, and the DNS servers to be used.

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, at least one of the network interfaces 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 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, at least one of the network interfaces 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 OS 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.

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 • None
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 • OS deployment • OS device-driver updates

Table 2. Role of each network interface based on network topology (continued)

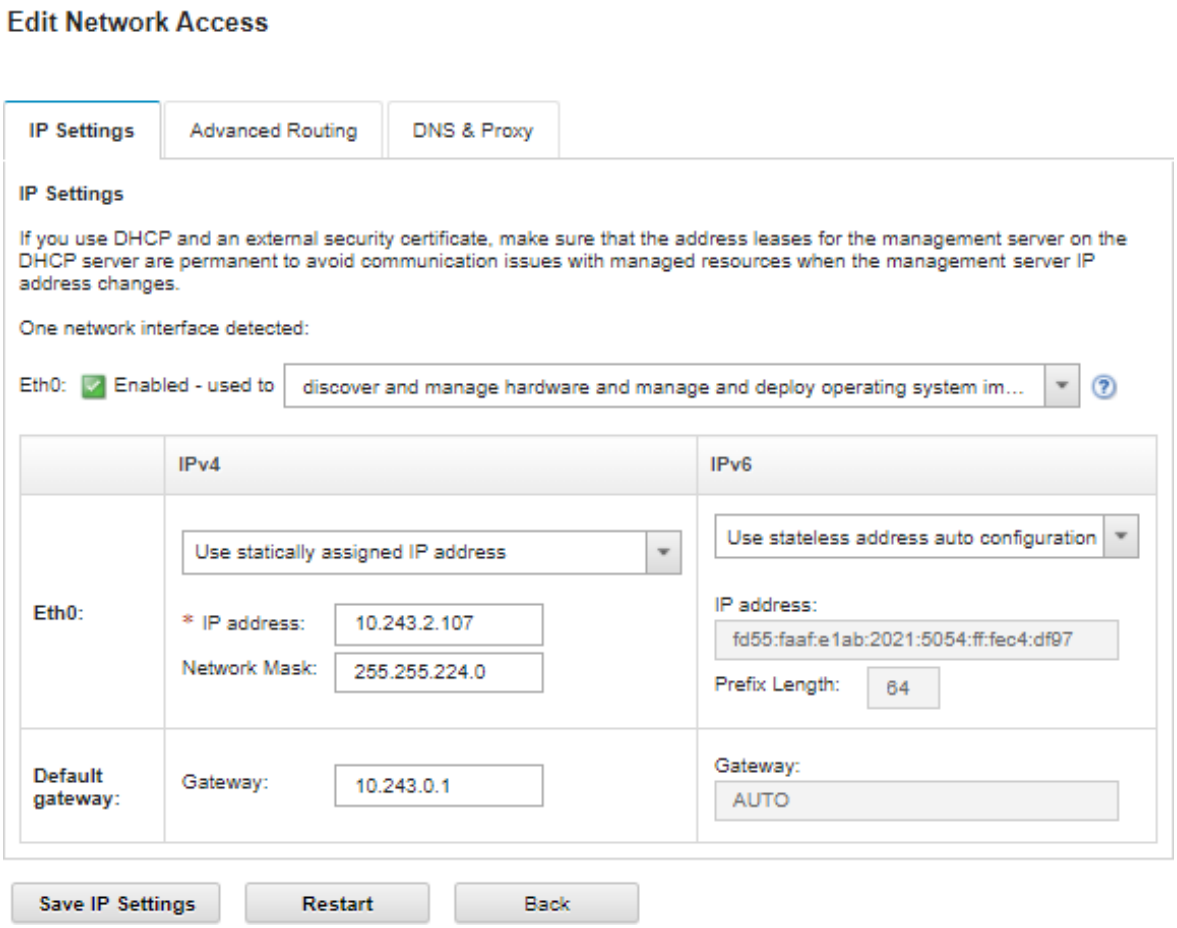
Network topology	Role of interface 1 (eth0)	Role of interface 2 (eth1)
Separate management network and data network without support for OS deployment and OS device-driver updates	Management network • Discovery and management • Server configuration • Firmware updates • Service data collection • Automatic problem notification (such as Call Home and Lenovo Update Facility) • Warranty data retrieval	Data network • None
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, see Network considerations.

Procedure

To configure the network access, complete the following steps.

Step 1. From the Initial Setup page, click **Configure Network Access**. The Edit Network Access page is displayed.



Step 2. 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 3. Specify 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 IP configuration limitations.

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.

If either interface uses DHCP to obtain an IP address, the default gateway also uses DHCP. To manually input a default gateway address that overrides the one received from DHCP server, select the **Override Gateway** checkbox.

Tips:

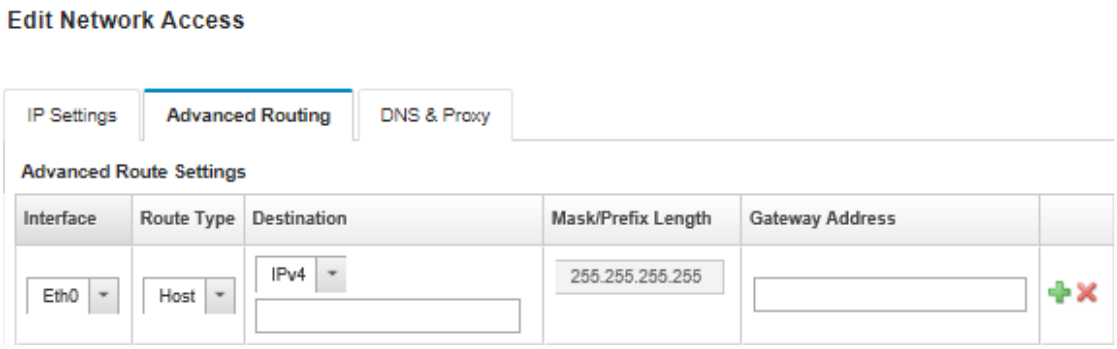
- Ensure that the gateway matches one of the network interfaces' subnet. The default gateway is automatically set through that network interface.
- To go back to a DHCP-provided gateway, clear the **Override Gateway** checkbox.

CAUTION:
If you choose to override the gateway, take care to input the correct gateway address; otherwise, this management server will be unreachable and there would be no way to remotely login to correct it.

d. Click **Save IP Settings**.

Step 4. Optional: **Optional:** Configure 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.

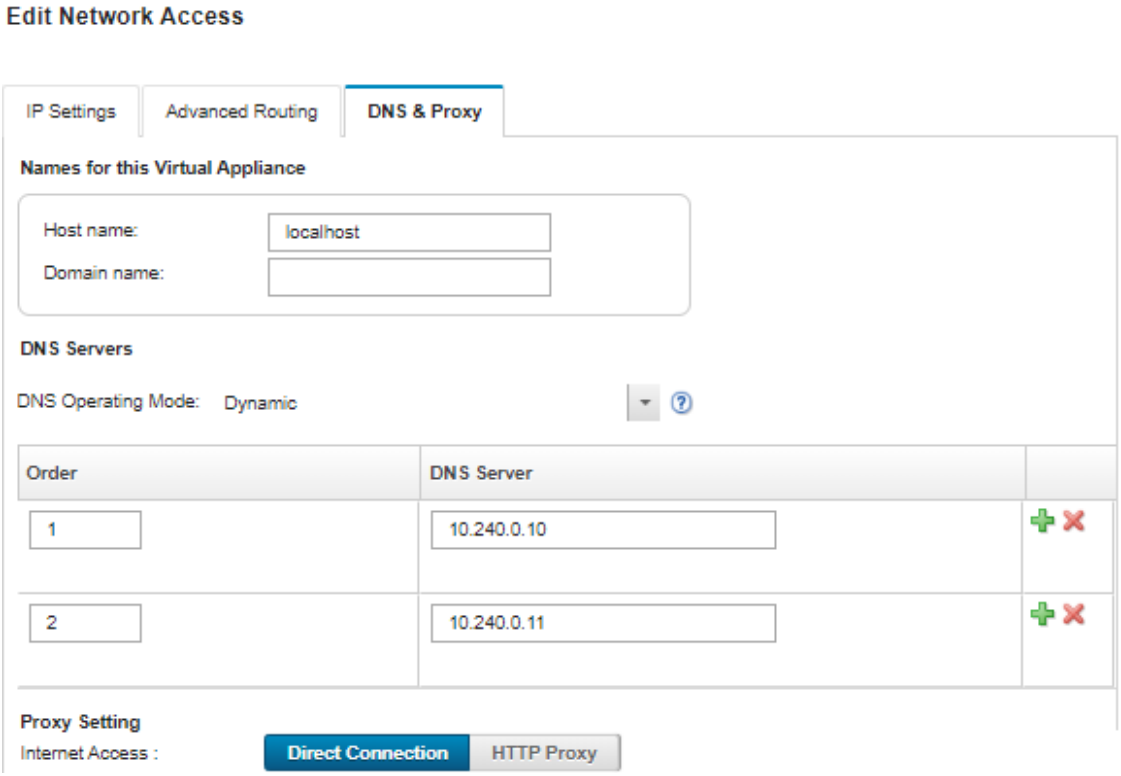
To define one or more route entries, complete the following steps.

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 5. Optionally, modify the DNS and proxy settings.

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**.

Attention: You must restart the management server when you change the DNS operating mode.

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**.

g. Push the XClarity Administrator management server fully-qualified domain name (FQDN) and DNS information to managed servers with IMM2, XCC, and XCC2 so that the managed servers can find the management server using this information.

1. Click **Push FQDN / DNS to BMC**.
2. Choose how to handle existing DNS entries in the baseboard management controller.
   - Keep the existing DNS entries, and append the management server DNS entries in the next available slot.
   - Replace all existing DNS entries with the management server DNS entries.
3. Type **YES** in the edit field.
4. Click **Apply**.

A job is created to perform this operation. You can monitor the progress of the job from the **Monitoring → Jobs** card. If the job did not complete successfully, click the job link to display details about the job (see Working with jobs in the XClarity Administrator online documentation .)

You can also remove the management server FQDN and DNS information from managed servers with IMM2, XCC, and XCC2 by clicking **Remove FQDN / DNS from BMC**. You can choose to keep other existing DNS entries, remove all DNS entries, or remove only entries that match the management server information.

Step 6. Click **Back**.

Step 7. Click **Test Connection** to verify the network settings.

Configuring the date and time

Although you can manually set the date and time for Lenovo XClarity Administrator, a better approach is to set up a Network Time Protocol (NTP) server that can be used to synchronize timestamps between XClarity Administrator and all managed devices.

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.

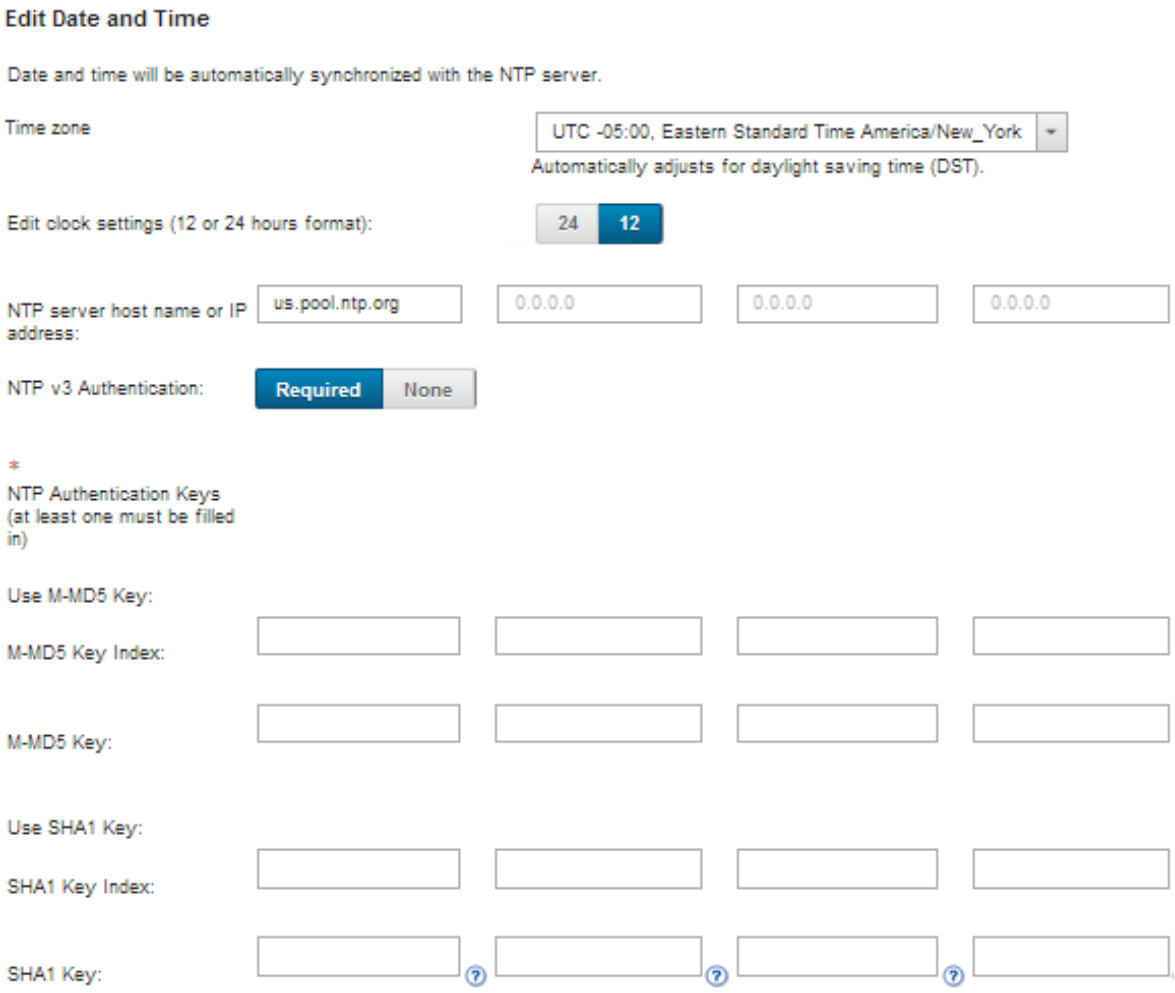
- For ESXi, following instructions on the VMware – Disabling Time Synchronization webpage.

- 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

To set up an NTP server for XClarity Administrator, complete the following steps.

Step 1. From the Initial Setup page, click **Configure Date and Time Preferences**. The Edit Date and Time page is displayed.



Step 2. 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 3. Click **Save**.

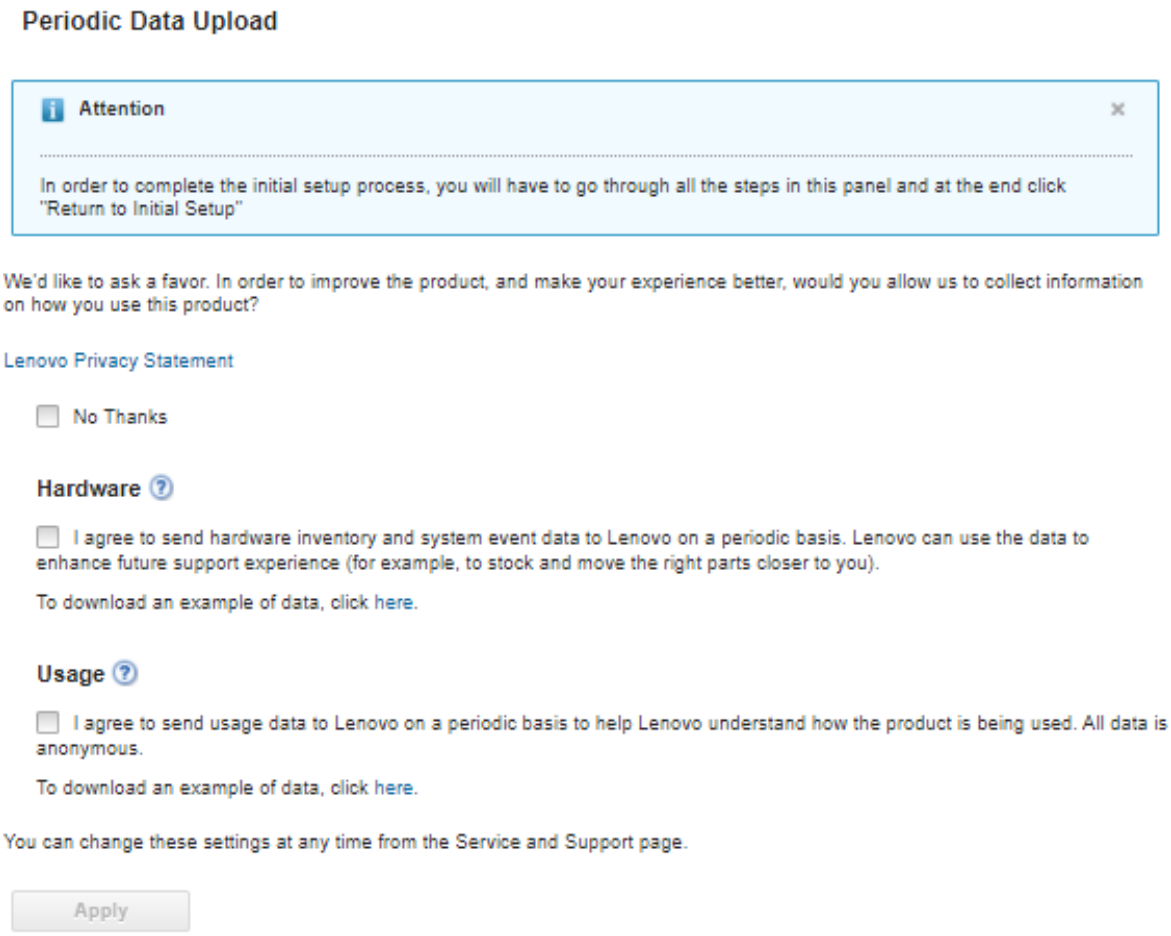
Configuring service and support

You can configure service and support settings, including usage data, Lenovo Support (Call Home), Lenovo Upload Facility, and product warranty.

Procedure

Complete the following steps to configure security.

Step 1. From the Initial Setup page, click **Configure Service and Support Settings**. The Service and Support page is displayed.



Step 2. Read and accept the Lenovo Privacy Statement.

Note: You cannot collect and send data to Lenovo without first accepting the Lenovo Privacy Statement. If you choose to decline the privacy statement, you can review and accept the privacy statement at a later time from the **Service and Support → Call Home Configuration** page.

Step 3. Optionally choose to allow Lenovo XClarity Administrator to collect usage and hardware information, and click **Apply**.

You can collect and send the following types of data to Lenovo.

- **Usage data**

  When you agree to send usage data to Lenovo, the following data is collected and sent on a weekly basis. This data *is anonymous*. No private data (including serial numbers, UUIDs, host names, IP addresses, and user names) is collected or sent to Lenovo.
  - Log of actions that were performed
  - List of events that were raised, and the timestamp when they were raised
  - List of audit events that raised, and the timestamp when they were raised
  - List of jobs that were run, and success or failure information for each job
  - XClarity Administrator metrics, including memory usage, processor usage, and disk space
  - Limited inventory data about all managed devices

- **Hardware data**

  When you agree to send hardware data to Lenovo, the following data is collected and sent on a periodic basis. This data *is not anonymous*. Hardware data includes attributes, such as UUIDs and serial numbers. It does not include IP addresses or hostnames.

- **Daily hardware data**. The following data is included for each inventory change.
  - Inventory-change event (FQXHMDM0001I)
  - Changes to inventory data for the device that is associated with that event
- **Weekly hardware data**. Inventory data is included for all managed devices.

When usage and hardware data is sent to Lenovo, an event is recorded in the audit log.

You can change this setting at any time and download the last archive that was collected and sent to Lenovo using the links on the clicking **Administration → Service and Support**, and then clicking the **Periodic Data Upload** tab.

Step 4. Optionally click **Call Home Configuration** to setup automatic problem notification to Lenovo Support (Call Home). Then, click **Apply & Enable** to create the Default Call Home service forwarder, or click **Apply only** to save the contact information.

For more information about setting up automatic problem notification to Lenovo Support, see Setting up call home in the XClarity Administrator online documentation.

Step 5. Optionally click **Lenovo Upload Facility** to setup automatic problem notification to the Lenovo Upload Facility. Then, click **Apply & Enable** to create the Default Lenovo Upload Facility service forwarder, or click **Apply only** to save the settings information.

For more information about setting up automatic problem notification to the Lenovo Upload Facility, see Setting up automatic problem notification to the Lenovo Upload Facility in the XClarity Administrator online documentation.

Step 6. Optionally click **Warranty** to enable external connections that are needed to collect warranty information for your managed devices.

For more information about viewing the warranty status (including extended warranties) of the managed devices, see Viewing warranty information in the XClarity Administrator online documentation.

Step 7. Optionally click **Lenovo Bulletin Service** to allow Lenovo to send service bulletins to XClarity Administrator, and click **Apply**

For more information about the types of service bulletins that Lenovo sends, see Getting bulletins from Lenovo in the XClarity Administrator online documentation.

Step 8. Specify the service-recovery password that you can use to collect and download service data and logs If XClarity Administrator becomes unresponsive and cannot be recovered.

For more information about the service-recovery password, see Changing the service-recovery password in the XClarity Administrator online documentation.

Step 9. Click **Return to Initial Setup**.

Configuring security

You can configure security, including role groups, authentication server, user-account security settings, cryptography, and certificates.

Procedure

Complete the following steps to configure security.

Step 1. From the Initial Setup page, click **Configure Additional Security Settings**. The Security page is displayed.

Step 2. Create customized role groups to manage authorization and access to resources (see Creating a role group in XClarity Administrator online documentation).

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

Step 3. Configure the authentication server (see Managing the authentication server in XClarity Administrator online documentation).

The *authentication server* is a Microsoft Active Directory (LDAP) server that is used to authenticate user credentials. XClarity Administrator uses a single authentication server for central user management of all managed devices (except Flex switches). When a device is managed by XClarity Administrator, the managed device and its installed components (except Flex switches) are configured to use 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 controller.

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

Step 4. Configure the user-account security settings, which control the password complexity, account lockout, and web-session inactivity timeout (see Changing the user-account security settings in the XClarity Administrator online documentation).

Step 5. Configure the cryptography setting that defines the communication modes and protocols that control the way that secure communications are handled between XClarity Administrator and the managed devices (see Setting the cryptography mode and communication protocols in the XClarity Administrator online documentation)

Step 6. If you plan to manage rack servers using local authentication instead of XClarity Administrator managed authentication, create one or more stored credentials that correspond with active user accounts on the device or in Active Directory that can be used to log in to the devices during the management process. For more information about stored credentials, see Managing stored credentials in the XClarity Administrator online documentation.

Step 7. If you plan to use a customized server certificate that includes your own information or use an externally-signed certificate, generate and deploy the new certificate before you begin managing systems. For information about generating your own security certificate, see Working with security certificates in the XClarity Administrator online documentation.

Step 8. From the vertical menu on the Security page, click **Return to Initial Setup**.

Managing devices

Lenovo XClarity Administrator can manage several types of systems, including the Flex System chassis, rack and tower servers, RackSwitch switches, and storage devices. You easily can discover and manage a large number of devices that are in your environment by importing information about your devices using a bulk-import file.

Before you begin

Important:

- You can manage a maximum of 300 devices at one time. Do not include more than 300 devices in a bulk import file.
- After you initiate a device-management operation, wait for the entire management job to complete before initiating another device-management operation.

Chassis components (such as CMMs, compute nodes, switches, and storage devices) are discovered and managed automatically when you manage the chassis that contains them. You cannot discover and managed chassis components separate from the chassis.

Certain ports must be available to communicate with the CMMs in the chassis and baseboard management controllers in the servers. Ensure that these ports are available before you attempt to manage systems. For more information about ports, see Port availability.

Ensure that the minimum required firmware is installed on each system that you want to manage using XClarity Administrator. You can find minimum required firmware levels from the XClarity Administrator Support – Compatibility webpage by clicking the **Compatibility** tab and then clicking the link for the appropriate device types.

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.

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).

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.

Important:

- 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.
- Multicast SLP forwarding must be enabled on each storage device before it can be discovered by XClarity Administrator.
- If you plan to use a customized server certificate that includes your own information or use an externally signed certificate, generate and deploy the new certificate before you begin managing systems. For information about generating your own security certificate, see Working with security certificates in the XClarity Administrator online documentation.
- 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.
- 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

About this task

XClarity Administrator can discover systems in your environment by probing for manageable devices that are on the same IP subnet as XClarity Administrator, by using a specified IP address or range of IP addresses, or by importing information from a spreadsheet.

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).

  Note: 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.

    Note: For Think Edge SE450, SE350 V2, and SE360 V2 servers, the default local user account remains enabled and all other local 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. 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 in the XClarity Administrator online documentation).

    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.

  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.

After systems are managed by XClarity Administrator, XClarity Administrator polls each managed system periodically to collect information, such as inventory, vital product data, and status. You can view and monitor each managed system and perform management actions (such as configuring system settings, deploying operating-system images, and powering on and off).

A system can be managed by only one XClarity Administrator at a time. Management by multiple managers is not supported. If a system is managed by one XClarity Administrator, and you want to manage it with another XClarity Administrator, you must first unmanage the system on the current XClarity Administrator. Then, you are can manage the system with another XClarity Administrator. For information about unmanaging a system, see Unmanaging chassis, Unmanaging servers, Unmanaging a RackSwitch switch, and Unmanaging a Lenovo Storage storage system in the XClarity Administrator online documentation.

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 system is managed (see Setting the cryptography mode and communication protocols in the XClarity Administrator online documentation).

Note: XClarity Administrator can be pre-populated with hardware inventory for a demo chassis (including CMM, compute nodes, and switches) and a demo rack or tower server that simulates real hardware. The demo devices are populated in the web interface pages and can be used to demonstrate management operations; however, the management operations will fail. For example, you can create a configuration pattern and deploy the pattern to a demo server, but the deployment will fail. You can remove the demo devices by unmanaging them (see Unmanaging chassis and Unmanaging servers in the XClarity Administrator online documentation). After the demo devices are deleted, they cannot be managed again..

Procedure

To discover and manage your systems in XClarity Administrator using a bulk-import file, complete the following steps.

Note: When managing switches using bulk import, HTTPS is enabled on the switch, and NTP clients on the switch are configured to use the NTP settings from the management server. To change these setting, you must manually manage the switches.

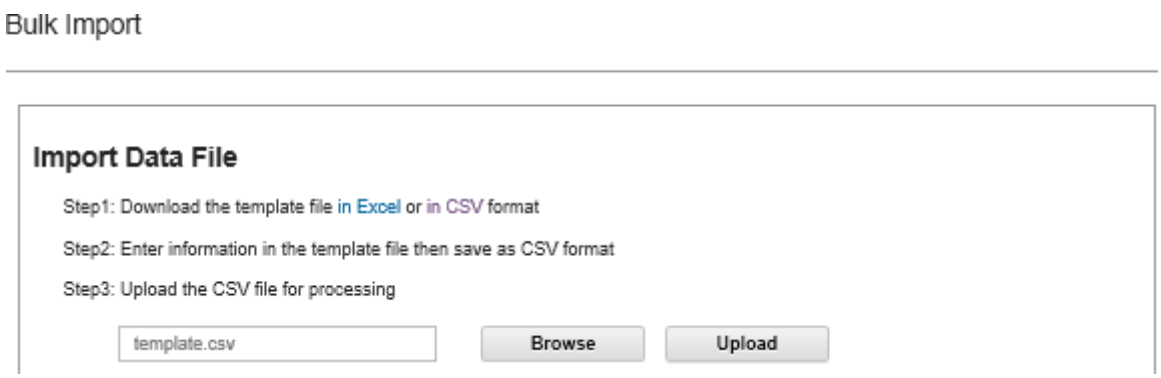
1. From the XClarity Administrator menu bar, click **Hardware → Discover and Manage New Devices**. The Discover and Manage page is displayed.
2. Click the **Enable encapsulation on all future managed devices** checkbox to change the firewall rules on all devices during the management process so that incoming requests are accepted from only XClarity Administrator.

   Notes:

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

   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 Recovering chassis management with a CMM after a management server failure and Recovering rack or tower server management after a management server failure in the XClarity Administrator online documentation.
3. Click **Bulk Import**. The Bulk Import wizard is displayed.



4. 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.
5. Fill in the data worksheet in the template file, and save the file in *comma-delimited* 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 devices in the bulk-import file, complete the following columns.

- (Columns A - C) For basic discovery, you must specify the device type and either the current IP address or serial number for the device. The following types are supported:
  - **filler**. Placeholders for an unmanaged device. In the rack view, this device is shown as generic filler graphic. See the **Readme** worksheet in the Excel template for additional filler types.
  - **flexchassis**. 10U Flex System chassis
  - **server**. Rack and tower servers that are supported by XClarity Administrator
  - **rack**. 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U, and 52U racks. Other rack heights are not supported. 52U is used by default.
  - **storage**. Storage devices
  - **switch**. RackSwitch switches

  Note: Flex System compute nodes, switches, and storage devices are considered part of the chassis discovery and management process.
- (Columns D - H) If you choose to use manually entered credentials instead of stored credentials (Columns Z) or identity (Columns AF – AJ), specify the current username and password. Manually entered credentials are useful if the credentials are different for some devices. If you do not specify credentials for one or more devices in the bulk-import file, the global credentials that you specify in the Bulk Import dialog are used instead. For more information about manually entered users and managed authentication, see Managing user accounts in the XClarity Administrator online documentation.

  Notes:
  - To use manually entered credentials, you must select XClarity Administrator managed authentication.
  - Some fields do not apply to some devices.
  - (For chassis) If you choose managed authentication (in column AA or in the Bulk Import dialog), you can must specify the `RECOVERY_ID` password either in column G of the bulk import file or in the Bulk Import dialog. If you choose local authentication, the recovery password is not allowed; do not specify the recovery password in column G of the bulk import file or in the Bulk Import dialog.
  - (For rack servers) If you choose managed authentication (in column AA or in the Bulk Import dialog), you can optionally specify a recovery password either in column G of the bulk import file or in the Bulk Import dialog. If you choose local authentication, the recovery password is not allowed; do not specify the recovery password in column G of the bulk import file or in the Bulk Import dialog.
  - (For rack switches) RackSwitch devices support only stored credentials (in column Z) for authenticating to the switches. Manual user credentials are not supported.
- (Columns I -U) You can optionally provide additional information if you want to apply changes to the device upon successful management.

Note: Some fields do not apply to some devices. These fields do not apply to RackSwitch switches.

- (Columns V- Z) You can optionally provide information for rack creation and assignment, including the rack name, location, room, lowest rack unit, and height.

  Notes:

  – When creating a rack, you must specify the rack name and rack height. The following rack heights are supported: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U, and 52U. Other rack heights are not supported.

  – When creating a generic filler, you must specify the rack name and filler height. The following filler heights are supported: 1U, 2U, and 4U.

  – When creating a specific filler, the filler height is ignored. XClarity Administrator knows the height of each specific filler. See the template spreadsheet for filler types and heights.

  – When assigning a device to rack, the device height is ignored. The device height is retrieved from the device inventory.

- (Column AA) 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.

  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.

  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.

- (Column AB) If you choose to use stored credentials instead of manually entered credentials (Columns D – H) or identity (Columns AF – AJ), specify a stored credential ID. You can find the stored credential ID on the Stored Credentials page by clicking **Administration → Security** from the XClarity Administrator menu and then clicking **Stored Credentials** from the left navigation. For more information about stored credentials and local authentication, see Managing stored credentials in the XClarity Administrator online documentation.

  Notes:

  – RackSwtich devices support only stored credentials for authentication. Manual user credentials (in column D) are not supported.

  – If you manage a device using stored credentials and enable managed authentication, you cannot edit those stored credentials.

- (Column AC) For chassis and rack servers, you chose to use choose managed authentication, you can must specify the RECOVERY_ID password either in column G of the bulk import file or in the Bulk Import dialog. If you choose local authentication, the recovery password is not allowed; do not specify the recovery password in column G of the bulk import file or in the Bulk Import dialog.

- (Column AD) For rack servers, you can optionally choose to use local authentication instead of XClarity Administrator managed authentication by specifying FALSE in this column. For more information about managed and local authentication, see Managing the authentication server in the XClarity Administrator online documentation.
- (Column AE) You can optionally specify a list of role groups that are permitted to view and manage the device. You can specify only role groups to which the current user belongs.

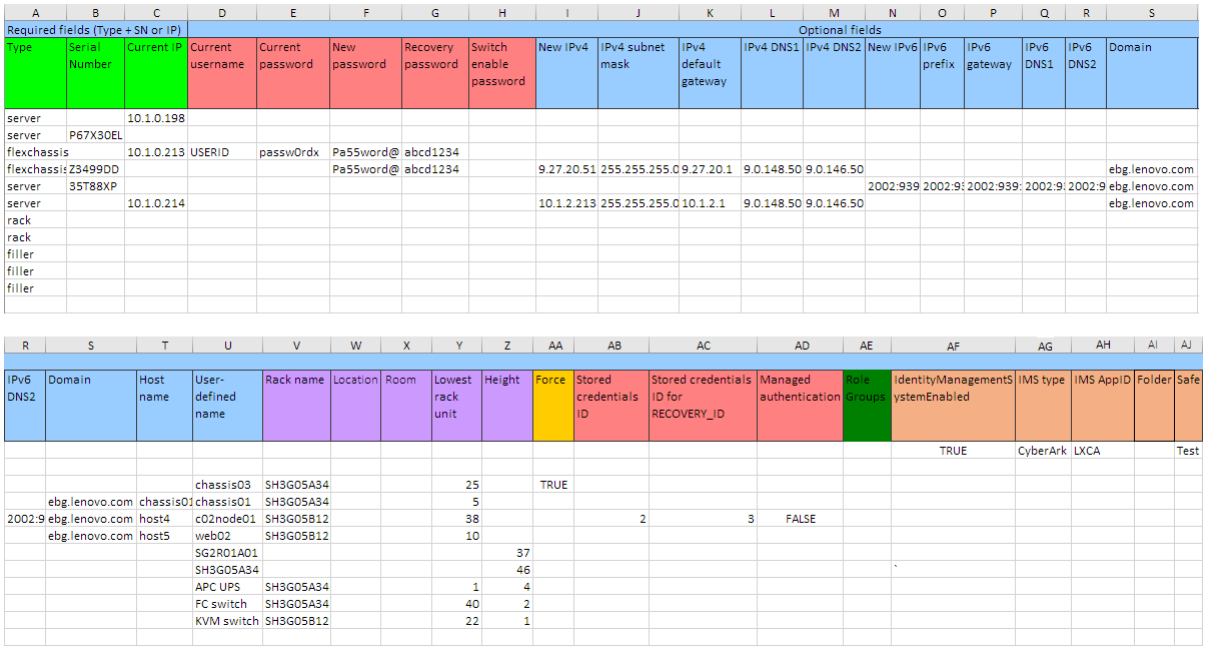
  Note: If you add devices to a managed chassis, the new devices will belong to the same role groups as the chassis.
- (Column AF – AJ) If you choose to use an identity management system instead of manually entered credentials (Columns D – H) or stored credentials (Columns AB), specify IP address or host 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 in the XClarity Administrator online documentation).

  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 in the XClarity Administrator online documentation).

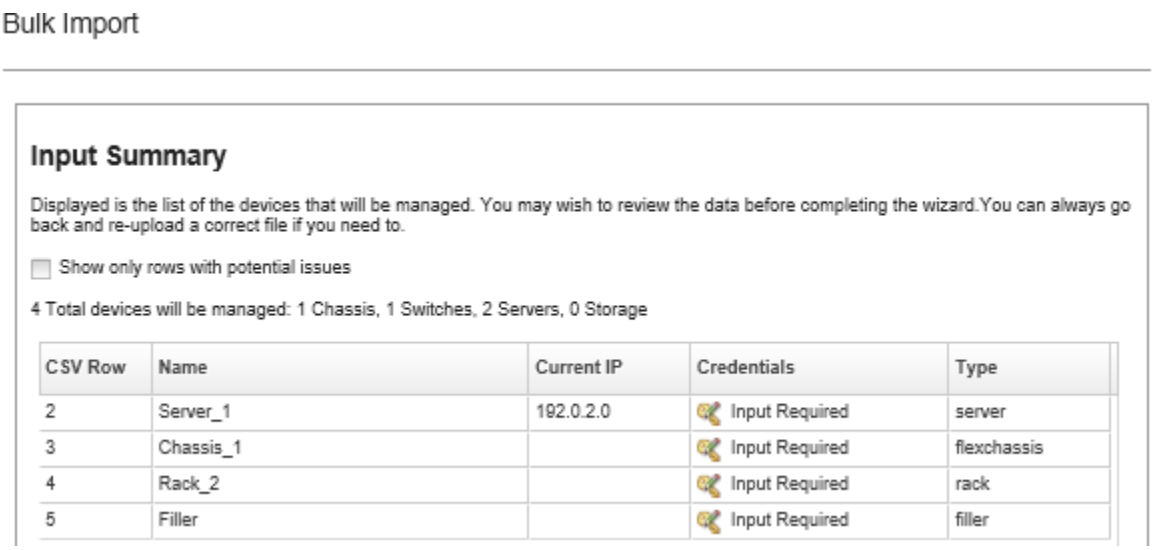
The following figure shows an example bulk-import file:



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Required fields (Type + SN or IP)			Optional fields															
Type	Serial Number	Current IP	Current username	Current password	New password	Recovery password	Switch enable password	New IPv4	IPv4 subnet mask	IPv4 default gateway	IPv4 DNS1	IPv4 DNS2	New IPv6	IPv6 prefix	IPv6 gateway	IPv6 DNS1	IPv6 DNS2	Domain
server		10.1.0.198																
server	P67X3OEL																	
flexchassis		10.1.0.213	USERID	passw0rdx	Pa55word@	abcd1234												
flexchassis	Z3499DD				Pa55word@	abcd1234		9.27.20.51	255.255.255.0	9.27.20.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
server	35T88XP												2002:939	2002:9:	2002:939:	2002:9	2002:9	ebg.lenovo.com
server		10.1.0.214						10.1.2.213	255.255.255.0	10.1.2.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
rack																		
rack																		
filler																		
filler																		
filler																		

R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
IPv6 DNS2	Domain	Host name	User-defined name	Rack name	Location	Room	Lowest rack unit	Height	Force	Stored credentials ID	Stored credentials ID for RECOVERY_ID	Managed authentication	Role Groups	IdentityManagementSystemEnabled	IMS type	IMS AppID	Folder	Safe
														TRUE	CyberArk	LXCA		Test
			chassis03	SH3G05A34			25		TRUE									
	ebg.lenovo.com	chassis01	chassis01	SH3G05A34			5											
2002:9	ebg.lenovo.com	host4	c02node01	SH3G05B12			38			2	3	FALSE						
	ebg.lenovo.com	host5	web02	SH3G05B12			10											
			SG2R01A01					37										
			SH3G05A34					46										
			APC UPS	SH3G05A34			1	4										
			FC switch	SH3G05A34			40	2										
			KVM switch	SH3G05B12			22	1										

6. 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.
7. Click **Upload** to upload and validate the file.
8. Click **Next** to display the Input Summary page with a list of devices to be managed.



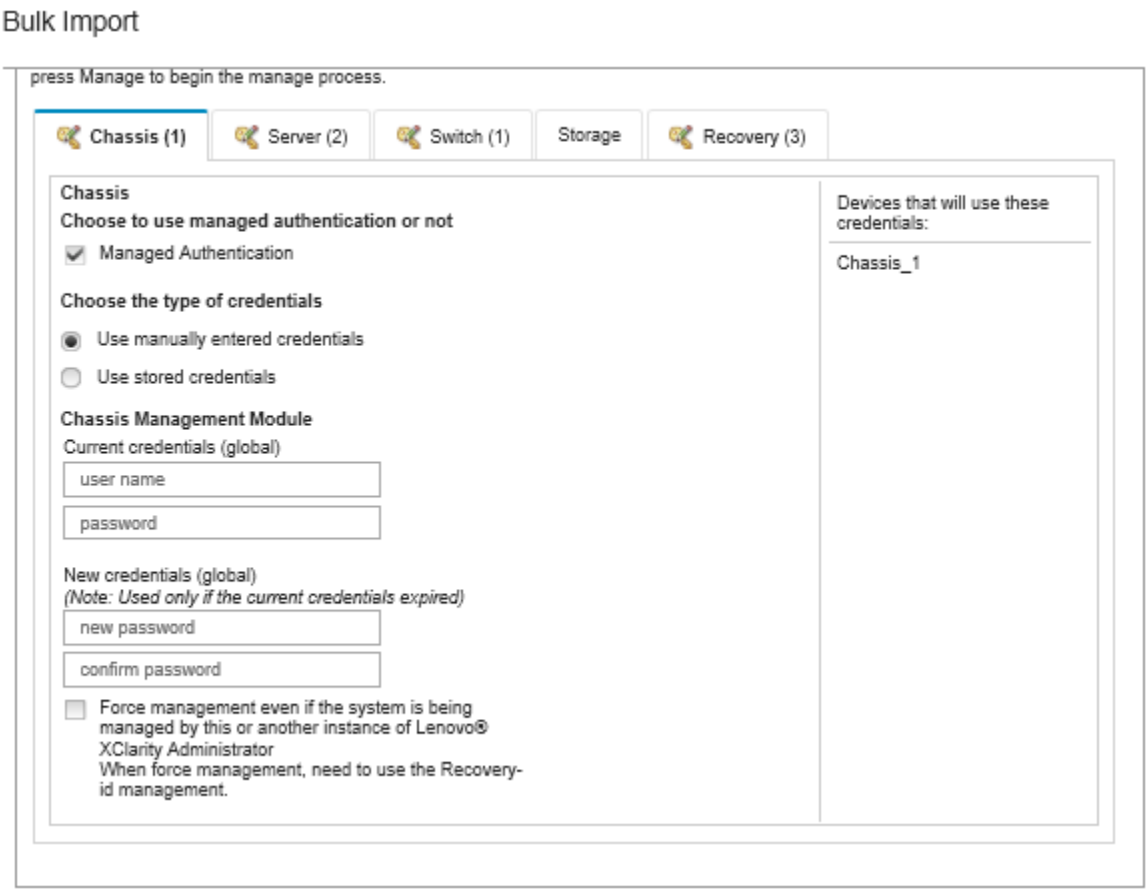
9. Review the summary of devices that you want to manage.

   Select **Show only rows with potential issues** to list row with incomplete data. Fix any issues in the bulk-import file, and then click **Back** to upload the corrected CSV file.

   Notes:

   - If required data is not provided in the bulk-import file, the associated devices are not managed.
   - The Input Summary page flags rows that do not have credential information. If you do not specify credentials in the bulk-import file, the global credentials that you specify in the Bulk Import wizard are used instead.

10. Click **Next** to display the Device Credentials page.



11. **Optional:** 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.

    If you choose to use the global credentials, the credentials for a specific device type must be the same for all devices of the same type that do not have credentials entered in the bulk-import file. For example, CMM credentials must be the same for all chassis, and the storage-management credentials must be the same for all storage devices. If the credentials are not the same, you must enter credentials in the bulk-import file.

    - **Chassis**. Specify the authentication mode and credentials type. Specify current credentials for logging in to all chassis that are defined in the bulk-import file. Specify the new password to use if the current CMM credentials are expired.

      If you force manage a chassis, specify the RECOVERY_ID account and password for the device credentials.
    - **Servers**. Specify the authentication mode and credentials type. Specify current credentials for logging in to all rack and tower servers that are defined in the bulk-import file. Specify new password to use if the current baseboard-management controller credentials are expired.

      If you force manage a server, specify the RECOVERY_ID account and password for the device credentials.
    - **Switches**. Specify the stored credentials for logging in to all RackSwitch switches that are defined in the bulk-import file. If set, also specify the "enable" password that is used to enter Privileged Exec Mode on the switch.
    - **Storage**. Specify current credentials for logging in to all storage devices that are defined in the bulk-import file.

- **Recovery**. Specify recovery password for logging in to all servers and chassis that are defined in the bulk import file.

  You can choose to use a local user account or stored recovery credential. In either case, the user name is always `RECOVERY_ID`.

  When a password is specified, the `RECOVERY_ID` account is created on the device, and all local user accounts are disabled.

  – For chassis, the recovery password is required.
  – For servers, 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.
  – 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.

Information that you specify in the bulk-import file overrides similar information that you specify on the Device Credentials page.

You can optionally choose to force manage each type of device if:

- The devices are currently managed by another management system, such as another XClarity Administrator instance or IBM Flex System Manager
- XClarity Administrator was taken down but the devices were not unmanaged before it went down
- The devices were not unmanaged correctly, and the CIM subscription was not cleared

Note: If the device is managed by another XClarity Administrator instance, the device appears to be managed by the original instance for a period of time after the forced management occurs. You can unmanage the device to remove it from the original XClarity Administrator instance.

12. 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 in the XClarity Administrator online documentation.

    If XClarity Administrator cannot log in to a device using the credentials that are specified in the bulk-import file or the global credentials that are specified in the dialog, the management of that device fails, and XClarity Administrator moves on to the next device in the bulk-import file.

    Notes: 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.

13. If the bulk-import file includes a new chassis, validate and change management network settings for the entire chassis (including compute nodes and Flex switches) and 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 the XClarity Administrator in the XClarity Administrator online documentation.

After you finish

After managing your systems, you can perform the following actions:

- Discover and manage additional systems (see Managing chassis, Managing racks, Managing servers, Managing storage devices, and Managing switches in the Lenovo XClarity Administrator online documentation).
- Configure the system information, local storage, I/O adapters, boot settings, and firmware settings by creating and deploying server patterns (see Configuring servers using the XClarity Administrator in the Lenovo XClarity Administrator online documentation).
- Deploy operating-system images to the servers that do not already have an operating system installed (see Deploying an operating system image in the XClarity Administrator online documentation).
- Update firmware on devices that are not in compliance with current policies (see Updating firmware on managed devices in the XClarity Administrator online documentation).
- Add the newly managed systems to the appropriate rack to reflect the physical environment (see Managing racks in the XClarity Administrator online documentation).
- Monitor hardware status and details (see Viewing the status of a managed server in the XClarity Administrator online documentation).
- Monitor events and alerts (see Working with events and Working with alerts in the XClarity Administrator online documentation).
- 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. 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.

Chapter 5. Registering XClarity Administrator

By registering your instance of Lenovo XClarity Administrator, you can use the basic features without receiving reoccurring warnings about the trial expiration and non-compliant licenses. After registering, the noncompliant-license warning is no longer displayed; however, all functions that require a license remain disabled until you purchase and install licenses based on the number of managed devices.

About this task

Registering your XClarity Administrator instance does not require sharing your contact information. Lenovo does not share the provided information with other external entities.

If you have installed licenses for advanced functions, you do not need to register your XClarity Administrator instance. For more information about licenses and advanced function, see Installing the full-function enablement license.

Procedure

To register XClarity Administrator, complete the following steps.

- If XClarity Administrator is connected to the Internet
  1. From the Lenovo XClarity Administrator menu bar, click **Administration → Registration** to display the Registration page.
  2. Click **Register** to register a new instance of XClarity Administrator.
  3. Fill in the company name, the number of devices to be managed by XClarity Administrator, and the country in which XClarity Administrator is located.
  4. Click **Submit**.
- If XClarity Administrator is not connected to the Internet
  1. Register XClarity Administrator.
     a. In a web browser, open the Lenovo XClarity Registration web portal.
     b. Fill in the company name, the number of devices to be managed by XClarity Administrator, and the country in which XClarity Administrator is located.
     c. Click **Submit** to receive a registration token.
  2. From the Lenovo XClarity Administrator menu bar, click **Administration → Registration** to display the Registration page.
  3. Click **Import** to import the registration token.
  4. Fill in the registration token that you received in step 1.
  5. Click **Submit**.

© Copyright Lenovo 2017, 2023

Chapter 6. Installing the full-function enablement license

After the 90-day free trial expires, you must purchase and install Lenovo XClarity Pro licenses for all managed devices that support advanced functions to continue using operating-system deployment and device-configuration features in Lenovo XClarity Administrator. You must have Lenovo XClarity Pro licenses for *all* managed devices to get XClarity Administrator service and support.

Learn more: XClarity Administrator: Installing the license

Before you begin

Review the following license considerations.

- A license *is not* tied to a specific device.
- A chassis license provides licenses for 14 devices.
- For System x3850 X6 (6241) scalable complex servers, each server needs a separate license, regardless of partitions.
- For System x3950 X6 (6241) scalable complex servers, if not partitioned, each server needs a separate license. If partitioned, each partition needs a separate license.
- The following devices *do not support* advanced functions and therefore *do not require* licenses for these features; however, a license must be purchased for each of these devices to get XClarity Administrator service and support.
  - ThinkServer servers
  - System x M4 servers
  - System x X5 servers
  - System x3850 X6 and x3950 X6 (3837) servers
  - Storage devices
  - Switches

You must have **lxc-supervisor** or **lxc-security-admin** privileges to install licenses.

About this task

XClarity Administrator supports the following license.

- **Lenovo XClarity Pro**. Each license provides the following entitlements for a single device.
  - Service and support for Lenovo XClarity Integrator
  - Service and support for XClarity Administrator
  - Advanced functions within XClarity Administrator:
    - Configuring servers using Configuration Patterns
    - Deploying operating systems
    - Reporting XClarity Administrator problems using Call Home (Call Home for hardware alerts is not affected.)

The activation period for the license starts when the license is purchased and the authorization code is created.

License compliance is determined based on the number of managed devices that support the advanced functions. The number of managed devices must not exceed the total number of licenses in all active license keys. If XClarity Administrator is not in compliance with the installed licenses (for example, if licenses expire

© Copyright Lenovo 2017, 2023

or if managing additional devices exceeds the total number of active licenses), you have a grace period of 90 days to install appropriate licenses. Each time XClarity Administrator becomes non-compliant, the grace period resets to 90 days. If the grace period (including the free trial) ends before licenses are compliant, advanced functions are disabled for all devices.

For example, if you manage an additional 100 ThinkSystem servers and 20 rack switches in an existing XClarity Administrator instance, you have 90 days to purchase and install 100 additional licenses before advanced functions are disabled in the user interface (for all devices). Licenses for the 20 rack switches are not needed to use the advanced functions; however, they are needed if you want service and support. If advanced functions are disabled, the advanced functions are re-enabled after you install enough licenses to be back in compliance.

If you are using a free trial license or you have a grace period to become compliant, and you upgrade to a later version of XClarity Administrator, the trial license or grace period resets to 90 days.

Notes:

- Server configuration and operating-system deployment features are disabled when the grace period expires.
- Call Home for XClarity Administrator issues (software Call Home feature) is disabled when licenses are out of compliance. There is no grace period for this feature. However, Call Home for hardware alerts is not affected.

If licenses are already installed, new licenses are *not* required when upgrading to a new release of XClarity Administrator.

You can determine the license status, including the number of days are left in the trial license, by clicking the user-actions menu (

) on the XClarity Administrator title bar, and then clicking **About**.

Getting help

- If you have issues and you used a Business Partner, contact your Business Partner to verify the transaction and entitlement.
- If you did not receive your electronic proof of entitlement, authorization codes, or activation keys, or if they were sent to wrong person, contact one of the regional representatives, based on your geography.
  - ESDNA@lenovo.com (North American countries)
  - ESDAP@lenovo.com (Asia Pacific countries)
  - ESDEMEA@lenovo.com (European, Middle Eastern, and Asian countries)
  - ESDLA@lenovo.com (Latin American countries)
  - ESDChina@Lenovo.com (China)
- If information about my entitlement is not correct, contact Lenovo Support at SW_override@lenovo.com and include the following information:
  - Order number
  - Your contact information, including email address.
  - Your physical address
  - Changes that you want made
- If you have issues or questions about downloading the license, contact Lenovo Support at -eSupport_-_Ops@lenovo.com.

Installing full-function enablement licenses using the XClarity Administrator web interface

If XClarity Administrator has access to the Internet, you can use the XClarity Administrator web interface to redeem and retrieve licenses for existing authorization, and then import and install the redeemed licenses.

Before you begin

Contact your Lenovo representative or authorized Business Partner to purchase Lenovo XClarity Pro licenses based on the functions that you want to enable and the number of devices that you want to manage. After purchasing licenses, an authorization code is sent to you in an *electronic proof of entitlement* email. The authorization code is a 22-character alphanumeric string, which you need to redeem and install the licenses. If you do not receive the email and you purchased licenses through a Business Partner, contact your Business Partner to request the authorization code.

You can also retrieve your authorization codes from the Features on Demand web portal by clicking **Retrieve authorization code**.

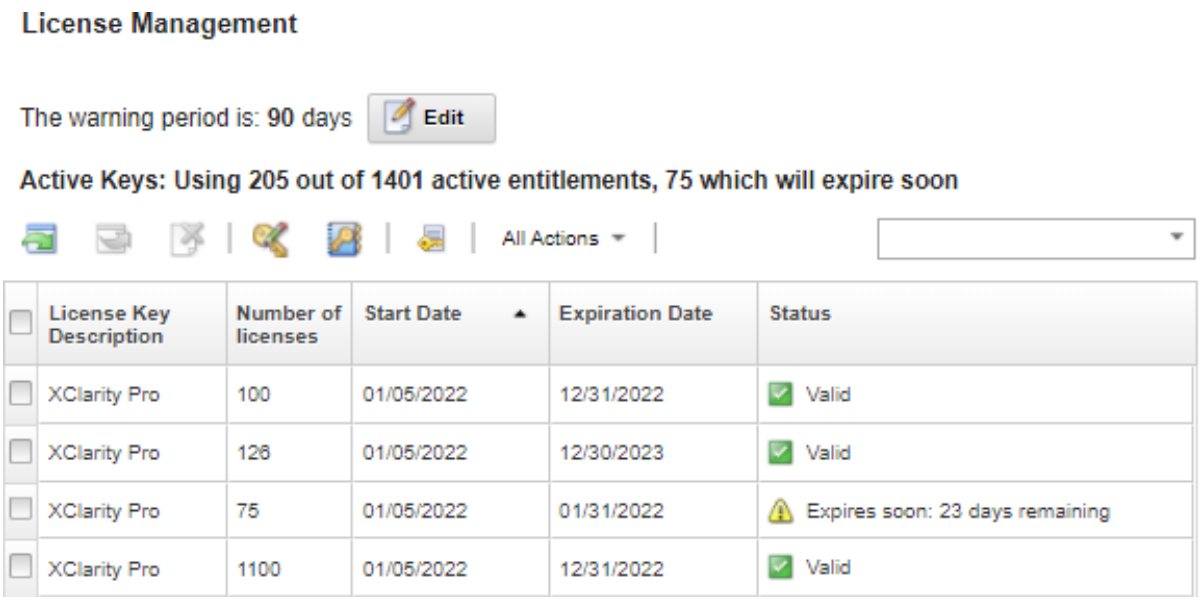
Procedure

To install Lenovo XClarity Pro licenses in the management server, complete one of the following procedures.

- **Redeem and install all or a subset of remaining licenses from a single authorization code**

  You can redeem all or a subset of available licenses for a single authorization code to create a license-activation key, which is a file that contains each information about redeemed license. You can then install the redeemed licenses using that license-activation key file.

  1. From the XClarity Administrator menu bar, click **Administration → Licenses** to display the License Management page.



  2. Click the **Request Activation Key** icon ( ) to display the Request Activation Key dialog.
  3. Click **Single Authorization Code**.
  4. Enter the 22-character authorization code, and click **Search** to fetch information about the purchased licenses for the specified authorization code from the Features on Demand website.

     If the authorization code that you received is not accepted, contact Lenovo Support.
  5. Enter your 10-digit Lenovo customer number in the **Lenovo Customer Number** field.
  6. Enter the number of licenses that you want to redeem in the **Redeem Quantity** field, and then click **Continue**.

     To redeem all the available licenses in the authorization code, match the number in **Available licenses** field.

If you redeem a subset of available licenses, you can redeem the remaining licenses later using the same authorization code.

Tip: Each XClarity Administrator supports up to 1,000 managed devices. Therefore, a single license-activation key that you can install in an XClarity Administrator instance cannot have more than 1,000 licenses.

7. Review the contact information for accuracy and make modifications if needed.
8. Click **Submit request** to redeem the licenses and create the license-activation key.
9. Select the license-activation key that contains the licenses to install.
10. Click **Install** to install the licenses in the management server.
11. Click **Close**.

- **Redeem and install all remaining licenses from multiple authorization codes**

  You can redeem all remaining licenses for multiple authorization codes. A license-activation key is created for each authorization code. You can then install the redeemed licenses using the license-activation keys. The authorization codes must be provided in a CSV-formatted file, using the provided template.

  1. From the XClarity Administrator menu bar, click **Administration → Licenses** to display the License Management page.
  2. Click the **Request Activation Key** icon ( ) to display the Request Activation Key dialog.
  3. Click **Multiple Authorization Codes**.
  4. Click the **Download Template** link to open an Excel file. Add each authorization code to the file, and save the file in CSV format to your local system.
  5. Click **Browse** to find and select the authorization-code CSV file, and then click **Search** to fetch information about the authorization code from the Lenovo Support website.
  6. Review the information about the purchased license and available license-activation keys that are associated with each authorization code.
  7. Enter your 10-digit Lenovo customer number in the **Lenovo Customer Number** field.
  8. Review the contact information for accuracy and make modifications if needed. Then, click **Continue**.
  9. Select **Yes, I'd like to redeem all valid authorization codes**, and then click **Submit request** to generate the license-activation keys.
  10. Select the license-activation keys that you want to install.
  11. Click **Install** to install the license-activation keys in the management server.
  12. Click **Close**.

- **Retrieve and install redeemed licenses**

  You can download license-activation keys to the local system from an XClarity Administrator instance that has access to the Features on Demand web portal, and then import and install those license-activation keys in another XClarity Administrator instance. This is useful when you want to install licenses on an XClarity Administrator instance that does not have Internet access or when you reinstalled XClarity Administrator and need to restore installed licenses.

  1. From the XClarity Administrator menu bar, click **Administration → Licenses** to display the License Management page.
  2. Click the **Retrieve History** icon ( ) to display the Retrieve History dialog.
  3. Enter your Lenovo customer number or 22-character authorization code.
  4. Click **Search** to retrieve information about available and redeemed licenses.

     If the authorization code that you received is not accepted, contact Lenovo Support.

5. Select the license-key files that you want to install.
6. Click **Install** to install the license-activation keys in XClarity Administrator.
7. Click **Close**.

- **Import and install redeemed licenses on another XClarity Administrator instance**

  If you redeemed licenses using one XClarity Administrator instances and want to install those licenses on another XClarity Administrator instance or if an error condition occurs that requires you to restore installed licenses, you can import the license-key file from the local system to the other XClarity Administrator instance.

  1. From an XClarity Administrator instance that has access to the Features on Demand web portal, retrieve license-activation keys from Features on Demand web portal and then save the license-activation keys as a file on your local system.
     a. From the XClarity Administrator menu bar, click **Administration → Licenses** to display the License Management page.
     b. Click the **Retrieve History** icon ( ) to display the Retrieve History dialog.
     c. Enter the 22-character authorization code.
     d. Click **Search** to retrieve information about available and redeemed licenses for that authorization code.

        If the authorization code that you received is not accepted, contact Lenovo Support.
     e. Select the license-activation keys files that you want to install.
     f. Click **Download** to save the license-key files to the local system.
  2. From the XClarity Administrator instance on which you want to install license-activation keys:
     a. From the XClarity Administrator menu bar, click **Administration → Licenses** to display the License Management page.
     b. Click the **Import and Apply** icon ( ) to import and install the licenses.
     c. Click **Browse** to select the license-activation keys for the licenses that you want to install.

        To import multiple license-activation keys, compress the .KEY files into a ZIP file, and select the ZIP file for import.
     d. Click **Accept License** to import and apply the licenses.

        When the installation is complete, the license-activation keys are listed in the table with the number of installed licenses and the activation period (start and expiration dates).

After you finish

You can perform the following actions from the Licenses page.

- Download one or more specific license-activation keys to the local system by clicking the **Export** icon ( ).

  Note: When you export multiple license-activation keys, the files are downloaded as a single ZIP file.
- Delete a specific license-activation keys by clicking the **Delete** icon ( ).
- Configure the license-warning period by clicking the **Edit** button at the top of the page. The license-warning period is the number of days before licenses expire when XClarity Administrator triggers a warning.

Getting help

- If you have issues and you used a Business Partner, contact your Business Partner to verify the transaction and entitlement.
- If you did not receive your electronic proof of entitlement, authorization codes, or activation keys, or if they were sent to wrong person, contact one of the regional representatives, based on your geography.
  - ESDNA@lenovo.com (North American countries)
  - ESDAP@lenovo.com (Asia Pacific countries)
  - ESDEMEA@lenovo.com (European, Middle Eastern, and Asian countries)
  - ESDLA@lenovo.com (Latin American countries)
  - ESDChina@Lenovo.com (China)
- If information about my entitlement is not correct, contact Lenovo Support at SW_override@lenovo.com and include the following information:
  - Order number
  - Your contact information, including email address.
  - Your physical address
  - Changes that you want made
- If you have issues or questions about downloading the license, contact Lenovo Support at -eSupport_-_Ops@lenovo.com.

Installing full-function enablement licenses using the Features on Demand web portal

If XClarity Administrator *does not* have access to the Internet, you can redeem and retrieve licenses for existing authorization codes using the Features on Demand web portal from another system that has network access to the XClarity Administrator. You can then use the XClarity Administrator web interface to import and install the redeemed licenses.

Procedure

To install Lenovo XClarity Pro licenses in the management server, complete the following steps.

Step 1. Purchase a Lenovo XClarity Pro license for each managed device.

Contact your Lenovo representative or authorized Business Partner to purchase Lenovo XClarity Pro licenses based on the functions that you want to enable and the number of devices that you want to manage. After purchasing licenses, an authorization code is sent to you in an *electronic proof of entitlement* email. The authorization code is a 22-character alphanumeric string, which you need to redeem and install the licenses. If you do not receive the email and you purchased licenses through a Business Partner, contact your Business Partner to request the authorization code.

You can also retrieve your authorization codes from the Features on Demand web portal by clicking **Retrieve authorization code**.

Step 2. Redeem all or a subset of licenses using the authorization code. When licenses are redeemed, a license-activation key file is generated.

1. Open the Features on Demand web portal from a web browser, and log in to the portal using your email address as your user ID.
2. Click **Request activation key**.
3. Select **Input a Single Authorization Code**.
4. Enter the 22-character authorization code, and click **Continue**.
5. Enter your Lenovo customer number in the **Lenovo Customer Number** field.
6. Enter the number of licenses that you want to redeem in the **Redeem Quantity** field, and then click **Continue**.

To redeem all the available licenses in this authorization code, match the number in **Available licenses** field.

If you redeem a subset of available licenses, you can redeem the remaining licenses in another license-activation key using the same authorization code.

Tip: Each XClarity Administrator supports up to 1,000 managed devices. Therefore, a single license-activation key that you install in an XClarity Administrator instance should not have more than 1,000 licenses.

7. Follow the prompts to enter product details and contact information, and click **Continue** to generate the license-activation key.
8. Optionally specify additional recipients to receive the license-activation keys.
9. Click **Submit** to send the license-activation keys.

   The person assigned to the purchase order and the additional recipients will receive an email with the license-activation key. The key is a file in .KEY format.

   Note: You can also download license-activation keys (individually or in batch) from the Features on Demand web portal by clicking **Retrieve History** and using your Lenovo customer number to find your of license-activation keys, and then download all or a subset of keys. Then, click **Email** to email the keys to you, or click **Download** to download the keys to your local system.

Step 3. Import and install the licenses in XClarity Administrator.

1. From the XClarity Administrator menu bar, click **Administration → Licenses** to display the License Management page.
2. Click the **Import and Apply** icon ( ) to install the licenses.
3. Click **Browse** to select the license-activation key file for the licenses that you want to install.

   Tip: To import multiple license-activation key, compress the .KEY files into a ZIP file, and select the ZIP file for import.
4. Click **Accept License** to import and apply the licenses.

   When the installation is complete, the license-activation key is listed in the table with the number of installed licenses and the activation period (start and expiration dates).

After you finish

You can perform the following actions from the Licenses page.

- Download one or more specific license-activation keys to the local system by clicking the **Export** icon ( ).

  Note: When you export multiple license-activation keys, the files are downloaded as a single ZIP file.
- Delete a specific license-activation keys by clicking the **Delete** icon ( ).
- Configure the license-warning period by clicking the **Edit** button at the top of the page. The license-warning period is the number of days before licenses expire when XClarity Administrator triggers a warning.

Getting help

- If you have issues and you used a Business Partner, contact your Business Partner to verify the transaction and entitlement.

- If you did not receive your electronic proof of entitlement, authorization codes, or activation keys, or if they were sent to wrong person, contact one of the regional representatives, based on your geography.
  - ESDNA@lenovo.com (North American countries)
  - ESDAP@lenovo.com (Asia Pacific countries)
  - ESDEMEA@lenovo.com (European, Middle Eastern, and Asian countries)
  - ESDLA@lenovo.com (Latin American countries)
  - ESDChina@Lenovo.com (China)
- If information about my entitlement is not correct, contact Lenovo Support at SW_override@lenovo.com and include the following information:
  - Order number
  - Your contact information, including email address.
  - Your physical address
  - Changes that you want made
- If you have issues or questions about downloading the license, contact Lenovo Support at -eSupport_-_Ops@lenovo.com.

Chapter 7. Updating XClarity Administrator

You can update the Lenovo XClarity Administrator virtual appliances to install the latest software.

Before you begin

Learn more: XClarity Administrator: Fix pack update

For all Electronic Customer Care (ECC) connections that are configured for a proxy, the proxy must be a forwarding proxy and must not terminate the connection. The call home and updates functions of XClarity Administrator use the ECC connections.

Notes:

- To manage XClarity Administrator v4.0 or later instances using Lenovo XClarity Orchestrator, XClarity Orchestrator v2.0 or later is required. If you are updating XClarity Administrator to v4.0 or later, ensure that XClarity Orchestrator is already at v2.0 or later.
- XClarity Administrator cPlus edition supports additional devices requested by China customers. You can apply XClarity Administrator cPlus edition to XClarity Administrator v3.5 or later. Before applying the XClarity Administrator cPlus edition patch, you must enable a global setting.
  1. From the XClarity Administrator main menu, click **Administration → Update Management Server** to display the Management Server Update page.
  2. Click **All Actions → Global Settings** to display the Global Settings: Update Management Server dialog.
  3. Select **Enable update to XClarity Administrator cPlus**.

  Attention:

  – XClarity Administrator cPlus edition *cannot* be uninstalled. To revert to XClarity Administrator (without the cPlus features), you must reinstall XClarity Administrator.

  – After applying the XClarity Administrator cPlus edition patch, you can only apply future XClarity Administrator cPlus patches. You cannot apply an XClarity Administrator patch without cPlus features.

  For more information about XClarity Administrator cPlus, see the XClarity Administrator cPlus online documentation.
- When you update XClarity Administrator, some predefined device drivers and boot files might also be updated. Any customized OS-image profiles that use those files are automatically updated to include the new files. For more information about customized OS-image profiles, see Customizing OS-image profiles in the XClarity Administrator online documentation.
- Management server updates (patches) without payloads that are earlier than the currently installed version are not listed in the table on the Management Server Update page. Patches with payloads that are earlier than the currently installed version are listed in the table with an applied status of **Not applicable** and cannot be applied to the management server.
- All repository packs (with or without payloads) are listed in the table on the Management Server Update page.
- Only stored credentials can be used to authenticate to ThinkServer server, System x M4 servers, and RackSwitch devices. Manual user accounts are not supported.
- When Call Home is enabled, service requests are first routed to the Lenovo Support, and then forwarded to IBM, if appropriate for certain devices.

© Copyright Lenovo 2017, 2023

About this task

XClarity Administrator supports the following types of updates:

- **Patch**. XClarity Administrator code changes, including new releases and fix packs.
- **Supplemental Packs**. Firmware-update repository packs, which contain firmware update packages for all manageable devices. When imported and applied, the firmware updates are added in the firmware-updates repository (see Downloading firmware updates in the XClarity Administrator online documentation).

Before you can update the XClarity Administrator management server, you must first check for available updates and then download the update package. When you download management-server updates, XClarity Administrator downloads the selected update package from the web and stores the update packages in the management-server updates repository.

To check for and download management-server updates, XClarity Administrator must be connected to the Internet. If it is not connected to the Internet, you can manually download the management-server updates from the XClarity Administrator download webpage using a web browser to a workstation that has network access to the XClarity Administrator host and then import the updates into the management-server updates repository.

You can determine which management-server updates are stored in the updates repository from the **Download Status** column on Update Management Server page. This column can contain the following values:

- **Downloaded**. The firmware-update repository pack or management-server update is stored in the repository.
- **Not downloaded**. The firmware-update repository pack or management-server update is available but not stored in the repository.
- **Cleaned up**. The update was successfully applied, and unneeded staging files were automatically removed.

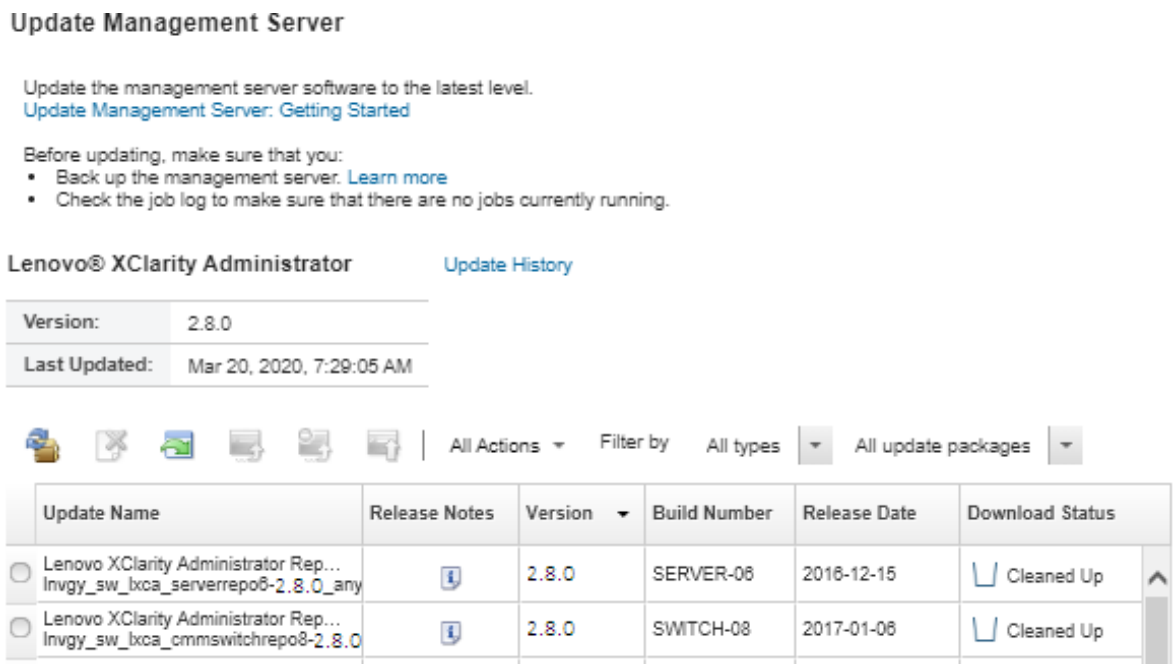
A message is displayed on the page when the repository is more than 50% full. Another message is displayed on the page when the repository is more than 85% full.

Procedure

To update XClarity Administrator, complete the following steps.

Step 1. From the XClarity Administrator main menu, click **Administration → Update Management Server** to display the Management Server Update page.

You can sort the table columns to make it easier to find specific updates. In addition, you can select an update type from the **Filter By Type** drop-down lists to list only those updates that meet the selected criteria.



Recapture in other languages

Step 2. Download the latest XClarity Administrator update:

- If XClarity Administrator is connected to the Internet:
  1. Retrieve information about the latest updates by clicking the **All Actions → Refresh Product Catalog**. New management-server updates and firmware-update repository packs are listed in the table on the Management Server Update page. Refreshing this information might take several minutes to complete.

     Note: Refreshing the product catalog does not automatically download update packages.
  2. Select the management-server update that you want to download.

     Tip: Ensure that the package that you select has Patch in the **Type** column.
  3. Click the **Download** icon ( ). When the download is complete, the **Download Status** for that update changes to “Downloaded.”
- If XClarity Administrator is not connected to the Internet:
  1. Download the management-server update from the XClarity Administrator download webpage to a workstation that has network connection to the XClarity Administrator host.
  2. From the Management Server Update page, click the **Import** icon ( ),
  3. Click **Select Files**, and browse to the location of the management-server update on the workstation.
  4. 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.
  5. Click the **Import**.When the import is complete, the management-server update is listed in the table on the Management Server Update page, and the **Download Status** for that software update is “Downloaded.”

You can monitor the import progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

Step 3. Back up the XClarity Administrator virtual appliance by creating a clone (see Backing up XClarity Administrator in the XClarity Administrator online documentation).

Step 4. Ensure that no jobs are currently running. You can view a list of currently running jobs from the Jobs log (see Monitoring jobs in the XClarity Administrator online documentation).

Step 5. Select the update package that you want to install.

You can sort the table columns to make it easier to find specific update packages. In addition, you can select an update-package type and age from the **Filter by** drop-down lists.

Note: Ensure that **Download Status** is "Downloaded." and the **Type** is "Patch."

Step 6. Click the **Perform Update** icon ( ).

You can monitor the update progress by clicking **Monitoring → Jobs** from the XClarity Administrator menu bar.

Step 7. Wait a few minutes for the update to complete and XClarity Administrator to be restarted.

If you have access to the virtual appliance host, you can monitor the progress from the virtual-appliance console, for example:

```
------------------------------------------------
Lenovo XClarity Administrator - Version 1.1.0
------------------------------------------------

eth0      Link encap:Ethernet  HWaddr 00:00:00:00:00:10
          inet addr:10.240.61.98  Bcase:10.240.63.255  Mask:255.255.252.0
          inet6 addr: fe80:200:ff:fe00:10/64 Scopt:Link

eth1      Disabled

idxhwmgr login: Lenovo XClarity Administrator Repository Update
Detected appliance version is 1.1.0
Applying XClarity Administrator Repository Update...
.
.
.
```

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

Step 8. Determine if the update is complete by refreshing the web browser. When completed, the **Applied Status** column changes to "Applied."

If you applied a management server update, the XClarity Administrator version that is listed above the table on the Update Management Server page changes to the version that was just applied.

Step 9. Clear the web browser cache.

After you finish

From this page, you can perform the following actions:

- View the current version and installed patches for the XClarity Administrator instance by clicking the user-actions menu (

) on the XClarity Administrator title bar, and then clicking **About**.
- View the update history for all updates that have been applied to the XClarity Administrator management server by clicking the **Update History** link.
- View the update history for a specific update that has been applied to the XClarity Administrator management server by clicking the update-status link in the **Applied Status** column.

- Delete only the image or payload file (.zip, .bin, .uxz, or .tgz). Information for a selected management-server update by clicking the **Delete only payload files** icon (. Metadata about the update, remains so that you can easily download the update again.

  Note: When you delete an image or payload, the payload (image and MIB) 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."
- Delete the full update package for a selected management-server update (including the image or payload file, change history file (.chg), readme file (.txt), and metadata file (.xml)) by clicking the **Delete all update-package files** icon ( ).

Chapter 8. Uninstalling XClarity Administrator

Complete these steps to uninstall a Lenovo XClarity Administrator virtual appliance or container.

Procedure

To uninstall the XClarity Administrator virtual appliance, complete the following steps.

Step 1. Unmanage all devices that are currently managed by XClarity Administrator (see Managing chassis, Managing servers, and Managing switches in the XClarity Administrator online documentation).

Step 2. Uninstall XClarity Administrator, depending on the operating system:

- **Docker-compose**

  Run the following command to stop the container and remove the networks and volumes.

  ```
  docker-compose down -v
  ```

- **CentOS, Red Hat,** Rocky, **and Ubuntu**
  1. Connect to the host using the Virtual Machine Manager.
  2. Right-click the virtual machine, and click **Shut Down → Force off**.
  3. Right-click the virtual machine again, and click **Delete**. The Delete confirmation dialog box is displayed.
  4. Select all check boxes, and click **Delete**.
- **ESXi**
  1. Connect to the host through the VMware vSphere Client.
  2. Right-click the virtual machine, and click **Power → Power Off**.
  3. Right-click the virtual machine again, and click **Delete from Disk**.
- **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 **Shut down**.
  4. Right-click the virtual machine again, and click **Delete**.

© Copyright Lenovo 2017, 2023

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.