



Lenovo ThinkAgile
SXM Series
Administrator's Guide



Notices

Note

Before using this information and the product it supports, be sure to read and understand the safety information and the safety instructions, which are available at the following address:

https://pubs.lenovo.com/safety_documentation/pdf_files

In addition, be sure that you are familiar with the terms and conditions of the Lenovo warranty for your solution, which can be found at the following address:

<http://datacentersupport.lenovo.com/warrantylookup>

Sixth Edition (November 2023)

© Copyright Lenovo 2017, 2023.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to 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
---------------------------	----------

Figuresiii
--------------------------	-------------

Tables	v
-------------------------	----------

Chapter 1. Administering ThinkAgile SXM Series solutions	1
---	----------

ThinkAgile SXM Administration considerations.	1
---	---

Chapter 2. Product management and changes	3
--	----------

Standard management	3
-------------------------------	---

Managing IDs and passwords	4
--------------------------------------	---

Chapter 3. Updating ThinkAgile SXM Series solution firmware	5
--	----------

Firmware maintenance and Best Recipe	5
--	---

Prerequisites	5
-------------------------	---

Preparing to update ThinkAgile SXM firmware	5
---	---

Configure XClarity Administrator for a specific Best Recipe	6
---	---

Update XClarity Administrator	6
---	---

Import firmware update packages	9
---	---

Import firmware compliance policy	11
---	----

Assign firmware compliance policy	13
---	----

Update the ThinkAgile SXM OEM Extension Package.	15
--	----

Prerequisites	16
-------------------------	----

Provide LXCA details to Azure Stack Hub	16
---	----

Determine current versions	18
--------------------------------------	----

Create the update storage container	18
---	----

Upload the OEM Extension Package.	20
---	----

Perform the update	22
------------------------------	----

Verify the update and Azure Stack Hub functionality	24
---	----

Update the ThinkAgile SXM switch firmware (Lenovo switches only)	24
--	----

Prerequisites	25
-------------------------	----

Prepare XClarity Administrator to update switch firmware	25
--	----

Update Lenovo TOR switch firmware	26
---	----

Update Lenovo BMC switch firmware	40
---	----

Fallback	51
--------------------	----

Updated CNOS command syntax	52
---------------------------------------	----

Chapter 4. Component service and replacement considerations	53
--	-----------

Replacing servers	53
-----------------------------	----

Replacing server parts	54
----------------------------------	----

Appendix A. XClarity Administrator deployment and configuration	55
--	-----------

Retire the current LXCA installation	55
--	----

Deploy and configure LXCA	60
-------------------------------------	----

Configure LXCA static IP address	63
--	----

Read and Accept Lenovo XClarity Administrator License Agreement task	66
--	----

Create User Account task	67
------------------------------------	----

Configure Network Access task	70
---	----

Configure Date and Time Preferences task	74
--	----

Configure Service and Support Settings task	75
---	----

Configure Additional Security Settings task	79
---	----

Start Managing Systems task	80
---------------------------------------	----

Apply LXCA Pro license.	81
---------------------------------	----

Apply LXCA update package	81
-------------------------------------	----

Manage the nodes.	84
---------------------------	----

Import and apply server pattern	87
---	----

Appendix B. Updating ThinkAgile SXM Series switches using the CLI (Lenovo switches only)	91
---	-----------

Prerequisites	91
-------------------------	----

Prepare switch image files.	91
-------------------------------------	----

Verify Azure Stack Hub health	93
---	----

Updating Lenovo TOR switch firmware using the CLI.	93
--	----

Back up TOR switch configurations	93
---	----

Update CNOS on TOR switches using the CLI	94
---	----

Updating BMC switch firmware using the CLI	97
--	----

Back up BMC switch configuration	97
--	----

Update the BMC switch using the CLI	97
---	----

Figures

1.	Administration menu → Update Management Server	7	40.	PuTTY security alert	34
2.	Upload LXCA update package	7	41.	Checking Azure Stack Hub Administrator Portal for alerts	39
3.	Perform management server update	8	42.	Verifying that TOR switch firmware updates are complete	40
4.	Restart message after XClarity Administrator update	8	43.	Selecting BMC switch for configuration backup	41
5.	XClarity Administrator update request message	9	44.	Verifying and commenting BMC switch for backup	41
6.	XClarity Administrator firmware update repository	9	45.	Selecting the configuration file backup for download	42
7.	Selecting files for import	10	46.	Selecting BMC update and activation rules	43
8.	Firmware import status	10	47.	Following BMC update progress on Jobs Page	44
9.	Product Catalog showing new updates	11	48.	Verifying new BMC firmware running in active image	45
10.	Firmware Updates: Compliance Policies window	12	49.	LXCA IPv4 settings to record	56
11.	Import firmware compliance policy	12	50.	Selecting LXCA server profiles to deactivate	57
12.	Imported firmware compliance policy	13	51.	Resetting BMC identity settings	58
13.	Firmware Updates: Apply/Activate window	13	52.	Unmanaging the nodes	59
14.	Global Settings: Firmware Updates window	14	53.	Selecting option to force unmanage nodes	60
15.	Firmware compliance policy showing noncompliant nodes	15	54.	Virtual Machine Connection window	64
16.	Credentials that are used to log in to LXCA	17	55.	Virtual machine parameters	65
17.	Checking current running Azure Stack Hub versions	18	56.	LXCA Initial Setup page	66
18.	Navigating to the updateadminaccount storage container	19	57.	Read and Accept Lenovo XClarity Administrator License Agreement task window	67
19.	Navigating to the Blobs storage container	19	58.	Create New Supervisor User window	68
20.	Creating the new container	20	59.	Local User Management window	69
21.	Selecting the storage container for upload	20	60.	Local User Management window with backup user	70
22.	Selecting the Upload control	21	61.	Edit Network Access window	71
23.	Selecting the update package files for upload	21	62.	DNS & Proxy settings tab	72
24.	Uploading the update package files	22	63.	Disabling IPv6 settings	73
25.	Verifying uploads completed successfully	22	64.	Saving IP Settings tab changes	73
26.	Initiating the update	23	65.	Initial Setup page with completed tasks checked	74
27.	Update progress indicators	23	66.	Edit Date and Time window	75
28.	Installation details	24	67.	Service and Support Periodic Data Upload tab	76
29.		26	68.	Service and Support Call Home Configuration tab	76
30.	Verifying Azure Stack Hub health before update	26	69.	Service and Support Lenovo Upload Facility tab	77
31.	Selecting both TOR switches	27	70.	Service and Support Warranty tab	78
32.	Backing up TOR configuration file	27	71.	Service Recovery Password page	79
33.	Backup configuration file dialog box	28	72.	Initial Setup window with one task remaining	80
34.	Backup configuration file results	28	73.	Selecting No, don't include Demo Data in Start Managing Systems window	80
35.	Selecting backup configuration file to download to local PC	29	74.	License Management page with valid LXCA Pro license shown	81
36.	Selecting TOR1 switch for update	30	75.	Selecting LXCA FixPack files	82
37.	Selecting options in the TOR1 Update Summary	31			
38.	Update progress on Jobs Page	32			
39.	Active and standby images	33			

76. Selecting the update package and performing update	83	86. Deploy pattern with full activation	89
77. Update package final statuses.	83	87. Jump to Profiles control	89
78. Four nodes selected to be managed	84	88. Server profiles with Active status	90
79. Manage stored credentials	85	89. Broadwell-based ThinkAgile SXM switch firmware update packages	92
80. Create a new stored credential.	85	90. Switch firmware update archive contents	92
81. Selecting new stored credential for management	86	91. ThinkAgile SXM switch firmware IMGs image files	93
82. Establishing management connections with each XClarity controller	86	92. Verifying Azure Stack Hub health.	93
83. View All Servers	87	93. Checking Azure Stack Hub Administrator Portal for alerts	96
84. Inventory collection completed	87		
85. Deploying a pattern	88		



Tables

Chapter 1. Administering ThinkAgile SXM Series solutions

This documentation refers to the following products:

- SXM4400
- SXM6400
- SXM4600

ThinkAgile SXM Administration considerations

The following considerations and limitations apply to ThinkAgile SXM solutions.

Limitation on automated service requests (Call Home)

Because ThinkAgile SXM products are serviced and supported at the rack level, it is recommended that you not activate Call Home functionality for the components. If you choose to activate Call Home, be aware that your entitlement might not be recognized.

Firmware and Best Recipe adherence

Lenovo publishes a ThinkAgile SXM firmware “Best Recipe”, which identifies the supported levels for the various components. Any specific firmware that is above or below the level indicated in the Best Recipe is not supported and might impact Lenovo’s ability to support any issues with the relevant component. See [“Firmware maintenance and Best Recipe” on page 5](#) for more details.

ThinkAgile SXM entitlement

ThinkAgile SXM solutions are entitled at the rack level.

If you need support for the product or any of its components or included software, be sure to use your rack serial number associated with Machine Type 9565. If you use the component or software serial number, ThinkAgile Advantage Support might not immediately recognize the correct entitlement, which could delay proper case handling. You can find the serial number on the rack label.

Chapter 2. Product management and changes

Because of the complexity of ThinkAgile SXM Series solutions, extra caution and planning should be exercised before making certain changes.

High impact changes

The following changes (or lack of adherence) can significantly impact the functionality of the solution.

- Changing the point-to-point cabling from the initial configuration.
- Changing any firmware, software, or operating system (including CNOS, ENOS and Cumulus Linux) to levels outside the Best Recipe.

See “[Firmware maintenance and Best Recipe](#)” on page 5 for more information.

- Changing the IPv4 network scheme, such as addresses and subnets.
- Changing the IPv4 addresses for servers or switches.
- Updating the management stack outside of the recommended levels.
- Resetting the IMM, XCC or UEFI to the initial manufacturing defaults.
- Resetting a network switch to its initial configuration.

Standard management

After the initial ThinkAgile SXM Series solution setup and configuration by Lenovo Professional Services, you should be able to manage the system routinely with the following software.

Lenovo XClarity Administrator

Use [Lenovo XClarity Administrator](#) to monitor and manage the hardware. Typical uses include the following:

- UEFI settings (per the ThinkAgile SXM pattern file)
- Firmware and device driver updates (per the ThinkAgile SXM Best Recipe) via the Microsoft Azure Stack Hub patch and update process
- Hardware alerts and problem resolution

See https://pubs.lenovo.com/thinkagile-sxm/printable_doc for relevant links.

Microsoft Azure Stack Hub portals

Microsoft Azure Stack Hub enables management via the following portals:

- Administrator portal

An Administrator can do the following:

- Perform administrative tasks.
- View Resources and Resource Groups.
- Create VMs, Plans, and Offers.
- Monitor solution health.

- Tenant portal

A Tenant can do the following:

- Use available resources to do work.

- Consume VMs, Plans, and Offers that have been created by an administrator.

See https://pubs.lenovo.com/thinkagile-sxm/printable_doc for relevant links.

Managing IDs and passwords

Proper maintenance of IDs and passwords is essential for the security of the components and the overall product. Lenovo's Software Security Review Board stresses in the strongest possible terms that customers should manage all product credentials according to the recommendations stated here.

Initial IDs and passwords

Applicable IDs and passwords will be set or changed during the Lenovo Professional Services deployment engagement. Lenovo Professional Services will provide a list of all credentials used to deploy and manage the ThinkAgile SXM Series solution in the documentation that is provided to the customer during the solution handover. Lenovo Professional Services will provide a list of all credentials used to deploy and manage the ThinkAgile SXM Series solution in the documentation that is provided to the customer during the solution handover.

Changing passwords

For password change procedures, refer to the relevant component documentation. See https://pubs.lenovo.com/thinkagile-sxm/printable_doc. In particular, the following Microsoft web page provides an overview and gives detailed instructions for rotating secrets in the Azure Stack Hub environment:

<https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-rotate-secrets>

Important: Changing some IDs or passwords without proper planning (for example, the IMM/XCC credentials on any of the scale unit nodes) can affect the overall configuration of the solution and could result in the inability to manage the nodes via XClarity Administrator.

Password criteria

The following password criteria are strongly recommended by Lenovo's Software Security Review Board:

- No less than twenty (20) characters.
- Includes letters, specifically mixed case.
- Includes numbers.
- Includes punctuation.
- Does not include any repeated characters.

It is also recommended that a random password generator be used. One example is the [Norton Identity Safe Password Generator](#). See the following Web site:

<https://identitysafe.norton.com/password-generator>

Chapter 3. Updating ThinkAgile SXM Series solution firmware

These topics include required steps to update firmware, device drivers, and software on the nodes and network switches of a running ThinkAgile SXM Series solution based on the current solution-specific Best Recipe.

The current ThinkAgile SXM Best Recipe can be viewed at the following URL:

<https://datacentersupport.lenovo.com/us/en/solutions/HT505122>

The complete process of system firmware update comprises the following main activities, and might differ slightly based on the version of Azure Stack Hub Build that is currently running.

Firmware maintenance and Best Recipe

ThinkAgile SXM Series solutions use a “Best Recipe” to identify the supported firmware levels for the product.

For information about ThinkAgile SXM Series Best Recipes, refer to the following Web site:

<https://datacentersupport.lenovo.com/solutions/ht505122>

Adherence to Best Recipe and Support impact

The ThinkAgile SXM Series Best Recipes include component firmware levels that have been tested in an appropriate environment. Any specific firmware that is above or below the level indicated in the Best Recipe is not supported and might impact Lenovo’s ability to support any issues with the relevant component or the entire solution.

Updating firmware

See https://pubs.lenovo.com/thinkagile-sxm/printable_doc for links to relevant documentation.

Prerequisites

Before work can begin, confirm that you have the following items available:

- Access credentials to the Azure Stack Hub Administrator Portal
- Access credentials to XClarity Administrator on the HLH
- USB thumb drive containing:
 - Lenovo ThinkAgile SXM firmware update files for the appropriate Best Recipe
 - XClarity Administrator firmware update policy file for the appropriate Best Recipe
 - Lenovo OEM Extension Package for the appropriate Best Recipe

Note: The above can be obtained from the ThinkAgile SXM repository located at the following URL:

<https://thinkagile.lenovo.com/SXM>

Preparing to update ThinkAgile SXM firmware

Complete the following steps to prepare for ThinkAgile SXM firmware update.

Step 1. Access the ThinkAgile SXM Updates Repository at <https://thinkagile.lenovo.com/SXM>.

At the top level are directories based on specific ThinkAgile SXM Best Recipes. Each directory contains a full set of files required for a given Best Recipe and hardware platform.

Step 2. Click the link for the directory associated with the current Best Recipe.

Step 3. Download the files required for your environment, based on the following criteria:

- Download the following for all environments:
 - AzureStackRecoveryHelper.ps1
 - LXCA_<date>.zip
 - OEM Extension Package for the Best Recipe
- If your solution is an SXM4400 or SXM6400, download **PurleyFirmware_SXMBR<yyyy>.zip** (yyyy is the solution Best Recipe version). This single archive contains the firmware update payload files for the SR650 nodes.
- If your solution is an SXM4600, download **EGSFirmware_SXMBR<yyyy>.zip** (yyyy is the solution Best Recipe version). This single archive contains the firmware update payload files for the SR650 V3 nodes.

Step 4. Expand all the zipped archives, and then copy all the expanded content to a USB thumb drive.

Step 5. Copy the expanded content from the USB thumb drive to the hardware lifecycle host (HLH) as follows:

1. Copy the AzureStackRecoveryHelper.ps1 script file to D:\Lenovo\Scripts.
2. Copy the **contents** (not the directory itself) of the LXCA_<date> directory to D:\Lenovo\LXCA, replacing any files or directories with the same name that are already in the directory.
3. Copy the directory containing the downloaded system firmware update content to D:\Lenovo\LXCA.

Configure XClarity Administrator for a specific Best Recipe

One of the main tasks handled by XClarity Administrator in a ThinkAgile SXM Series solution is to provide a simple way to manage firmware updates on the Azure Stack Hub scale unit nodes. Firmware updates must be imported into XClarity Administrator before they can be applied to any managed system. Since the Azure Stack Hub nodes must run firmware versions according to specific firmware [Best Recipes](#), the appropriate firmware update packages for each published Best Recipe are provided in a single directory.

Once XClarity Administrator has been prepared for a given Best Recipe, firmware updating can take place at any time that is convenient.

Preparing XClarity Administrator to manage firmware updates requires these main activities:

Update XClarity Administrator

Follow the steps in this topic to update XClarity Administrator if necessary (check the current Best Recipe) before proceeding with the remainder of these instructions.

To update XClarity Administrator, follow the steps in this topic. Updating LXCA typically is a two-step process. First, LXCA is updated to a new “base version” and then a “fix pack” is applied. For example, to update LXCA to v2.6.6, the LXCA v2.6.0 update package is applied to any previous v2.x version of LXCA and then the v2.6.6 FixPack is applied to LXCA v2.6.0.

The examples below show the process to update XClarity Administrator v2.1.0 to v2.4.0, but these instructions are valid for updating to any version.

- Step 1. Copy the LXCA Update Package directory to D:\Lenovo\LXCA on the HLH.
- Step 2. On the HLH server, sign in to XClarity Administrator.
- Step 3. At the top menu of the XClarity Administrator browser interface, select **Administration** → **Update Management Server**.

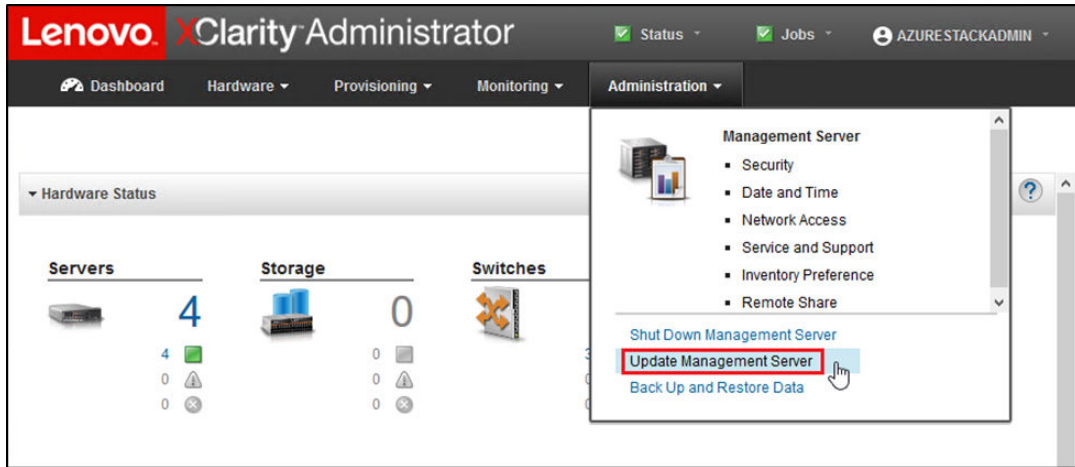



Figure 1. Administration menu → Update Management Server

- Step 4. Click the **Import** button ().
- Step 5. Click **Select Files**.
- Step 6. Navigate to D:\Lenovo\LXCA\LXCA Update Package, select all four files in the directory, and then click **Open**. The example image below shows the update package files for XClarity Administrator v2.4.0, which might vary, depending on the version of XClarity Administrator specified in the current Best Recipe.

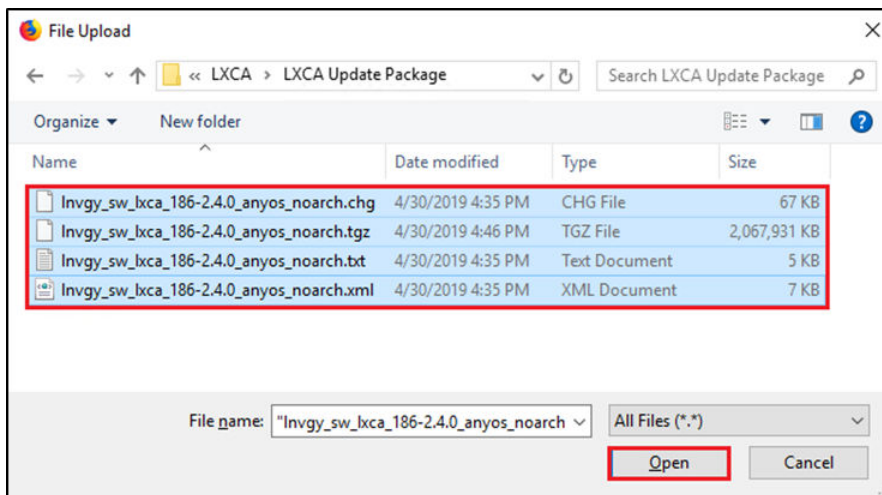

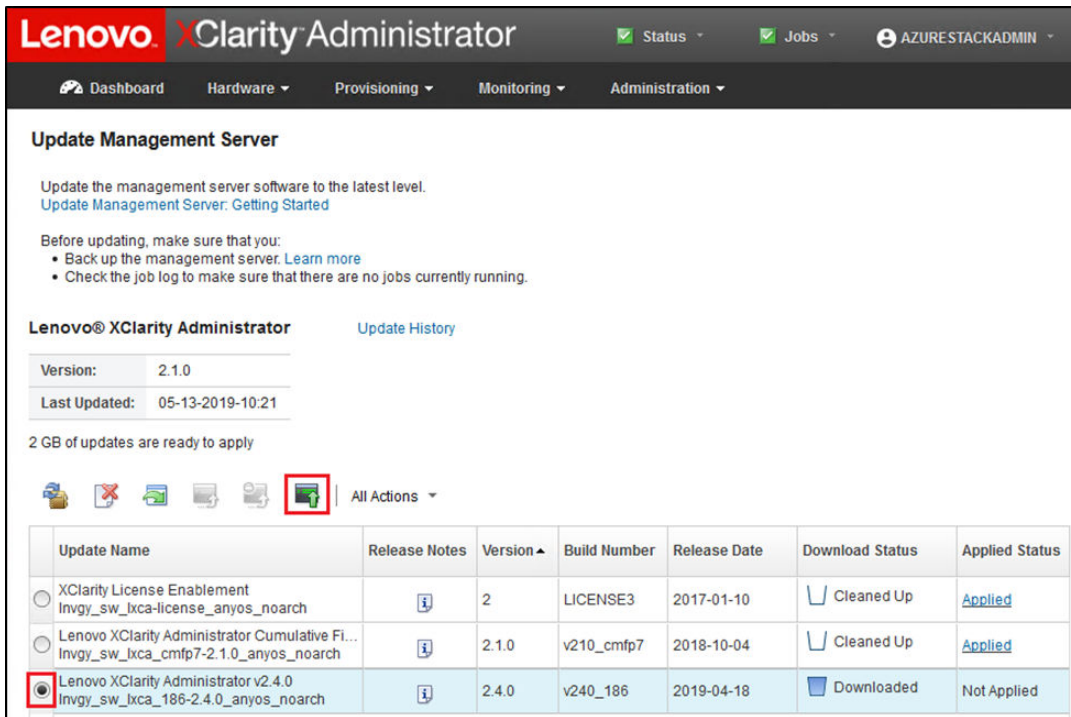


Figure 2. Upload LXCA update package

- Step 7. Back in the Import window, click **Import**.
- Step 8. Status is displayed during the import process. Once complete, verify that the Download Status column shows Downloaded for the XClarity Administrator update package.

Step 9. Select the update package by clicking the radio button to the left of the package name, and then click the **Perform Update** button ().



Update Management Server

Update the management server software to the latest level.
[Update Management Server: Getting Started](#)


Before updating, make sure that you:

- Back up the management server. [Learn more](#)
- Check the job log to make sure that there are no jobs currently running.

Lenovo® XClarity Administrator [Update History](#)

Version: 2.1.0
 Last Updated: 05-13-2019-10:21

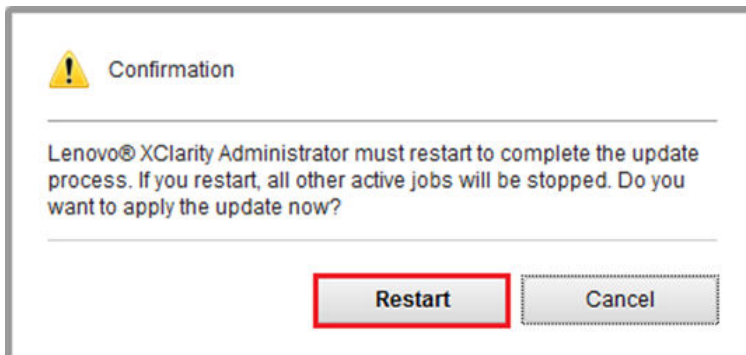
2 GB of updates are ready to apply



Update Name	Release Notes	Version	Build Number	Release Date	Download Status	Applied Status
<input type="radio"/> XClarity License Enablement Invgy_sw_lxca-license_anyos_noarch		2	LICENSE3	2017-01-10	Cleaned Up	Applied
<input type="radio"/> Lenovo XClarity Administrator Cumulative Fi... Invgy_sw_lxca_cmf7-2.1.0_anyos_noarch		2.1.0	v210_cmf7	2018-10-04	Cleaned Up	Applied
<input checked="" type="radio"/> Lenovo XClarity Administrator v2.4.0 Invgy_sw_lxca_186-2.4.0_anyos_noarch		2.4.0	v240_186	2019-04-18	Downloaded	Not Applied

Figure 3. Perform management server update

Step 10. In the Confirmation window that displays, click **Restart**.



Confirmation

Lenovo® XClarity Administrator must restart to complete the update process. If you restart, all other active jobs will be stopped. Do you want to apply the update now?

Restart

Figure 4. Restart message after XClarity Administrator update

Step 11. After a few seconds, the XClarity Administrator browser interface is replaced by the following message:

The update request has been submitted to the management server.
 Please wait...this update could take several minutes...
 Refresh the browser window to check if the management server has completed the update.

Figure 5. XClarity Administrator update request message

Step 12. Once XClarity Administrator is back online, reconnect and sign in to the XClarity Administrator browser interface. It can take several minutes after logging in for all servers and switches to be accurately reflected in the XClarity Administrator interface. Initially, you might see Status as “Disconnected.”

Import firmware update packages

To import the firmware updates, follow these steps:

Step 1. At the top menu of XClarity Administrator, select **Provisioning** → **Repository**. Initially, the firmware repository may be empty (for example, if you have just installed and configured XClarity Administrator), as indicated by the blue informational alert in the illustration below.

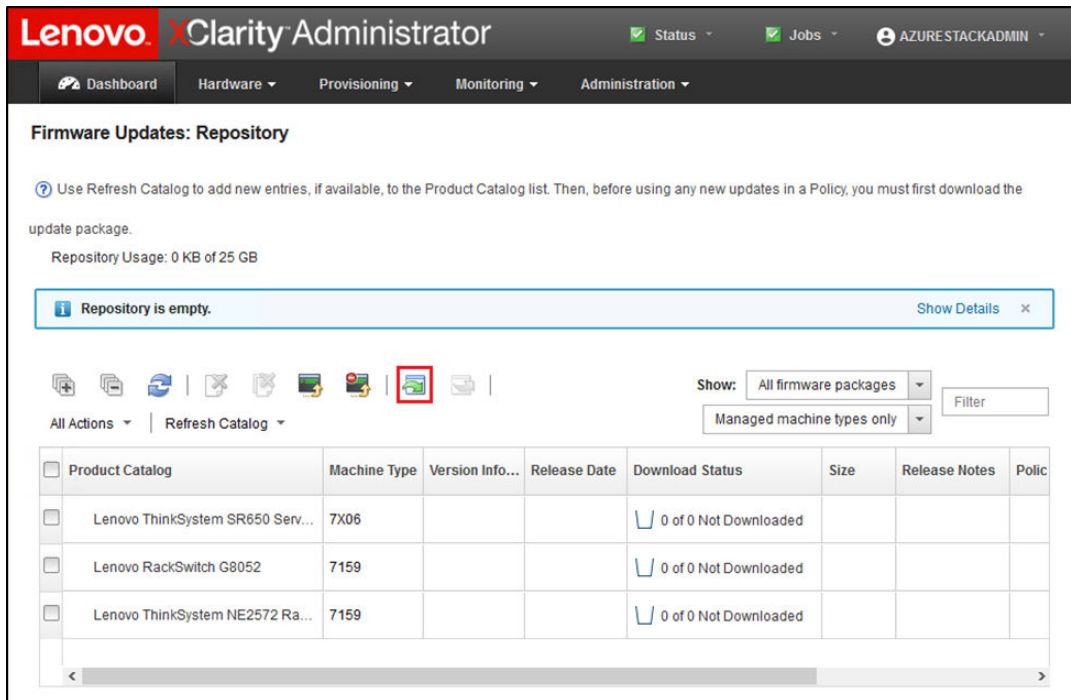



Figure 6. XClarity Administrator firmware update repository

- Step 2. Click the **Import** icon () and then click **Select Files...**
- Step 3. Navigate to the appropriate firmware directory located in D:\Lenovo\IXCA as described above, select all files in the directory, and click **Open**.

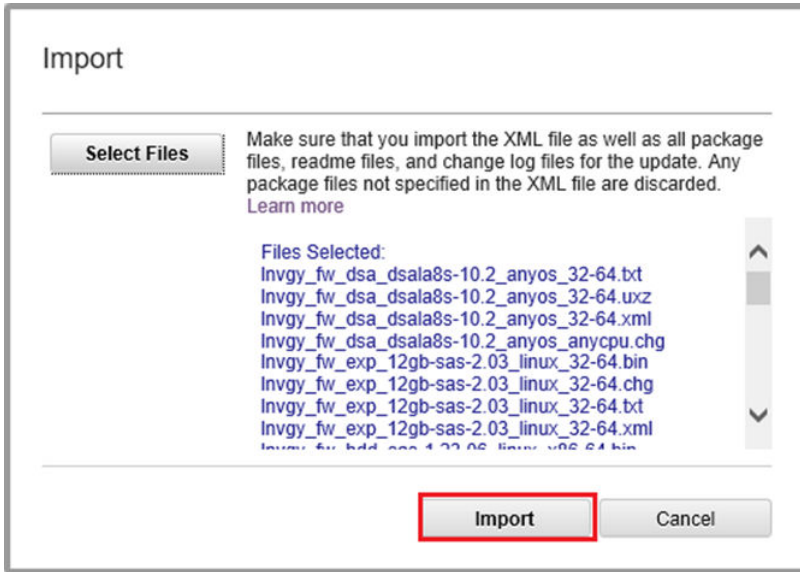


Figure 7. Selecting files for import

Step 4. Click **Import**. A status bar appears at the top of the window during import and validation.

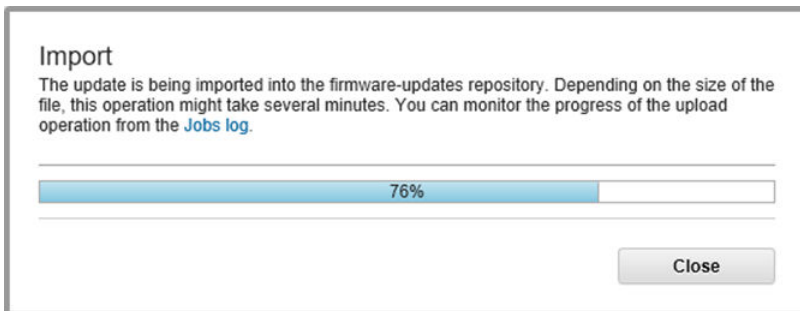


Figure 8. Firmware import status

You can now expand the Product Catalog to reveal each component firmware update version contained in the repository.

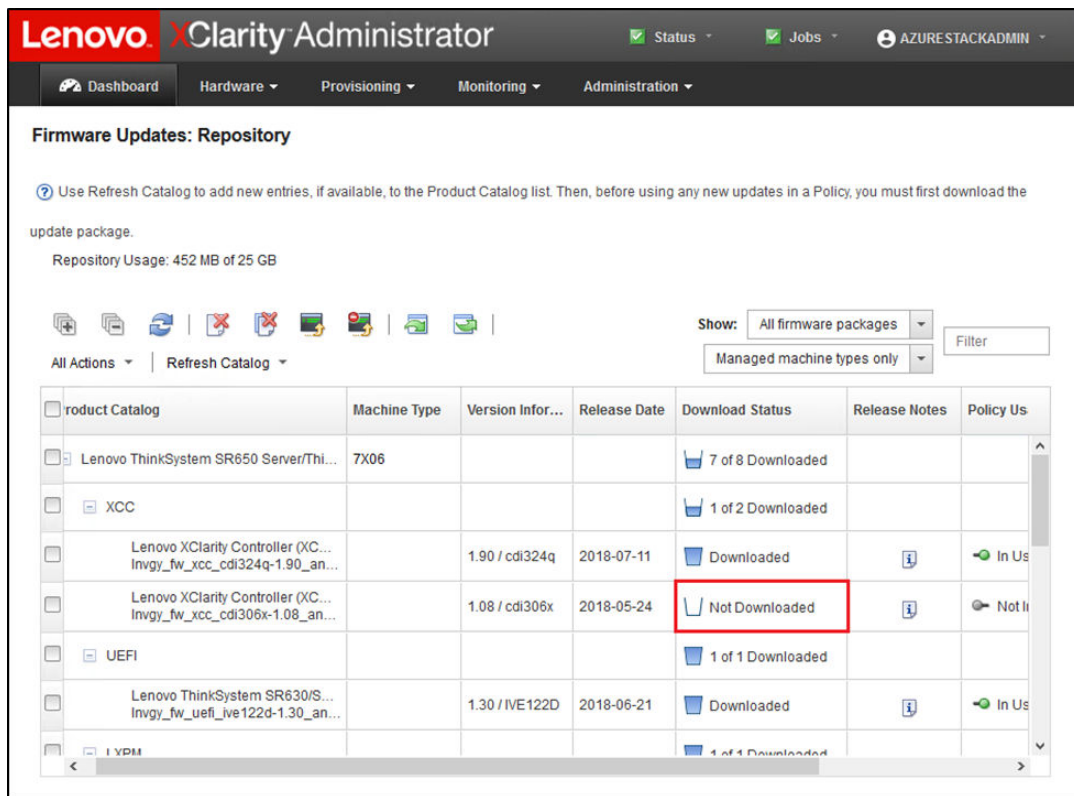


Figure 9. Product Catalog showing new updates

Import firmware compliance policy

XClarity Administrator compliance policies contained in the LXCA_<date>.zip archive downloaded from the ThinkAgile SXM Updates Repository have a name in the following format for easy recognition of the Best Recipe for which they are intended:

<Platform>Policy_SXMBRyyyy

where <Platform> is either “Purley” or “EGS” and yyyy is the ThinkAgile SXM Best Recipe version.

To import the XClarity Administrator firmware compliance policy, follow these steps:


- Step 1. At the top menu of the XClarity Administrator browser interface, select **Provisioning** → **Compliance Policies**. Similar to the firmware repository, there may or may not be firmware update policies already shown. This list will grow over time as additional policies are added for new Best Recipes. In the example screenshot below, you see three previous policies for Best Recipes SXMBR1903, SXMBR1905, and SXMBR1910 for the Purley platform. We will continue with this example, preparing XClarity Administrator for Best Recipe SXMBR2002 for the Purley platform.

Firmware Updates: Compliance Policies

Compliance Policy allows you to create or modify a policy based on the acquired updates in the Firmware Repository.

Compliance Policy Name	Usage Status	Compliance Pol...	Last Modified	Description
PurleyPolicy_SXMBR1903	Not Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...
PurleyPolicy_SXMBR1905	Not Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...
PurleyPolicy_SXMBR1910	Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...

Figure 10. Firmware Updates: Compliance Policies window

- Step 2. Click the **Import** icon () and then click **Select Files....**
- Step 3. Navigate to D:\Lenovo\LXCA, select the file titled <Platform>Policy_SXMBRyyy.xml, and then click **Import**. As stated previously, the “<Platform>” portion of the file name is either “Purley” or “EGS” depending on your solution, and the “yyy” portion of the file name reflects the ThinkAgile SXM Best Recipe version for which the policy file was created. Once the policy is imported, it is shown on the Firmware Updates: Compliance Policies page.

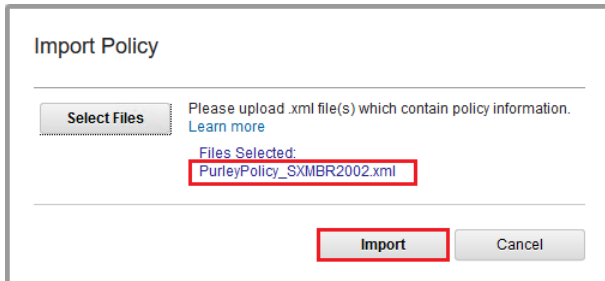


Figure 11. Import firmware compliance policy

Firmware Updates: Compliance Policies

Compliance Policy allows you to create or modify a policy based on the acquired updates in the Firmware Repository.

| All Actions

Compliance Policy Name	Usage Status	Compliance Pol...	Last Modified	Description
<input type="checkbox"/> PurleyPolicy_SXMBR1903	Not Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...
<input type="checkbox"/> PurleyPolicy_SXMBR1905	Not Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...
<input type="checkbox"/> PurleyPolicy_SXMBR1910	Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...
<input type="checkbox"/> PurleyPolicy_SXMBR2002	Not Assigned	User Defined	This policy was edi...	Includes firmware updates from ThinkAgile ...

Figure 12. Imported firmware compliance policy

Assign firmware compliance policy

Now that the repository is populated with firmware update packages and the firmware compliance policy has been imported, the policy can be assigned to the scale unit nodes. To do so, follow these steps:

- Step 1. At the top menu of the XClarity Administrator browser interface, select **Provisioning** → **Apply / Activate**. Initially, the assigned compliance policy for each system might be “No assignment” or reflect a policy from a previous Best Recipe. In the example illustration below, all four nodes already have the policy associated with Best Recipe SXMBR1910 assigned to them. Furthermore, all four nodes are shown as “Compliant” with that policy.

Lenovo XClarity Administrator Status Jobs AZURESTACKADMIN

Dashboard Hardware Provisioning Monitoring Administration

Firmware Updates: Apply / Activate

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

Update with Policy | Update without Policy

| All Actions

Filter By Filter

Critical Release Information Show: All Devices

Device	Power	Installed Version	Assigned Compliance Policy	Compliance Target
<input type="checkbox"/> Lenovo-01 10.30.8.3	On	Compliant	PurleyPolicy_SXMBR1910	
<input type="checkbox"/> Lenovo-02 10.30.8.4	On	Compliant	PurleyPolicy_SXMBR1910	
<input type="checkbox"/> Lenovo-03 10.30.8.5	On	Compliant	PurleyPolicy_SXMBR1910	
<input type="checkbox"/> Lenovo-04 10.30.8.6	On	Compliant	PurleyPolicy_SXMBR1910	

Figure 13. Firmware Updates: Apply/Activate window

- Step 2. Before assigning the firmware update policy to the nodes, global settings for firmware updates must be set. To do this, click **All Actions** and then select **Global Settings** in the dropdown list that appears.
- Step 3. In the Global Settings: Firmware Updates window that opens, select to enable the checkboxes for all three options, and then click **OK**.

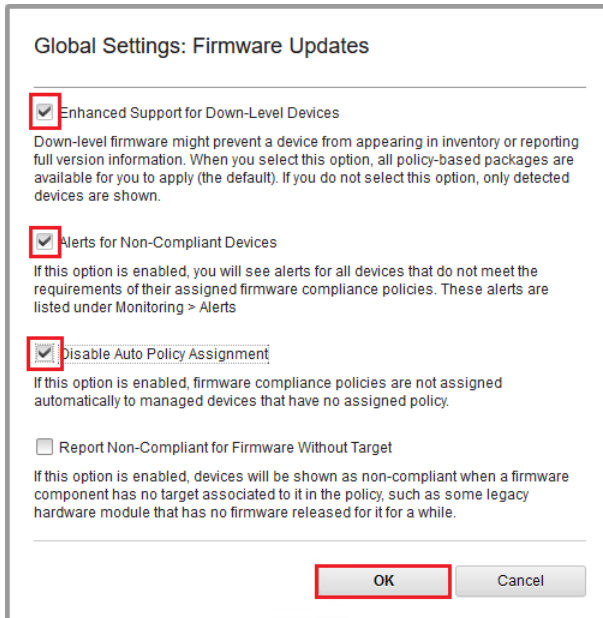


Figure 14. Global Settings: Firmware Updates window

- Step 4. Now that global settings have been configured, on the Firmware Updates: Apply / Activate page, change the assigned compliance policy to the policy that was just imported. Notice in the following example illustration of a 4–node Purley solution that the policy has been changed to support Best Recipe SXMBR2002 for Purley solutions and all nodes now show as “Not Compliant” (highlighted by the red boxes) since the firmware has not yet been updated to SXMBR2002 levels. Also, because of the global settings that were configured, if any server is flagged as Not Compliant, the **Status** icon in the XClarity Administrator top banner (highlighted by the yellow box) will indicate a warning alert. It might take a minute or two for this alert icon to be updated.

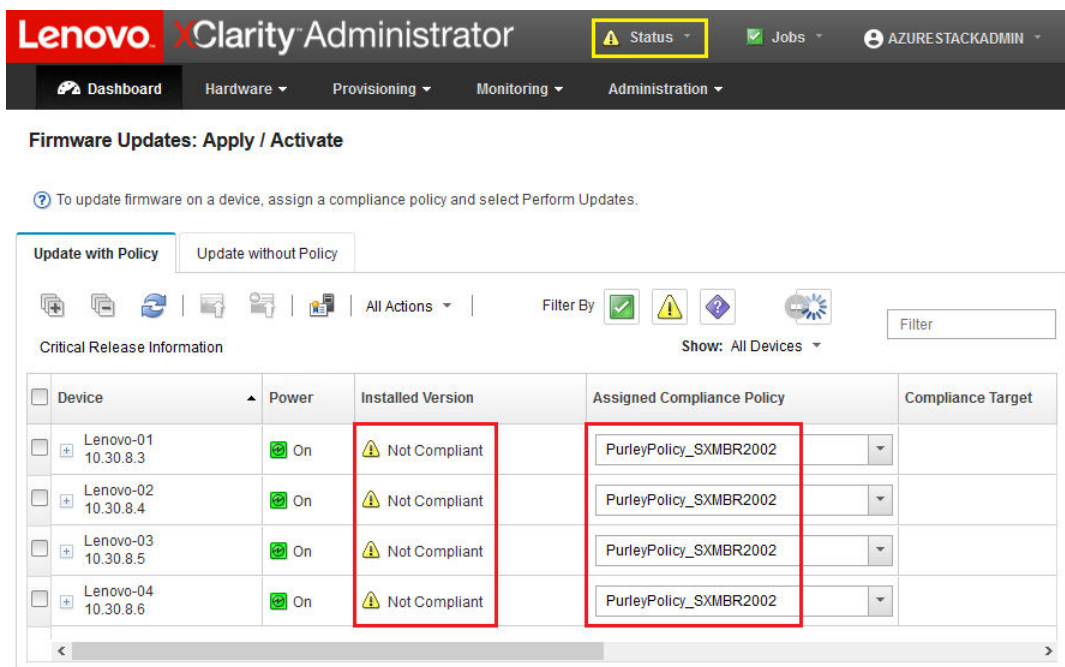


Figure 15. Firmware compliance policy showing noncompliant nodes

XClarity Administrator is now ready to perform firmware updates on the ThinkAgile SXM Series solution. Proceed to [“Update the ThinkAgile SXM OEM Extension Package” on page 15](#) at the start of the scheduled maintenance window for firmware updating of the solution.

Update the ThinkAgile SXM OEM Extension Package

These topics detail the process of applying an OEM Extension Package update to a running ThinkAgile SXM Series solution. The OEM Extension Package is the construct provided by Microsoft that contains device drivers for all components in the Azure Stack Hub nodes. As such, it is designed to work with the system firmware from a ThinkAgile SXM Best Recipe. This is why the OEM Extension Package is listed in each Best Recipe.

OEM Extension Packages are contained in a zip archive with the following name format:

OEMv<x>_SXMBR<yyyy> where <x> is either “2.2” or “3.0” and yyyy is the Best Recipe version for which it is intended.

To prepare for updating the OEM Extension Package, download the appropriate zip archive from the repository.

The high-level activities associated with updating the OEM Extension Package are:

- [“Provide LXCA details to Azure Stack Hub” on page 16](#)
- [“Determine current versions” on page 18](#)
- [“Create the update storage container” on page 18](#)
- [“Upload the OEM Extension Package” on page 20](#)
- [“Perform the update” on page 22](#)
- [“Verify the update and Azure Stack Hub functionality” on page 24](#)

Microsoft recommends keeping Azure Stack Hub running at the latest available version.

Prerequisites

Before work can begin, ensure that you have a USB thumb drive containing the appropriate OEM Extension Package available.

Also, do not attempt to update the OEM Extension Package until LXCA has been prepared, as described in [“Configure XClarity Administrator for a specific Best Recipe” on page 6](#).

Provide LXCA details to Azure Stack Hub

The Patch and Update (PnU) feature of Azure Stack Hub requires the LXCA IP address and credentials to be stored in a specific variable within the Azure Stack Hub fabric to communicate all firmware update requests to LXCA and to handle its respective authentication.

Notes:

- The steps in this topic are required to be completed before the first PnU firmware update is executed. Every time the LXCA credentials are changed, these steps should be run again.

A helper script has been created to make this process easier. Follow these steps to use the script:

Step 1. Copy “AzureStackManagerCredsHelper.ps1” to “D:\Lenovo\Scripts” on the HLH.

Step 2. Open a new instance of PowerShell ISE as Administrator, and then open the helper script. The script includes comments throughout to assist in using it.

```
# Set the variables used by the rest of the lines
#
# <EmergencyConsoleIPAddresses> is the IP address of a PEP
$ip = "<EmergencyConsoleIPAddresses>"

# <Password> is the password for the Azure Stack Hub Administrator account
$pwd = ConvertTo-SecureString "<Password>" -AsPlainText -Force

# <DomainFQDN> is the domain name of the scale unit
# <UserID> is the UserID of the Azure Stack Hub admin account (often "CloudAdmin")
$cred = New-Object System.Management.Automation.PSCredential ("<DomainFQDN>\<UserID>", $pwd)
Enter-PSSession -ComputerName $ip -ConfigurationName PrivilegedEndpoint -Credential $cred

# The following command will pop up a window for LXCA Credentials
# <LXCAIPAddress> is the IP Address of LXCA
Set-DEMExternalVM -VMType HardwareManager -IPAddress "<LXCAIPAddress>"
```

This script includes bracketed parameters that must be replaced by real values from your environment. These values can be found in the table contained in the **Lenovo ThinkAgile SXM - Customer Deployment Summary** document that was left with you and copied to the HLH (“D:\Lenovo\Azure Stack Deployment Details”) after Azure Stack Hub was initially deployed in your datacenter. Replace the bracketed parameters as follows:

- *<EmergencyConsoleIPAddresses>* is the IP address of a Privileged Endpoint (PEP), which can be found in the *Emergency Recovery Console Endpoints* section of the table. Any of the three IP addresses can be used.
- *<Password>* is the password for the Azure Stack Hub Administrator account, which can be found in the *Azure Stack Infrastructure* section of the table. This is the password that is used to log in to the Azure Stack Hub Administrator Portal.
- *<DomainFQDN>* is the domain name of the scale unit, which can be found in the *Azure Stack Hub Infrastructure* section of the table.

- `<UserID>` is the UserID of the Azure Stack Hub Administrator account, which can be found in the *Azure Stack Infrastructure* section of the table. This is the UserID that is used to log in to the Azure Stack Hub Administrator Portal.
- `<LXCAIPAddress>` is the IP address of the LXCA virtual machine, which can be found in the *LXCA* section of the table.

Step 3. After replacing all bracketed parameters with real values, save the script so it can be reused in the future if the LXCA credentials are changed.

Step 4. Select all lines in the script except the last three lines, and run the selected portion by clicking the **Run Section** (📄) button. It is normal to see an orange warning message, displaying the following text:

The names of some imported commands from the module 'ECEClient' include unapproved verbs that might make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.

Step 5. A window will pop up, requesting credentials. **Enter the credentials that are used to log in to LXCA.** The credentials at the time of Azure Stack Hub deployment can be found in the same table referenced above, in the **LXCA** section of the table.

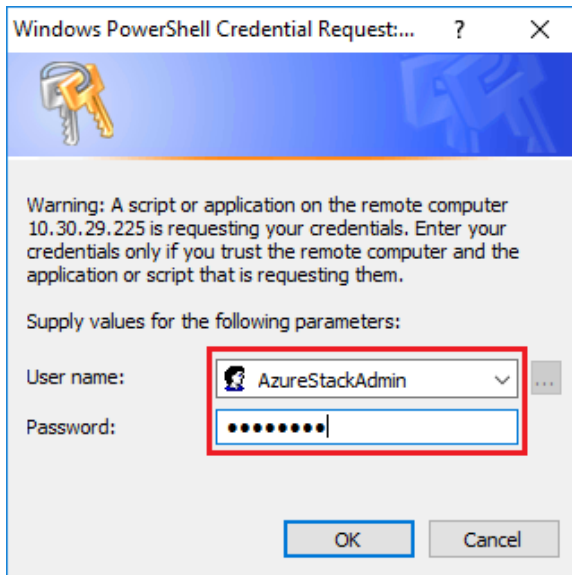


Figure 16. Credentials that are used to log in to LXCA

It will take a few minutes for the command to complete. PowerShell will periodically update with the following verbose status messages:

VERBOSE:

Overall action status: 'Running'

VERBOSE:

VERBOSE: Step 'OEM Hardware Manager password update' status: 'InProgress'

VERBOSE:

Once complete, you will see a final status update ("VERBOSE: DONE") before a summary of what was done is displayed.

This completes the steps required to provide XClarity Administrator details to the scale unit. Please proceed to [“Determine current versions” on page 18](#).

Determine current versions

Follow this procedure to check your Microsoft Azure Stack Hub version.

Check the Dashboard blade in the Azure Stack Hub Administrator Portal to ensure that there are no current alerts shown. All alerts need to be resolved before performing any update to the OEM Extension Package or Azure Stack Hub Build. Otherwise, the update process will simply wait for the scale unit to become healthy before attempting the update.

To determine whether an update is necessary, check the current version. To do this, sign in to the Azure Stack Hub Administrator Portal. To find the version of the OEM Extension Package currently used by the solution, click the Update tile to open the Update blade.

The OEM Extension Package version currently used by the solution is shown as “Current OEM version” as shown in the following illustration. Make a note of the versions found, so they can be compared against the latest versions available. In the example screen capture below, the solution is running Azure Stack Hub Build 1910 (in the yellow box) and OEM Extension Package version 2.1.1910.503 (in the light blue box).

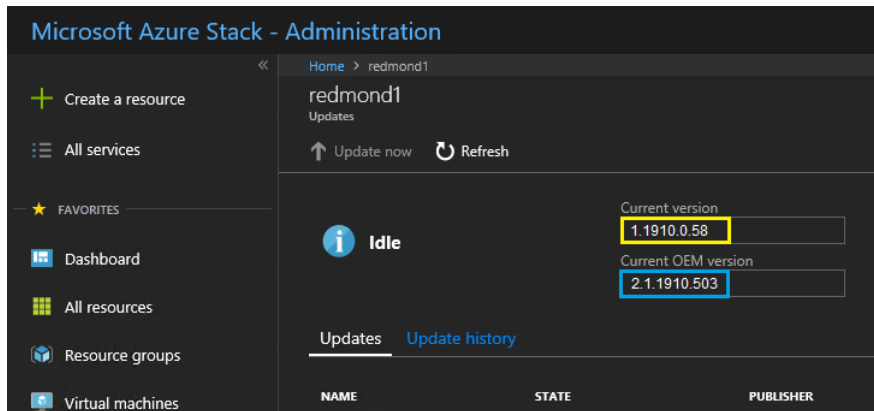


Figure 17. Checking current running Azure Stack Hub versions

Create the update storage container

Follow this procedure for creating a storage container within Azure Stack Hub to import the update package.

For an OEM Extension Package to be applied to Azure Stack Hub, it must be imported into a specific storage container within Azure Stack Hub. This container must be created as follows:

- Step 1. Sign in to the Administrator Portal of Azure Stack Hub.
- Step 2. In the Azure Stack Hub Administrator Portal, navigate to **All services** → **Storage Accounts** (found under DATA + STORAGE).
- Step 3. In the filter box, type `update`, and select **updateadminaccount**.

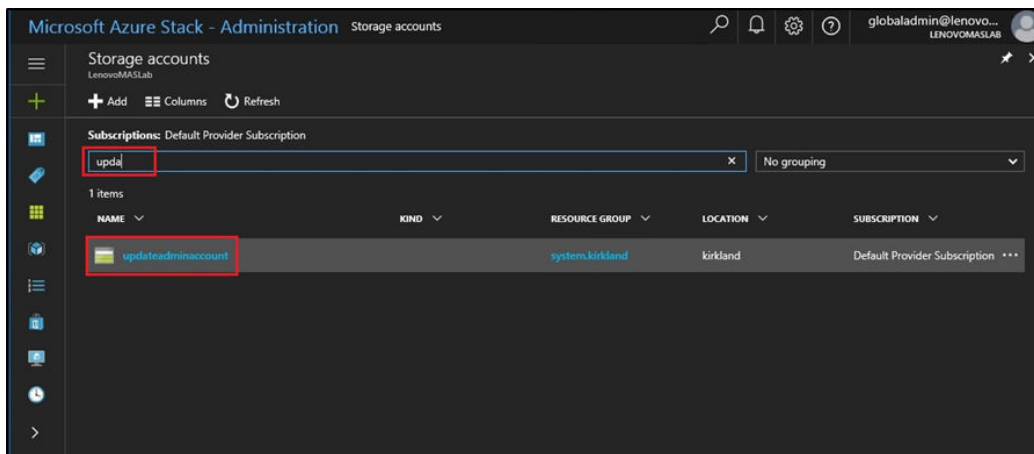


Figure 18. Navigating to the updateadminaccount storage container

Step 4. In the updateadminaccount storage account details, under Services, select **Blobs**.

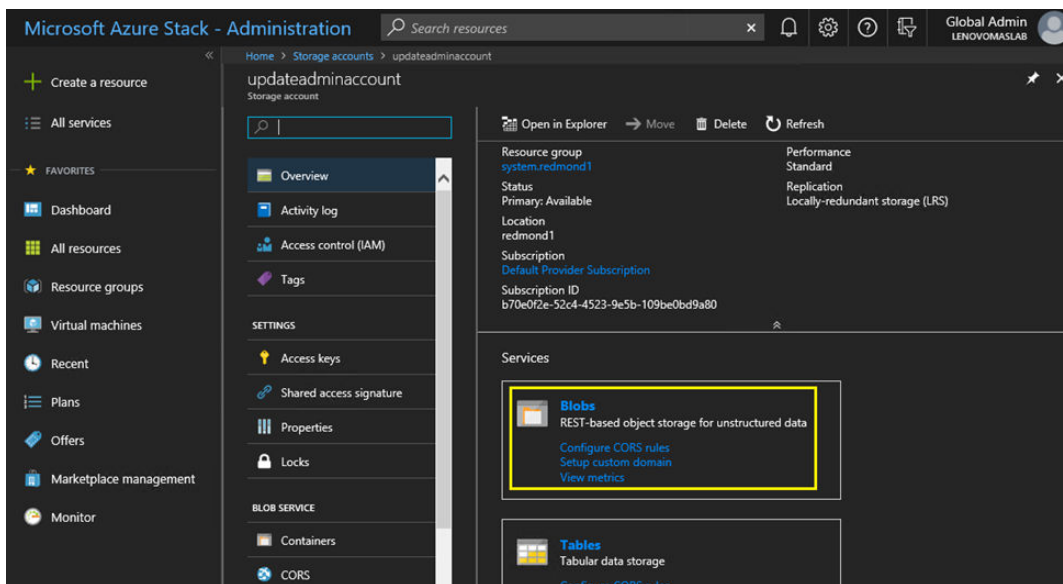


Figure 19. Navigating to the Blobs storage container

Step 5. On the Blob service tile, click **+ Container** to create a container, enter a name for the container (for example, **oem-update-2002**), and click **OK**.

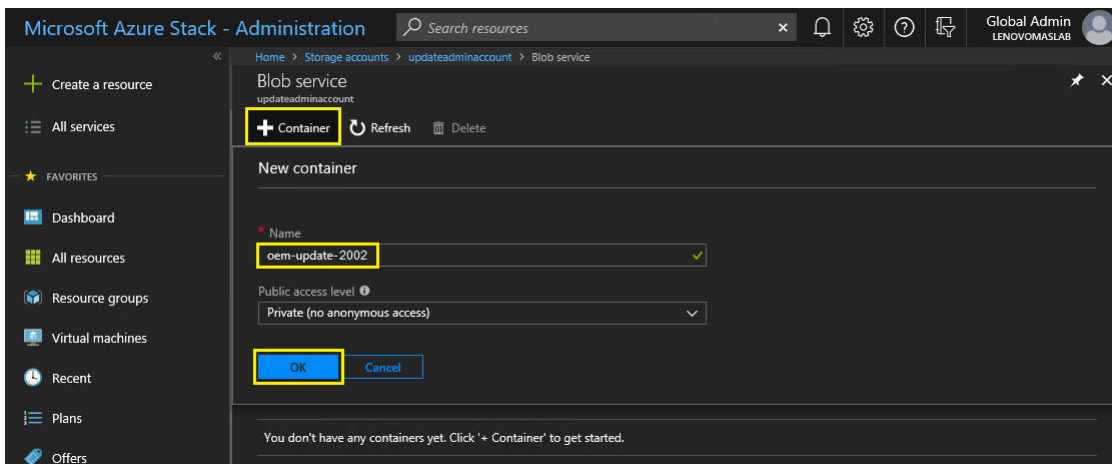


Figure 20. Creating the new container

Upload the OEM Extension Package

Now that the storage container has been created, the update package files must be uploaded into the container. To do this, follow these steps:

Step 1. After the container is created, select it to open a new tile.

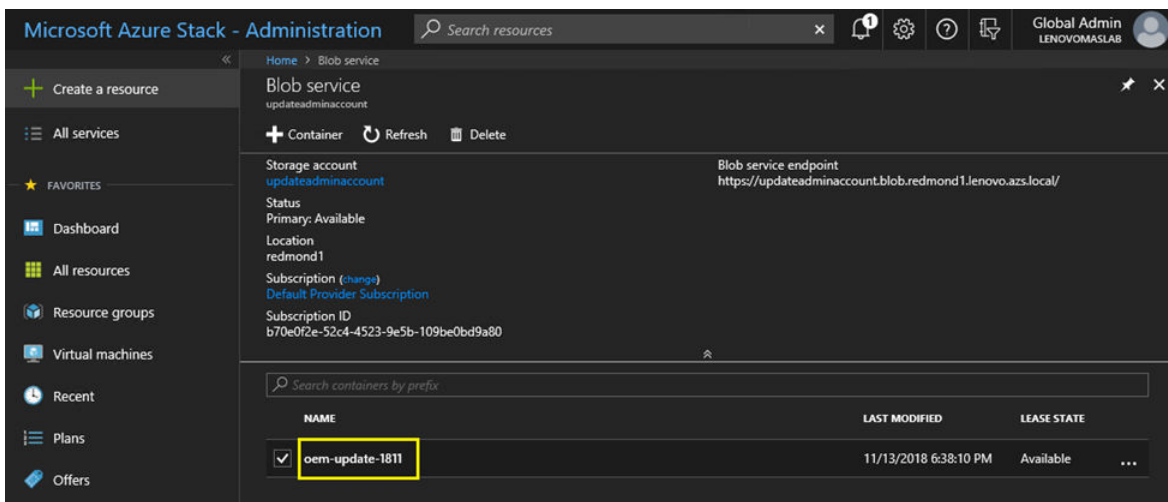


Figure 21. Selecting the storage container for upload

Step 2. Click **Upload**.

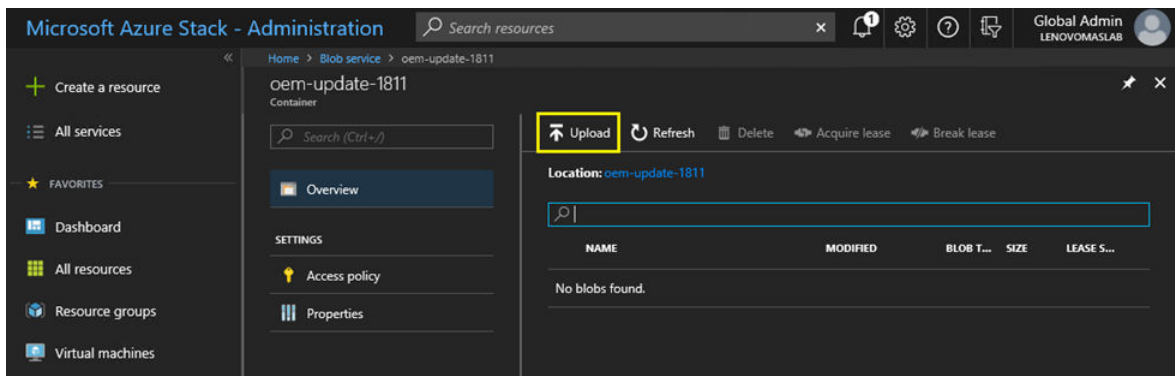


Figure 22. Selecting the Upload control

Step 3. Browse to the update package, select both package files, and click **Open** in the file explorer window.

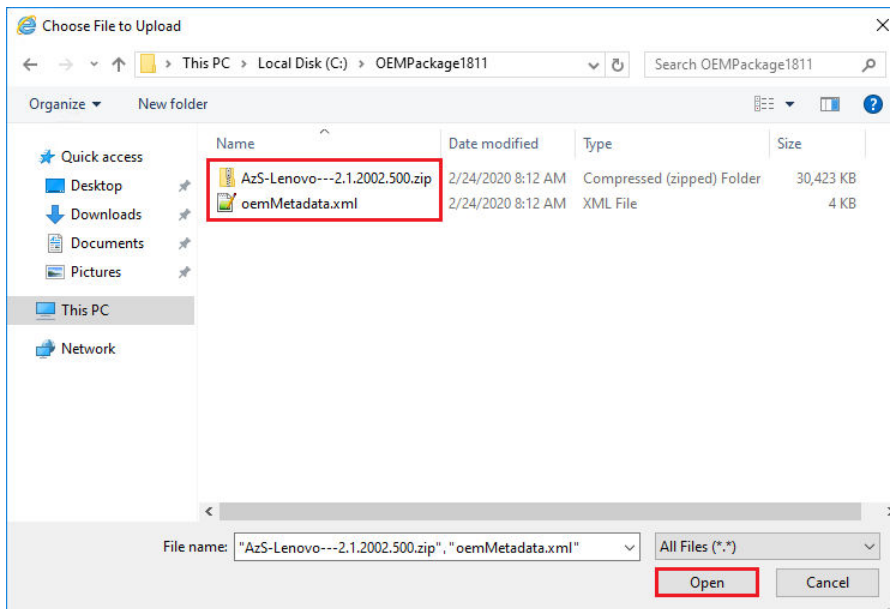


Figure 23. Selecting the update package files for upload

Step 4. Click **Upload** in the administrator portal.

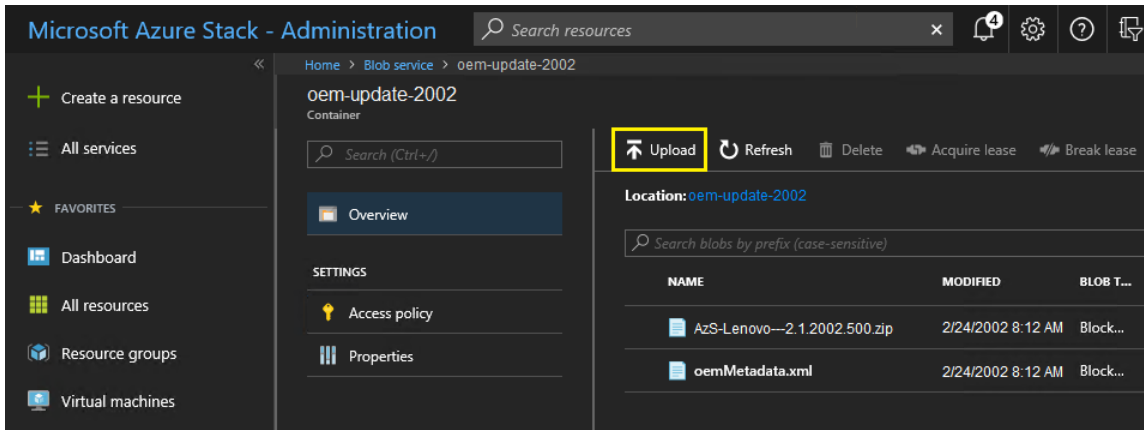


Figure 24. Uploading the update package files

When the upload is complete, all package files are listed in the container. You can review the Notifications area (🔔) to verify that each upload has completed.

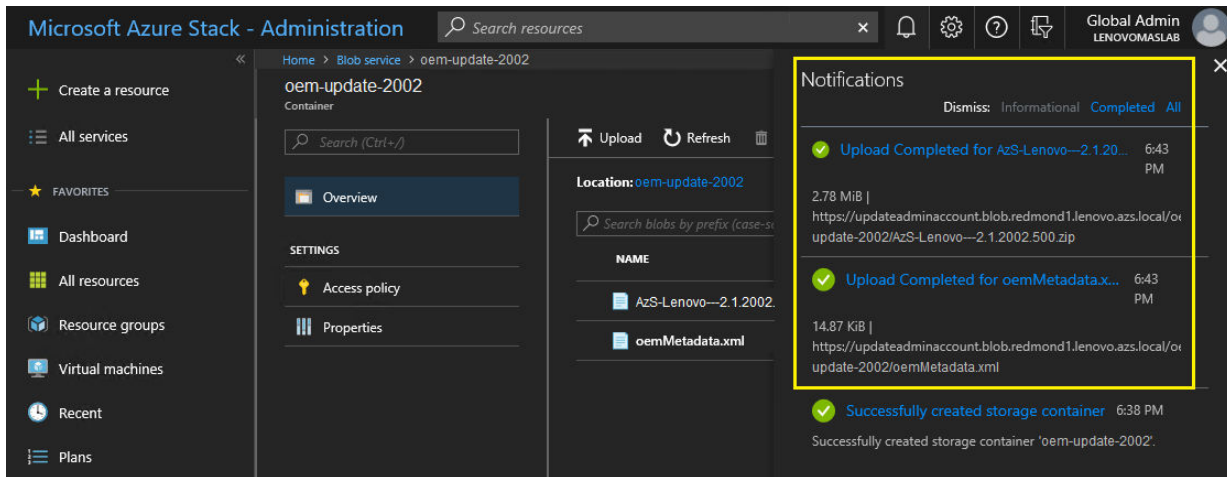


Figure 25. Verifying uploads completed successfully

Perform the update

Once the OEM Extension package files have been uploaded to their container, return to the Dashboard view. The Update tile now displays “Update available.” The OEM Extension Package update can now be applied as follows:

- Step 1. Select **Update** to review the newly added update package with version number.
- Step 2. To install the update, select the OEM Extension Package update marked as **Ready** . Note that if an Azure Stack Hub Update is available, it will be listed along with the OEM Extension Package update and will require a completely separate update process. Make sure to select the correct update before proceeding.

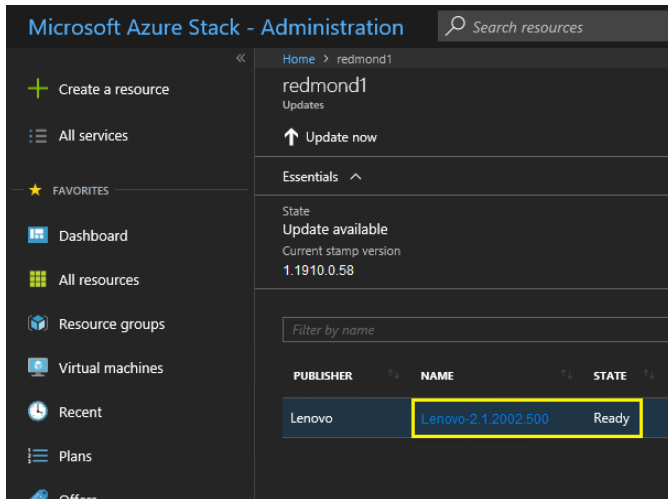


Figure 26. Initiating the update

- Step 3. With the OEM Extension Package update selected, either right-click and select **Update now**, or click **Update now** in the command bar at the top of the window to begin the update process. The state of the update at the bottom of the Portal changes to “In progress” and the state of any other update available changes to “Not applicable” since an update is now in progress.

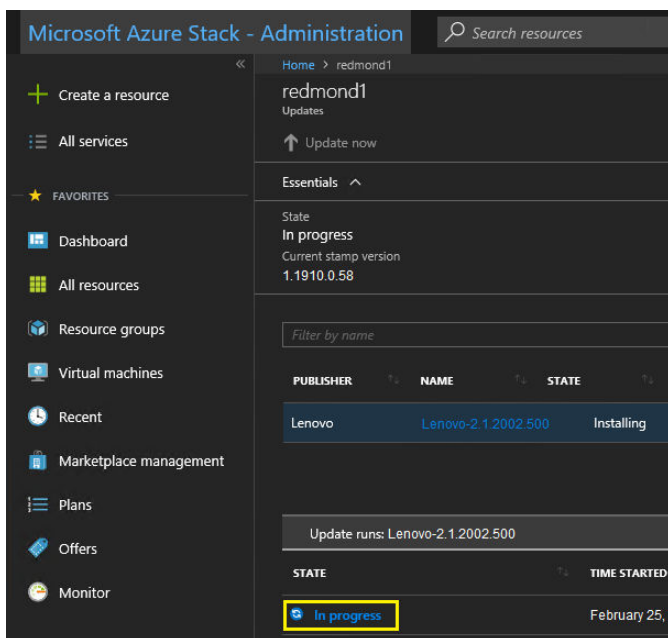


Figure 27. Update progress indicators

- Step 4. Click the **In progress** indicator to open the Update run details tile to view details of the currently installing update package.

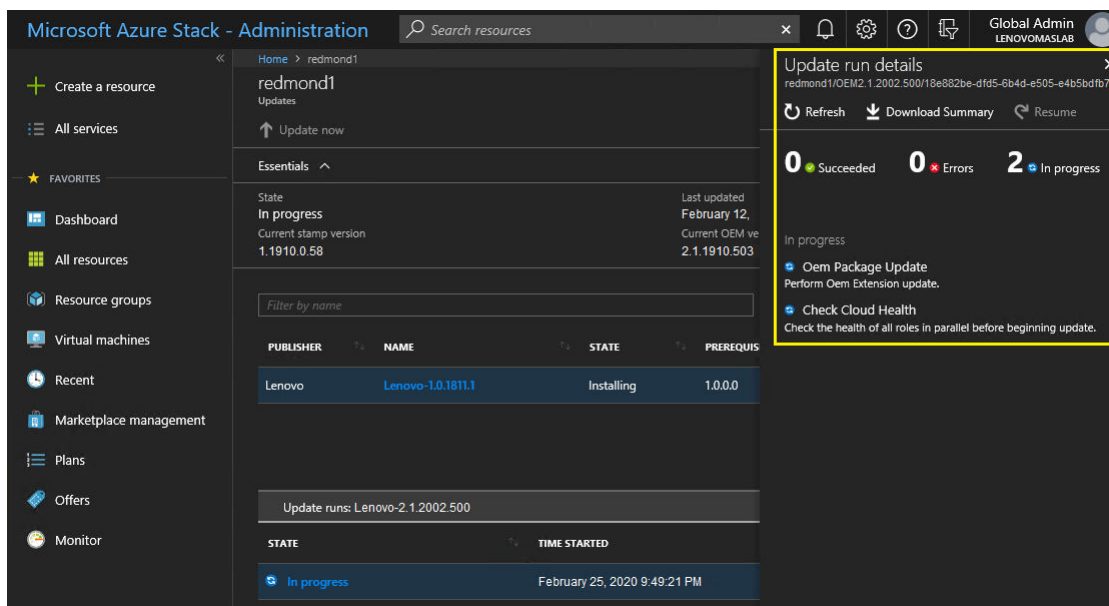


Figure 28. Installation details

Step 5. The entire update process can take a significant amount of time, since each node is drained, redeployed from bare metal, and resumed during the process. Once the update is complete, you will see that the STATE column updates to “Succeeded” and the Update run details tile on the right side of the portal shows no updates in progress.

Verify the update and Azure Stack Hub functionality

Once the update has been applied successfully, it can take some time (two hours or more) for Azure Stack Hub to “settle down” and return to normal behavior. During the update process and this settling period, alerts may appear based on infrastructure component availability.

You can verify that the update has been applied by checking the version of the current environment in the Azure Stack Hub Administrator Portal. Return to the dashboard and click **Update** to open the Update blade. Check that the “Current OEM version” is as expected.

The Azure Stack Hub validation tool (**Test-AzureStack**) is a PowerShell cmdlet that lets you run a series of tests on your system to identify failures if present. It is a recommended practice to run the Test - AzureStack cmdlet after applying each update. See here for Microsoft’s current instructions for performing this test: <https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-diagnostic-test>.

Update the ThinkAgile SXM switch firmware (Lenovo switches only)

Current ThinkAgile SXM Series solutions are no longer shipped with Lenovo network switches. This topic presents the steps required to update Lenovo BMC and TOR switches in a running Lenovo ThinkAgile SXM Series solution that was shipped with Lenovo switches. Steps are included to backup the switch configurations, update the Network Operating System (NOS) on each switch, and verify that the switches are operating properly.

Introduction

Once a ThinkAgile SXM Series solution has been deployed and is running workloads, it is essential to ensure minimal disruption of the production environment. It is necessary to maintain active network connectivity at all times, even during updates of the network switch operating systems and configurations. The Azure Stack Hub network design incorporates two redundant TOR switches to achieve this level of high availability.

In these topics, the steps include entering switch credentials in the form of “admin/<password>.” You must substitute the actual credentials for each switch in order to complete this process. You can find these credentials in the Customer Deployment Summary document left with you at solution turnover. You can modify passwords after updating the switch successfully.

The switch firmware update process includes the following activities:

- Prepare XClarity Administrator to update switch firmware
- Back up TOR switch configurations
- Update the TOR switches
- Verify TOR switch functionality
- Back up BMC switch configuration
- Update the BMC switch
- Verify BMC switch functionality

Prerequisites

Follow the instructions in this topic before starting the process of switch firmware update.

Before work can begin, confirm that you have the following items available:

- Access credentials to the Azure Stack Hub Administrator Portal
- Access credentials to XClarity Administrator on the HLH
- In case a direct serial connection to a switch is needed for troubleshooting:
 - Lenovo-specific serial cable (Mini-USB-RJ45-Serial) supplied with switch
 - USB-to-serial cable
 - USB thumb drive containing:
 - Lenovo ThinkAgile SXM firmware update files for the appropriate Best Recipe
 - XClarity Administrator firmware update policy file for the appropriate Best Recipe

Note: The above files can be obtained from the ThinkAgile SXM repository located at the following URL:

<https://thinkagile.lenovo.com/SXM>

- This guide assumes that your ThinkAgile SXM Series solution is running Lenovo XClarity Administrator version 2.x on the HLH to perform firmware updates on the ThinkAgile SXM network switches. If XClarity Administrator version 2.x is running on the HLH, it is easily updated to any other version 2.x following the instructions in the topic [Update XClarity Administrator](#).
- The minimum switch NOS versions required to use XClarity Administrator to perform updates are CNOS v10.6.1.0 (on the TOR switches and NE0152T BMC switch) and ENOS v8.4.8.0 (on the G8052 BMC switch). If a switch is running an earlier version, you cannot use XClarity Administrator to update the NOS on the switch. In this situation, refer to [Appendix B “Updating ThinkAgile SXM Series switches using the CLI \(Lenovo switches only\)” on page 91](#) for instructions on how to use the switch CLI method to update switch firmware.
- Establish a solution maintenance window, during which the expectation is that the solution might not be available. Lenovo recommends allowing a minimum 2-hour maintenance window for all three switches.

Prepare XClarity Administrator to update switch firmware

Follow the instructions in this topic to prepare XClarity Administrator to update Lenovo switch firmware.

Using XClarity Administrator to update Lenovo switch firmware is straightforward and quick. Before updating, the switches must be managed by XClarity Administrator. To verify that XClarity Administrator manages the switches, use the top menu in XClarity Administrator to navigate to **Hardware → Switches**. If you do not see all the solution switches as shown in the screen capture below, refer to the “Manage the switches” topic in [Appendix A “XClarity Administrator deployment and configuration”](#) on page 55 for steps to manage the switches.

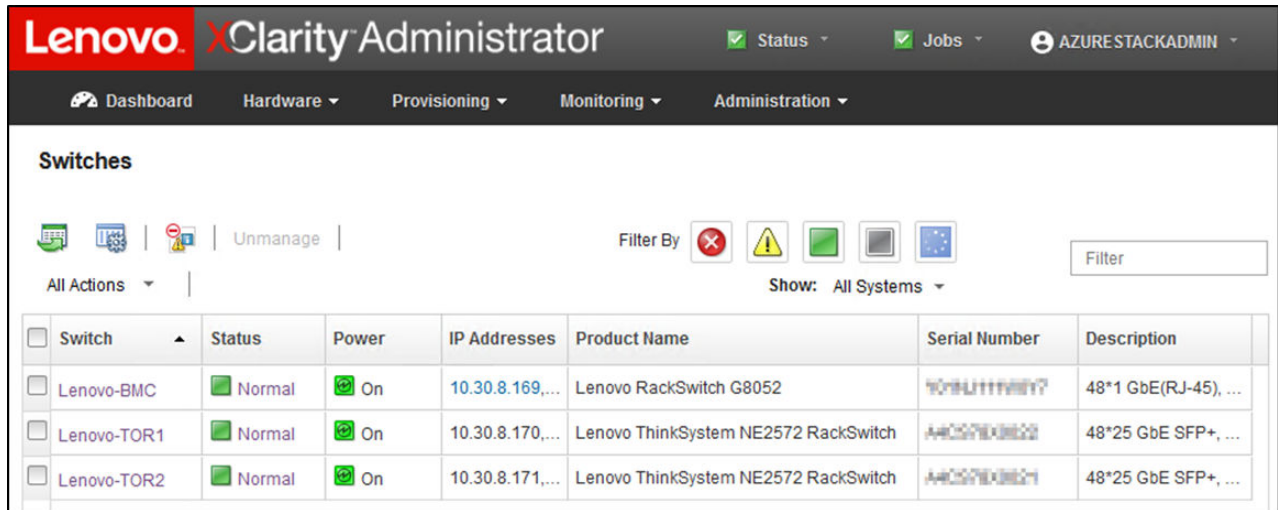


Figure 29.

XClarity Administrator must be prepared to perform switch firmware updates exactly as it is prepared to update node firmware. If not already done, refer to “[Preparing to update ThinkAgile SXM firmware](#)” on page 5 and “[Configure XClarity Administrator for a specific Best Recipe](#)” on page 6 to prepare XClarity Administrator to update the switch firmware.

Once XClarity Administrator has been prepared to update the firmware on the switches, it is important to verify that the Azure Stack Hub environment is healthy. Sign in to the Azure Stack Hub Administrator Portal and verify that no alerts are displayed. We will refer back to the portal throughout this process to check the general health of the solution.

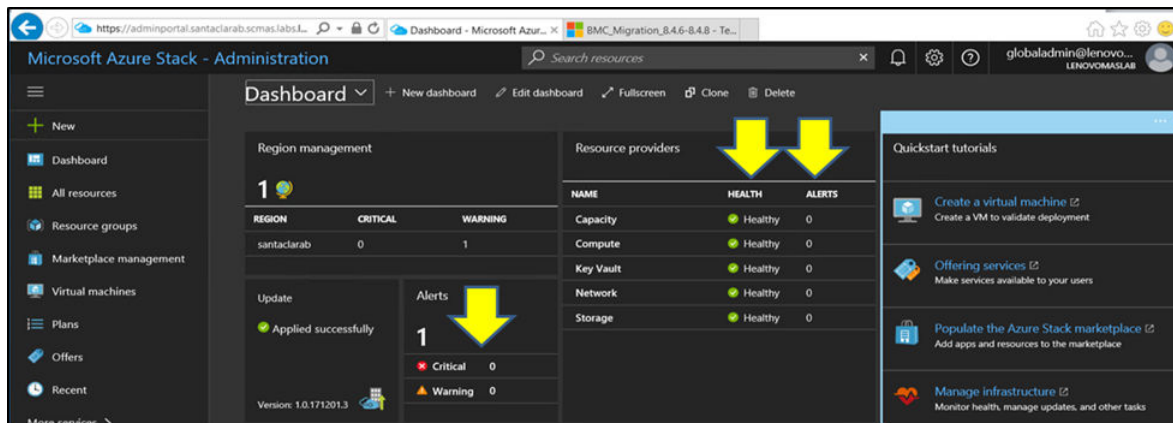


Figure 30. Verifying Azure Stack Hub health before update

Update Lenovo TOR switch firmware

This topic outlines the sequence of steps required to update the CNOS image of the TOR switches.

Back up Lenovo TOR switch configurations

Before beginning the update procedure, ensure that both Lenovo TOR switch configurations have been backed up.

Backing up the switch configuration files from the TOR switches is a simple matter of a few clicks in XClarity Administrator. Follow these steps:

- Step 1. At the top menu of the XClarity Administrator browser interface, select **Hardware** → **Switches**.
- Step 2. Select both TOR switches by clicking the checkbox to the left of each switch.

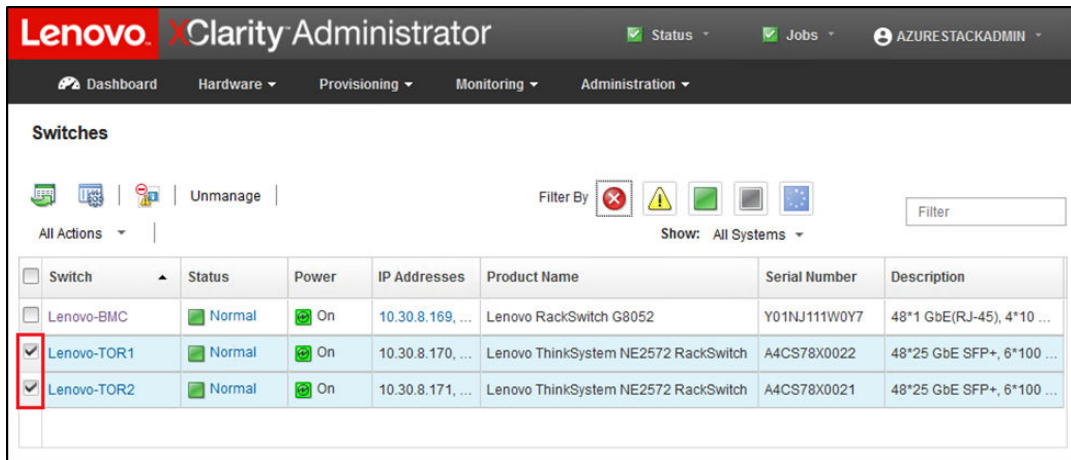


Figure 31. Selecting both TOR switches

- Step 3. Select **All Actions** → **Configuration** → **Backup configuration file**.

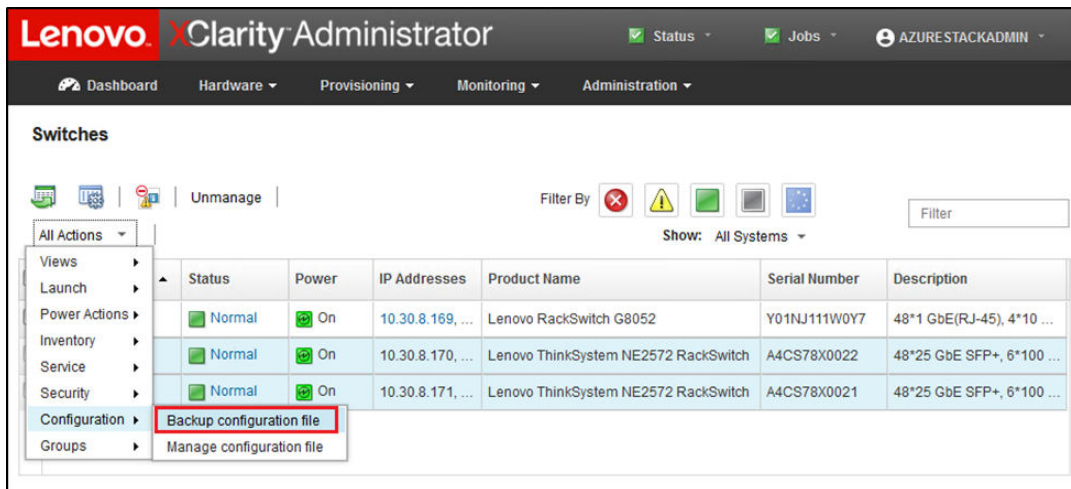


Figure 32. Backing up TOR configuration file

- Step 4. Verify that both TOR switches display in the **Selected Switches** field. Enter a descriptive comment for the backup, and click **Backup**.

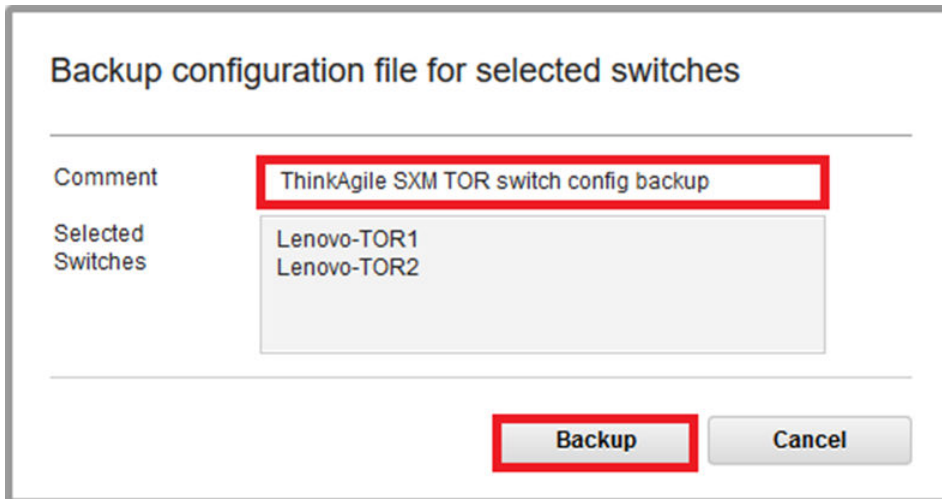


Figure 33. Backup configuration file dialog box

Step 5. The window should confirm successful backup. Click **Close** to dismiss this window.

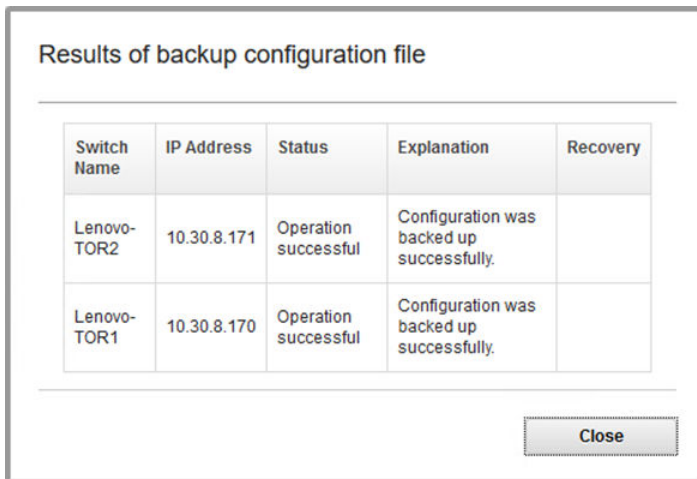


Figure 34. Backup configuration file results

Step 6. The backup switch configuration files are stored internal to XClarity Administrator, but it is a good idea to save a more accessible copy. To save a copy to the HLH, click a switch to open a detailed view of the switch.

Step 7. In the left pane, select **Configuration Files**, and click the checkbox to the left of the file name to select the backed up configuration file.

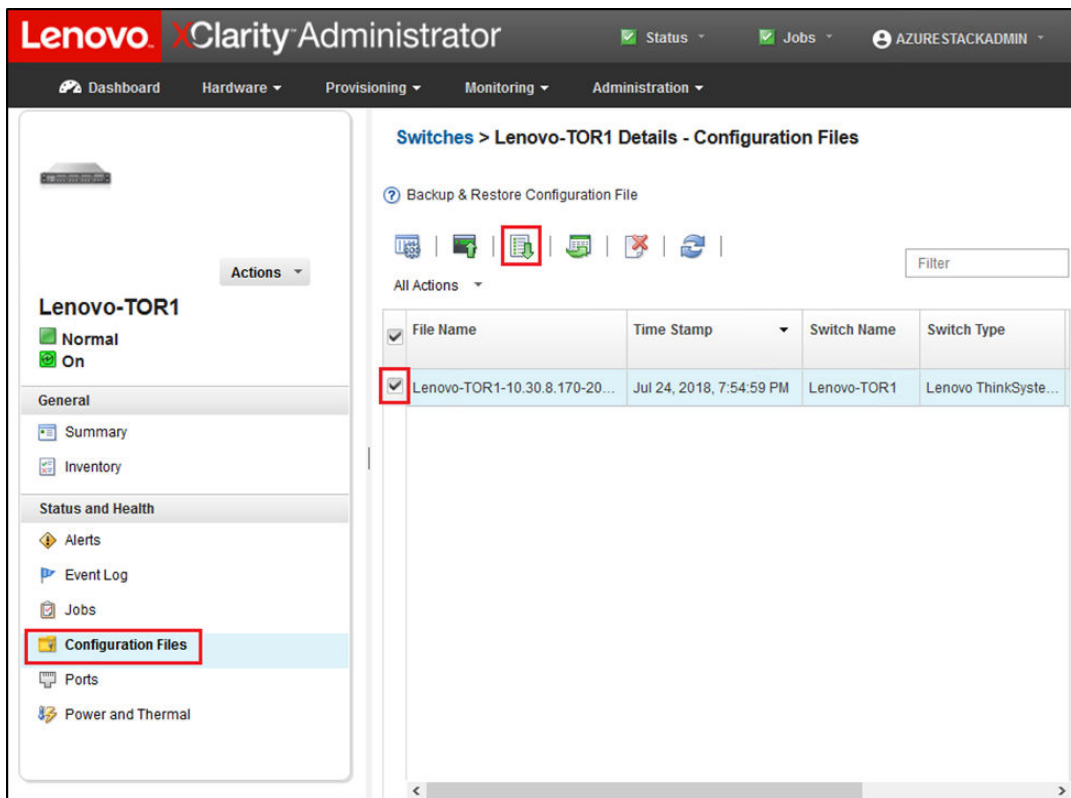




Figure 35. Selecting backup configuration file to download to local PC

- Step 8. Click the **Download configuration file from XClarity to local PC** button ()
- Step 9. Depending on the browser being used, specify a download location and save the file. The default file name provided by XClarity Administrator is in the following format: <SwitchHostname>-<IPAddress>-<Date>-<Time>.cfg.
- Step 10. Repeat steps 6 through 9 for the other TOR switch.
- Step 11. If not already present, create the directory D:\Lenovo\SwitchConfigBackups on the HLH and move the TOR configuration backup files into this directory.

Update CNOS on Lenovo TOR switches

With the switch configuration files backed up, update the Lenovo TOR switch firmware using XClarity Administrator.

The process includes updating the firmware on a single TOR switch, validating TOR switch functionality, and updating the other TOR switch and confirming functionality. To update the first TOR switch, follow these steps:

- Step 1. Use the XClarity Administrator top menu to navigate to **Provisioning → Apply / Activate**.
- Step 2. Verify that the TOR switches display as “Not Compliant” for the Best Recipe firmware update policy assigned to them. In the example screenshot below, the TOR switches are non-compliant, but the BMC switch is shown as “Compliant” so it does not need to be updated.
- Step 3. Select the TOR1 switch by clicking the checkbox to the left, and click **Perform Updates** ()

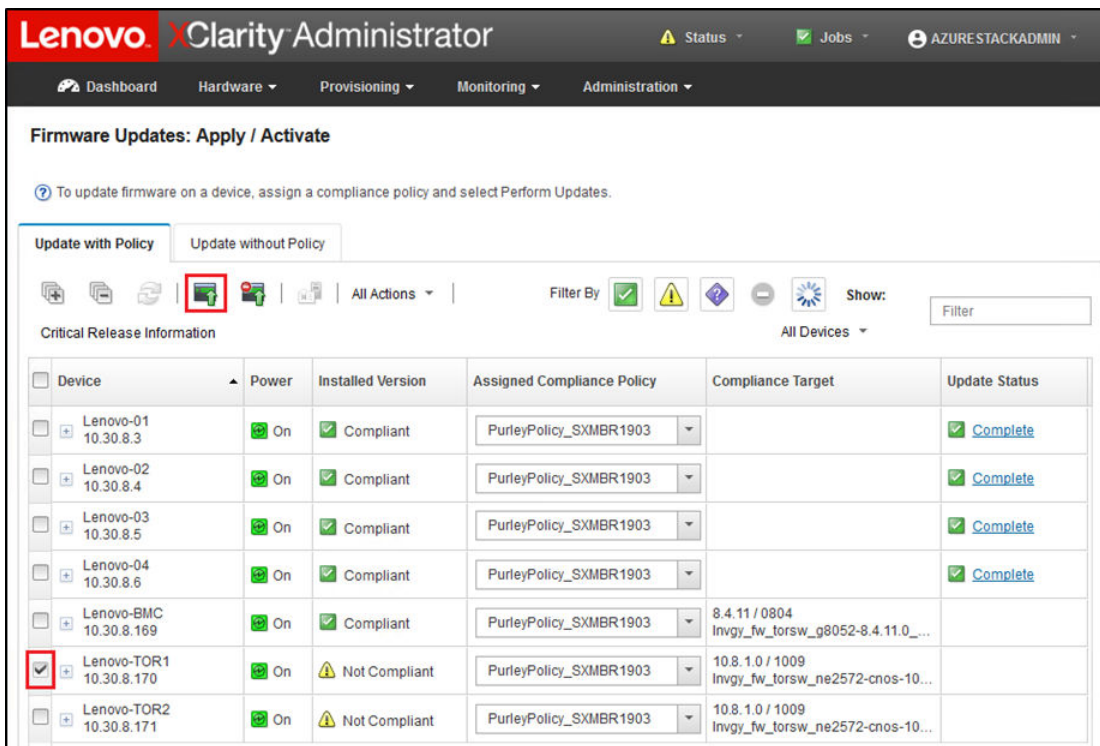


Figure 36. Selecting TOR1 switch for update

Step 4. In the Update Summary window, set the following options, and select **Perform Update**:

- Update Rule: **Stop all updates on error**
- Activation Rule: **Immediate activation**

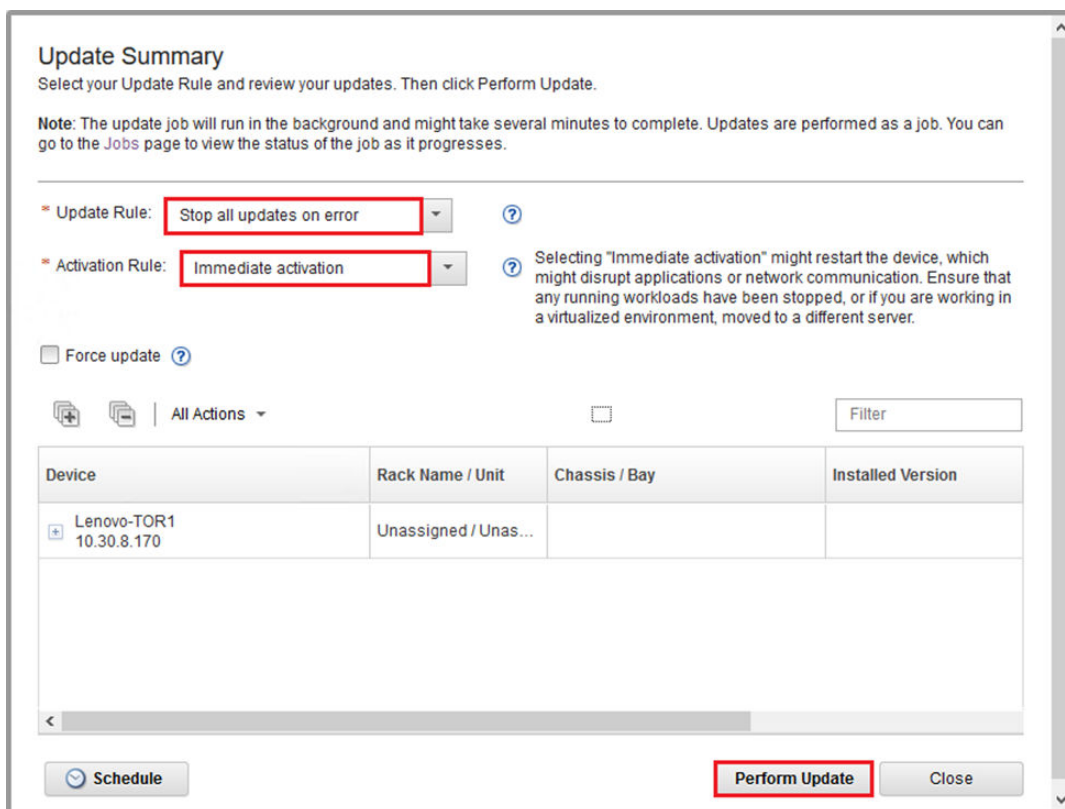


Figure 37. Selecting options in the TOR1 Update Summary

Step 5. Open the Jobs page to follow the update progress.

Lenovo XClarity Administrator Status Jobs AZURESTACKADMIN

Dashboard Hardware Provisioning Monitoring Administration

Jobs Page > Firmware Updates

Job	Start	Complete	Targets	Status
<input type="checkbox"/> Firmware Updates	January 9, 2019 at 15:08:26		Lenovo-TOR1	Executing - 64.00%
<input type="checkbox"/> Firmware Updates <ul style="list-style-type: none"> <input type="checkbox"/> Lenovo-TOR1 	January 9, 2019 at 15:08:26		Lenovo-TOR1	Executing - 64.00%
<input checked="" type="checkbox"/> RackSwitch Readiness Check	January 9, 2019 at 15:08:26	January 9, 2019 at 15:08:26	Lenovo-TOR1	Complete
<input type="checkbox"/> Applying RackSwitch firmware	January 9, 2019 at 15:08:28		Lenovo-TOR1	Executing - 28.00%

Summary for *Firmware Updates* job and sub-jobs

No summary available

Lenovo XClarity Administrator Status Jobs AZURESTACKADMIN

Dashboard Hardware Provisioning Monitoring Administration

Jobs Page > Firmware Updates


Job	Start	Complete	Targets	Status
<input checked="" type="checkbox"/> Firmware Updates	January 9, 2019 at 15:08:26	January 9, 2019 at 15:13:20	Lenovo-TOR1	Complete
<input checked="" type="checkbox"/> Firmware Updates <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Lenovo-TOR1 	January 9, 2019 at 15:08:26	January 9, 2019 at 15:13:20	Lenovo-TOR1	Complete
<input checked="" type="checkbox"/> RackSwitch Readiness Check	January 9, 2019 at 15:08:26	January 9, 2019 at 15:08:26	Lenovo-TOR1	Complete
<input checked="" type="checkbox"/> Applying RackSwitch firmware	January 9, 2019 at 15:08:28	January 9, 2019 at 15:13:20	Lenovo-TOR1	Complete

Summary for *Applying RackSwitch firmware* job and sub-jobs

Severity: i Informational
 Description: The task has completed successfully.
 Action: No action required for this task.

Figure 38. Update progress on Jobs Page

Step 6. Return to the Firmware Updates: Apply / Activate page in XClarity Administrator to verify that the new switch firmware is now running in the Active image on the TOR switch. You may need to click

Refresh () to get an accurate display.

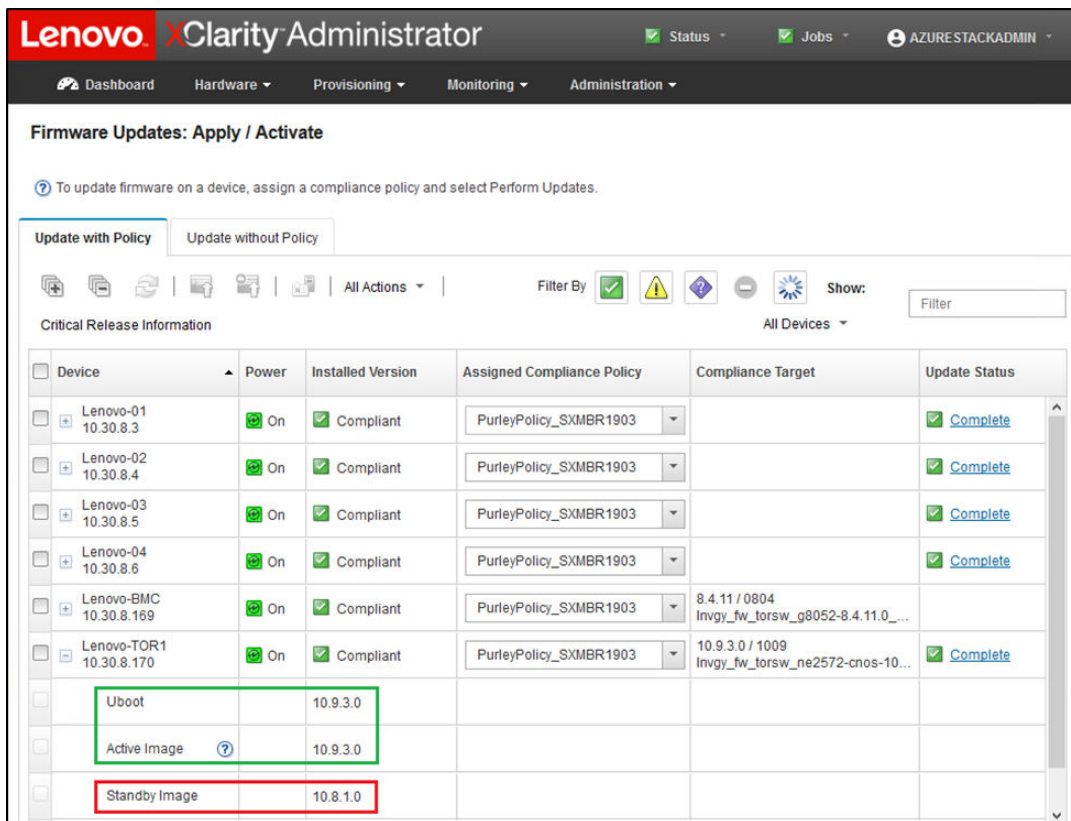


Figure 39. Active and standby images

Note: For the TOR switches running CNOS, XClarity Administrator updates only the Uboot and standby image and makes it the active image before reloading the switch. Therefore, the “N-1” switch firmware version from a Best Recipe perspective is always available as the standby image. In the screenshot above, The Uboot and Active image are running the new firmware (shown in the green box) and the Standby image still holds the previous firmware (shown in the red box).

Step 7. From an SSH session with the TOR switch that was just updated (you can use PuTTY, which is available on the HLH), issue the following command to save the running configuration to the startup configuration.

```
write
```

Verify Lenovo TOR switch functionality

After updating the Lenovo TOR switch, ensure that the switch is fully functional, based on the solution configuration.

In addition to comparing the running configuration of the switch to the backup configuration file saved before updating the switch firmware, the following suggested validation procedures help to verify that:

- Switch NOS is updated and set to boot to it
- vLAG ISL is intact and operational
- BGP connections are up and sessions are established
- VRRP master and backup are up and forwarding
- All links are up and IP addresses are assigned
- ACLs are in place and counters are incrementing

Perform the following tasks to ensure that the updated TOR switch is working properly before proceeding. Use PuTTY on the HLH to connect to the TOR switch. Select **Yes** in the PuTTY Security Alert that displays.

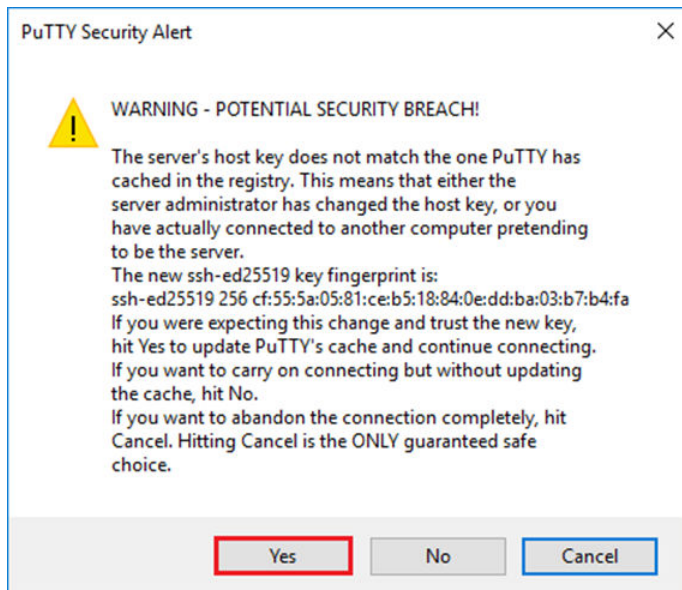


Figure 40. PuTTY security alert

Verify Lenovo TOR switch update

To verify that the Lenovo TOR switch NOS update has been applied, enter the following command:

```
Show version
```

```
Example
Lenovo-TOR1#show version
Lenovo Networking Operating System (NOS) Software
Technical Assistance Center: http://www.lenovo.com
Copyright (C) Lenovo, 2016. All rights reserved.

Software:
  Bootloader version: 10.8.1.0
  System version: 10.8.1.0
  System compile time: Jul 18 17:06:53 PDT 2018
Hardware:
  NE2572 ("48x25GE + 6x100GE")
  Intel(R) Celeron(R) CPU with 8192 MB of memory

  Device name: Lenovo-TOR1
  Boot Flash: 16 MB

Kernel uptime is 0 day(s), 0 hour(s), 6 minute(s), 46 second(s)

Last Reset Reason: Power Cycle
Lenovo-TOR1#

2019-01-09T23:18:00.924+00:00 Lenovo-TOR1(cnos:default) %VLAG-5-OS_MISMATCH: vLAG OS version mismatch,
local OS version is 10.8.x.x peer OS version is 10.6.x.x
2019-01-09T23:18:10.924+00:00 Lenovo-TOR1(cnos:default) %VLAG-5-OS_MISMATCH: vLAG OS version mismatch,
local OS version is 10.8.x.x peer OS version is 10.6.x.x
```

Note: You might see informational messages display periodically, as shown at the end of the example above, indicating an OS mismatch between the two TOR switches. This is expected at this point in the process. These messages should stop displaying after updating the second TOR switch.

Verify boot image

To verify that the TOR switch is set to boot to the new firmware image (which is now the active image), enter the following command:

```
show boot
```

Example

```
Lenovo-TOR1#show boot
Current ZTP State: Enable
Current FLASH software:
  active image: version 10.8.1.0, downloaded 00:33:35 PST Thu Jan 10 2019
  standby image: version 10.6.1.0, downloaded 18:24:35 PST Fri Jan 12 2018
  Grub: version 10.8.1.0, downloaded 23:09:14 PST Wed Jan  9 2019
  BIOS: version 020AB, release date 02/14/2018
  Secure Boot: Enabled
  ONIE: version unknown, downloaded unknown
Currently set to boot software active image
Current port mode:
  Port Ethernet1/37 is set in 10G mode
  Port Ethernet1/38 is set in 10G mode
  Port Ethernet1/39 is set in 10G mode
  Port Ethernet1/40 is set in 10G mode
  Port Ethernet1/45 is set in 10G mode
  Port Ethernet1/46 is set in 10G mode
  Port Ethernet1/47 is set in 10G mode
  Port Ethernet1/48 is set in 10G mode
Next boot port mode:
  Port Ethernet1/37 is set in 10G mode
  Port Ethernet1/38 is set in 10G mode
  Port Ethernet1/39 is set in 10G mode
  Port Ethernet1/40 is set in 10G mode
  Port Ethernet1/45 is set in 10G mode
  Port Ethernet1/46 is set in 10G mode
  Port Ethernet1/47 is set in 10G mode
  Port Ethernet1/48 is set in 10G mode
Currently scheduled reboot time: none
```

Verify links

To verify that all links are up and IP addresses are assigned, run the following command:

```
show interface brief | include up
```

Example

```
Lenovo-TOR1#show interface brief | include up
Ethernet1/1      7      eth trunk up      none      25000    --
Ethernet1/2      7      eth trunk up      none      25000    --
Ethernet1/3      7      eth trunk up      none      25000    --
Ethernet1/4      7      eth trunk up      none      25000    --
Ethernet1/40     --     eth routed up     none      10000    --
Ethernet1/43     --     eth routed up     none      25000    --
Ethernet1/44     --     eth routed up     none      25000    --
Ethernet1/47     --     eth routed up     none      10000    --
Ethernet1/48     --     eth routed up     none      10000    --
Ethernet1/49     99     eth trunk up      none      100000   101
Ethernet1/50     99     eth trunk up      none      100000   101
po101            99     eth trunk up      none      100000   lacp
mgmt0            management up      10.30.8.170      1000 1500
Vlan7            --     up      --
Vlan107         --     up      --
loopback0        up      Loopback0_Rack1_TOR1
```

Note: The state of Ethernet interfaces 1/5 through 1/16 depend on the number of nodes in the scale unit. The above example is taken from a 4-Node SXM4400 solution.

Verify vLAG ISL

To verify that the vLAG ISL is intact and operational, run the following command:

```
show vlag information
```

Example

```
Lenovo-TOR1#show vlag information
Global State:          enabled
VRRP active/active mode: enabled
vLAG system MAC:      08:17:f4:c3:dd:63
ISL Information:
  PCH      Ifindex      State      Previous State
  -----+-----+-----+-----
  101      100101      Active     Inactive

Mis-Match Information:
                Local                Peer
  -----+-----+-----+-----
Match Result : Match                Match
Tier ID      : 100                  100
System Type  : NE2572                NE2572
OS Version   : 10.8.x.x              10.8.x.x

Role Information:
                Local                Peer
  -----+-----+-----+-----
Admin Role   : Primary                Secondary
Oper Role    : Secondary              Primary
Priority     : 0                      0
System MAC   : a4:8c:db:bb:0b:01      a4:8c:db:bb:0c:01

Consistency Checking Information:
State        : enabled
Strict Mode  : disabled
Final Result : pass
```

Verify BGP is operational

To verify that the BGP connections are up and sessions are established, run the following command:

```
show ip bgp summary
```

Example

```
Lenovo-TOR1#show ip bgp summary
BGP router identifier 10.30.8.152, local AS number 64675
BGP table version is 74
2 BGP AS-PATH entries
0 BGP community entries
8 Configured ebgp ECMP multipath: Currently set at 8
8 Configured ibgp ECMP multipath: Currently set at 8

Neighbor      V      AS MsgRcv MsgSen TblVer InQ  OutQ Up/Down State/PfxRcd
10.30.8.146   4  64675   72    74    74    0    0 01:09:14     5
10.30.8.158   4  64675   74    74    74    0    0 01:09:15    33
10.30.8.162   4  64675   74    74    74    0    0 01:09:24    33
10.30.29.12   4  64719  235   215    74    0    0 01:09:17    25
10.30.29.13   4  64719  235   214    74    0    0 01:09:17    25

Total number of neighbors 5

Total number of Established sessions 5
```

Note that the above example is from a statically routed solution. A solution using dynamic routing also includes two BGP sessions for the Border switches, totaling 7 sessions.

Verify VRRP is operational

To verify that the VRRP master and backup are up and forwarding, run the following command on each TOR switch:

```
show vrrp vlag
```

Example

```
Lenovo-TOR1#show vrrp vlag
Flags: F - Forwarding enabled on Backup for vLAG
vLAG enabled, mode: vrrp active
Interface      VR  IpVer Pri Time    Pre State  VR IP addr
-----
(F)Vlan7       7  IPV4  100 100  cs  Y   Backup 10.30.29.1
(F)Vlan107     107 IPV4  100 100  cs  Y   Backup 10.30.28.1

Lenovo-TOR2#show vrrp vlag
Flags: F - Forwarding enabled on Backup for vLAG
vLAG enabled, mode: vrrp active
Interface      VR  IpVer Pri Time    Pre State  VR IP addr
-----
Vlan7          7  IPV4  100 100  cs  Y   Master 10.30.29.1
Vlan107        107 IPV4  100 100  cs  Y   Master 10.30.28.1
```

Verify ACLs are present and operational

To verify that ACLs are in place and counters are incrementing, run the following commands:

```
show ip access-lists summary
show ip access-lists
```

Example

```
Lenovo-TOR-1#show ip access-lists summary
IPV4 ACL Rack01-CL01-SU01-Infra_IN
  statistics enabled
  Total ACEs Configured: 28
  Configured on interfaces:
    Vlan7 - ingress (Router ACL)
  Active on interfaces:
    Vlan7 - ingress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL Rack01-CL01-SU01-Infra_OUT
  statistics enabled
  Total ACEs Configured: 28
  Configured on interfaces:
    Vlan7 - egress (Router ACL)
  Active on interfaces:
    Vlan7 - egress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL Rack01-CL01-SU01-Stor_IN
  statistics enabled
  Total ACEs Configured: 6
  Configured on interfaces:
    Vlan107 - ingress (Router ACL)
  Active on interfaces:
    Vlan107 - ingress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL Rack01-CL01-SU01-Stor_OUT
  statistics enabled
  Total ACEs Configured: 6
  Configured on interfaces:
    Vlan107 - egress (Router ACL)
  Active on interfaces:
    Vlan107 - egress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL UPLINK_ROUTED_IN
  statistics enabled
  Total ACEs Configured: 4
  Configured on interfaces:
    Ethernet1/47 - ingress (Router ACL)
    Ethernet1/48 - ingress (Router ACL)
  Active on interfaces:
    Ethernet1/47 - ingress (Router ACL)
  Configured and active on VRFs:
IPV4 ACL copp-system-acl-authentication
  Total ACEs Configured: 3
  Configured on interfaces:
  Active on interfaces:
  Configured and active on VRFs:
IPV4 ACL copp-system-acl-bgp
  Total ACEs Configured: 2
  Configured on interfaces:
  Active on interfaces:
  Configured and active on VRFs:
...
```

Example

```
Lenovo-TOR-1#show ip access-lists
IP access list Rack01-CL01-SU01-Infra_IN
  statistics per-entry
  500 remark "Permit R01-C01-SU01-INF (10.20.25.0/24)_TO_R01-C01-SU01-INF
(10.20.25.0/24)"
  510 permit any 10.20.25.0/24 10.20.25.0/24 [match=70214264]
  520 remark "Permit R01-C01-SU01-INF (10.20.25.0/24)_TO_azs-hlh-dvm00 (10
.20.3.61/32)"
  530 permit any 10.20.25.0/24 host 10.20.3.61 [match=11180]
  540 remark "Permit R01-C01-SU01-INF (10.20.25.0/24)_TO_R01-C01-SU01-InVI
P (10.20.126.128/25)"
  550 permit any 10.20.25.0/24 10.20.126.128/25
  560 remark "Permit R01-C01-SU01-InVIP (10.20.126.128/25)_TO_R01-C01-SU01
-INF (10.20.25.0/24)"
  570 permit any 10.20.126.128/25 10.20.25.0/24 [match=27814360]
  580 remark "Permit R01-C01-SU01-INF (10.20.25.0/24)_TO_pub-adm-vip (10.2
0.23.0/27)"
  590 permit any 10.20.25.0/24 10.20.23.0/27 [match=80158]
  600 remark "Permit pub-adm-vip (10.20.23.0/27)_TO_R01-C01-SU01-INF (10.2
0.25.0/24)"
  610 permit any 10.20.23.0/27 10.20.25.0/24 [match=76824]
  620 remark "Permit 112 any (0.0.0.0/0)_to_Multicast (224.0.0.18/32)"
  630 permit 112 any host 224.0.0.18 [match=62576]
  640 remark "Permit UDP any_TO_any(BOOTP) port 67"
  650 permit udp any any eq bootps [match=443]
...
```

Verify solution network connectivity

Once the basic system convergence is verified in the updated Lenovo TOR switch, test solution connectivity using the following steps:

1. Use the top menu of the XClarity Administrator browser interface to navigate to **Administration** → **Network Access**.
2. Click the **Test Connection** button near the top of the interface.
3. In the **Host** field, enter 8.8.8.8, and click **Test Connection**.
4. A success window displays. Click **Close** to dismiss this window.
5. As an additional verification step, sign in to the Azure Stack Hub Administrator Portal.
6. Check the Azure Stack Hub Administrator Portal to ensure that no alerts are currently visible.

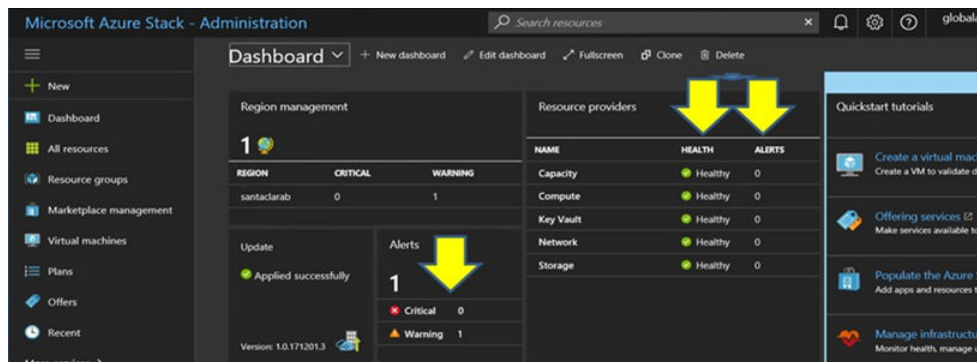


Figure 41. Checking Azure Stack Hub Administrator Portal for alerts

Wait until network traffic and reachability fully reconverge and the systems stabilize. Also check the Azure Stack Hub Administrator Portal to ensure all component status indicators are shown as healthy. Once the solution has stabilized, return to the “Update CNOS on TOR switches” topic and repeat the process on the other TOR switch. Once both TOR switches have been updated and their functionality and stability have been verified, proceed with the BMC switch update.

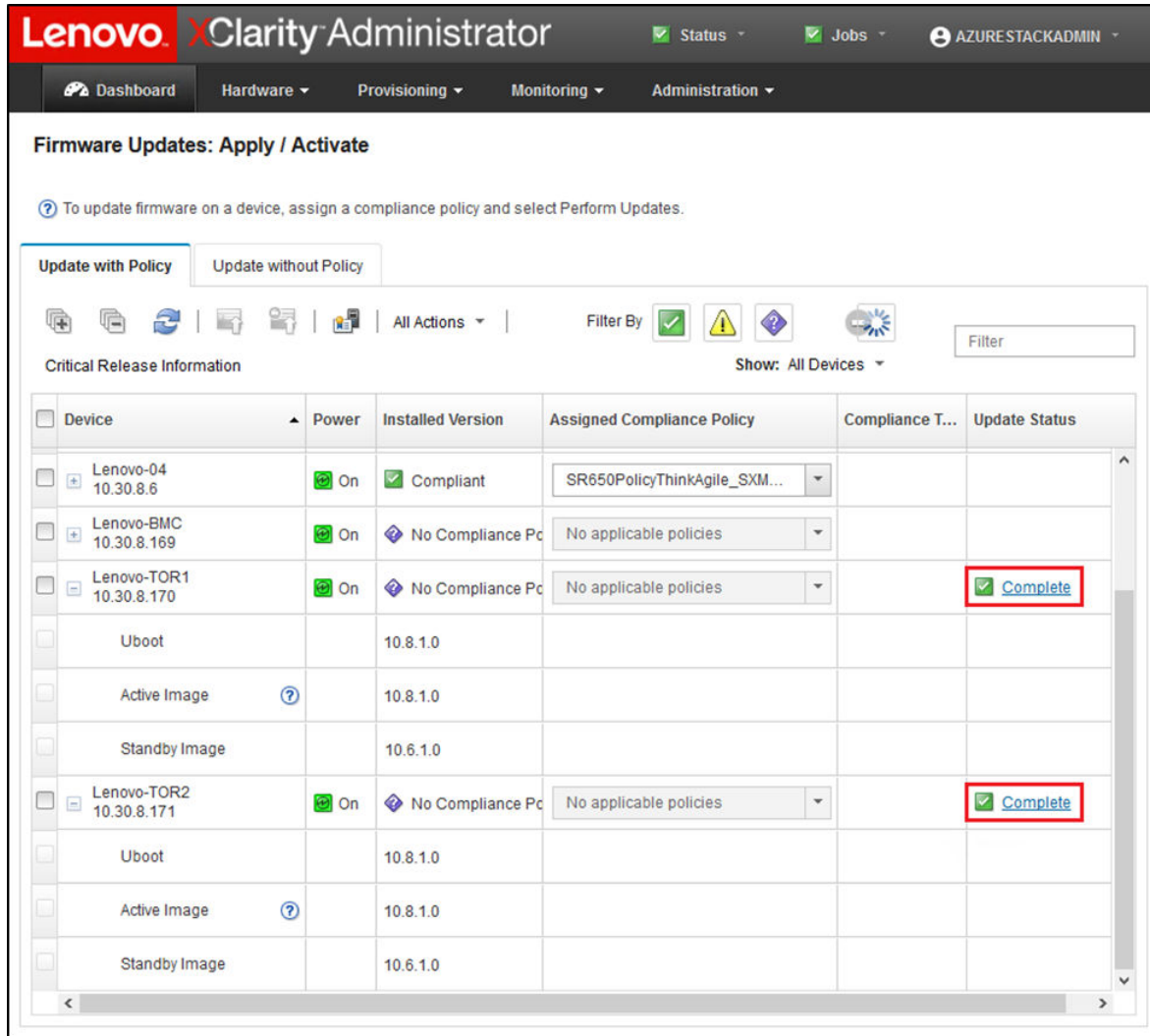


Figure 42. Verifying that TOR switch firmware updates are complete

Update Lenovo BMC switch firmware

This topic outlines the steps required to update the firmware image on a Lenovo BMC switch.

Note: If the Lenovo ThinkSystem NE0152T RackSwitch is not being managed by LXCA, use the steps in “Updating BMC switch firmware using the CLI” on page 97 to update this switch if it exists in your solution.

Back up BMC switch configuration

Before beginning the update procedure, ensure that the BMC switch configuration has been backed up.

Note: If the Lenovo ThinkSystem NE0152T RackSwitch is not being managed by LXCA, use the steps in “Updating BMC switch firmware using the CLI” on page 97 to update this switch if it exists in your solution.

Backing up the switch configuration files from a Lenovo BMC switch is simple in XClarity Administrator. Follow these steps:

- Step 1. At the top menu of the XClarity Administrator browser interface, select **Hardware → Switches**.
- Step 2. Click the checkbox to select the BMC switch.

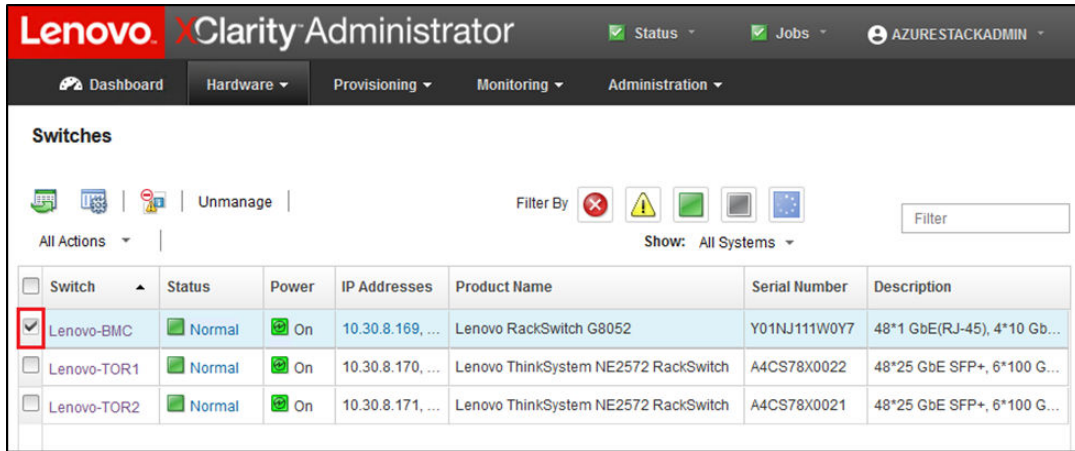


Figure 43. Selecting BMC switch for configuration backup

- Step 3. Select **All Actions → Configuration → Backup configuration file**.
- Step 4. In the window that displays, verify that the BMC switch displays in the **Selected Switches** field. Enter a descriptive comment for the backup, and click **Backup**.

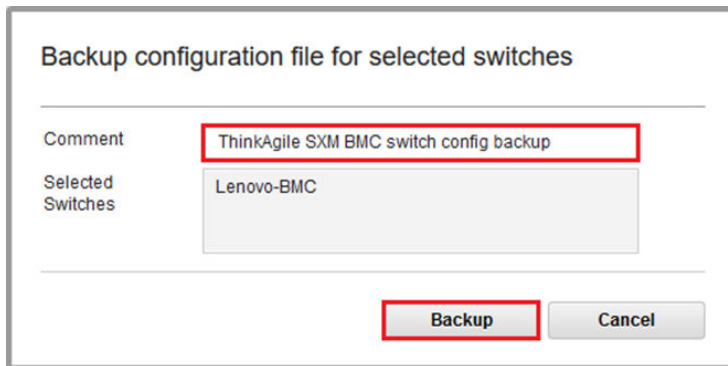


Figure 44. Verifying and commenting BMC switch for backup

- Step 5. A successful backup confirmation message displays. Click **Close** to dismiss this message.
- Step 6. The backup switch configuration files are stored internal to XClarity Administrator, but we must provide a more accessible copy. To save a copy to the HLH, click a switch to open a detailed view of the switch.
- Step 7. In the left pane, select **Configuration Files**, and click the checkbox next to the file name to select the backup configuration file.

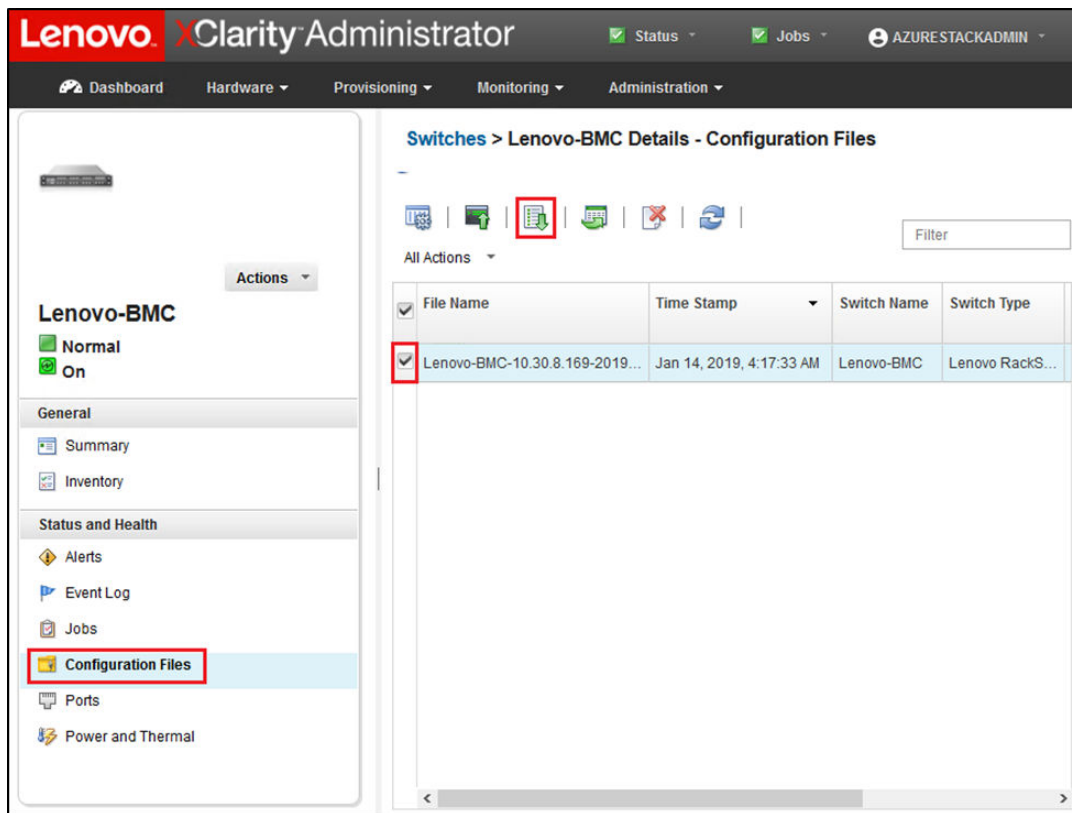



Figure 45. Selecting the configuration file backup for download


- Step 8. Click the **Download configuration file from XClarity to local PC** button ()
- Step 9. Depending on the browser being used, specify a download location and save the file. The default file name provided by XClarity Administrator is in the following format:
`<SwitchHostname>-<IPAddress>-<Date>-<Time>.cfg`
- Step 10. Move the BMC configuration backup file into the D:\Lenovo\Switch Config Backups directory on the HLH.

Update the Lenovo BMC switch

With the switch configuration file backed up, use XClarity Administrator to update the BMC switch firmware.

Note: If the Lenovo ThinkSystem NE0152T RackSwitch is not being managed by LXCA, use the steps in [“Updating BMC switch firmware using the CLI” on page 97](#) to update this switch if it exists in your solution.

The process includes updating the firmware on the BMC switch and validating BMC switch functionality. To update a Lenovo BMC switch, follow these steps:

- Step 1. Sign in to XClarity Administrator if necessary and use the top menu to navigate to **Provisioning** → **Apply / Activate**.
- Step 2. Verify that the BMC switch displays as “Not Compliant” for the Best Recipe firmware update Policy assigned to them. If the switch is shown as “Compliant,” no update is necessary.
- Step 3. If the switch is non-compliant, select the BMC switch by clicking the checkbox to the left of it, and click the **Perform Updates** button ()

- Step 4. In the Update Summary window that opens, set the following options, and click **Perform Update**:
- **Update Rule: Stop all updates on error**
 - **Activation Rule: Immediate activation**
 - **Install prerequisite firmware**

The screenshot shows the 'Update Summary' window with the following configuration:

- Update Rule: Stop all updates on error
- Activation Rule: Immediate activation
- Force update:
- Install prerequisite firmware:
- Memory test:

Below the options is a table with the following data:

Device	Rack Name / Unit	Chassis / Bay	Installed Version
HCI-Node01 10.241.83.201	M5 / Unit 1		

At the bottom of the window, there are three buttons: 'Schedule', 'Perform Update', and 'Close'. The 'Perform Update' button is highlighted with a red box.

Figure 46. Selecting BMC update and activation rules

- Step 5. Open the Jobs Page to follow the update progress.

Jobs Page > Firmware Updates

Job	Start	Complete	Targets	Status
✱ Firmware Updates	January 14, 2019 at 12:50:55		Lenovo-BMC	Executing - 64.00%
✱ Lenovo-BMC	January 14, 2019 at 12:50:55		Lenovo-BMC	Executing - 64.00%
✓ RackSwitch Readiness Check	January 14, 2019 at 12:50:55	January 14, 2019 at 12:50:56	Lenovo-BMC	Complete
✱ Applying RackSwitch firmware	January 14, 2019 at 12:50:57		Lenovo-BMC	Executing - 28.00%

Summary for Firmware Updates job and sub-jobs
No summary available


Jobs Page > Firmware Updates

Job	Start	Complete	Targets	Status
✓ Firmware Updates	January 14, 2019 at 12:50:55	January 14, 2019 at 12:54:51	Lenovo-BMC	Complete
✓ Lenovo-BMC	January 14, 2019 at 12:50:55	January 14, 2019 at 12:54:51	Lenovo-BMC	Complete
✓ RackSwitch Readiness Check	January 14, 2019 at 12:50:55	January 14, 2019 at 12:50:56	Lenovo-BMC	Complete
✓ Applying RackSwitch firmware	January 14, 2019 at 12:50:57	January 14, 2019 at 12:54:51	Lenovo-BMC	Complete

Summary for Applying RackSwitch firmware job and sub-jobs
Severity: i Informational
Description: The task has completed successfully.
Action: No action required for this task.

Figure 47. Following BMC update progress on Jobs Page

Step 6. Return to the Firmware Updates: Apply / Activate page in XClarity Administrator to verify that the new switch firmware is running in the Active image on the BMC switch. You may need to click the

Refresh button () to get an accurate display.

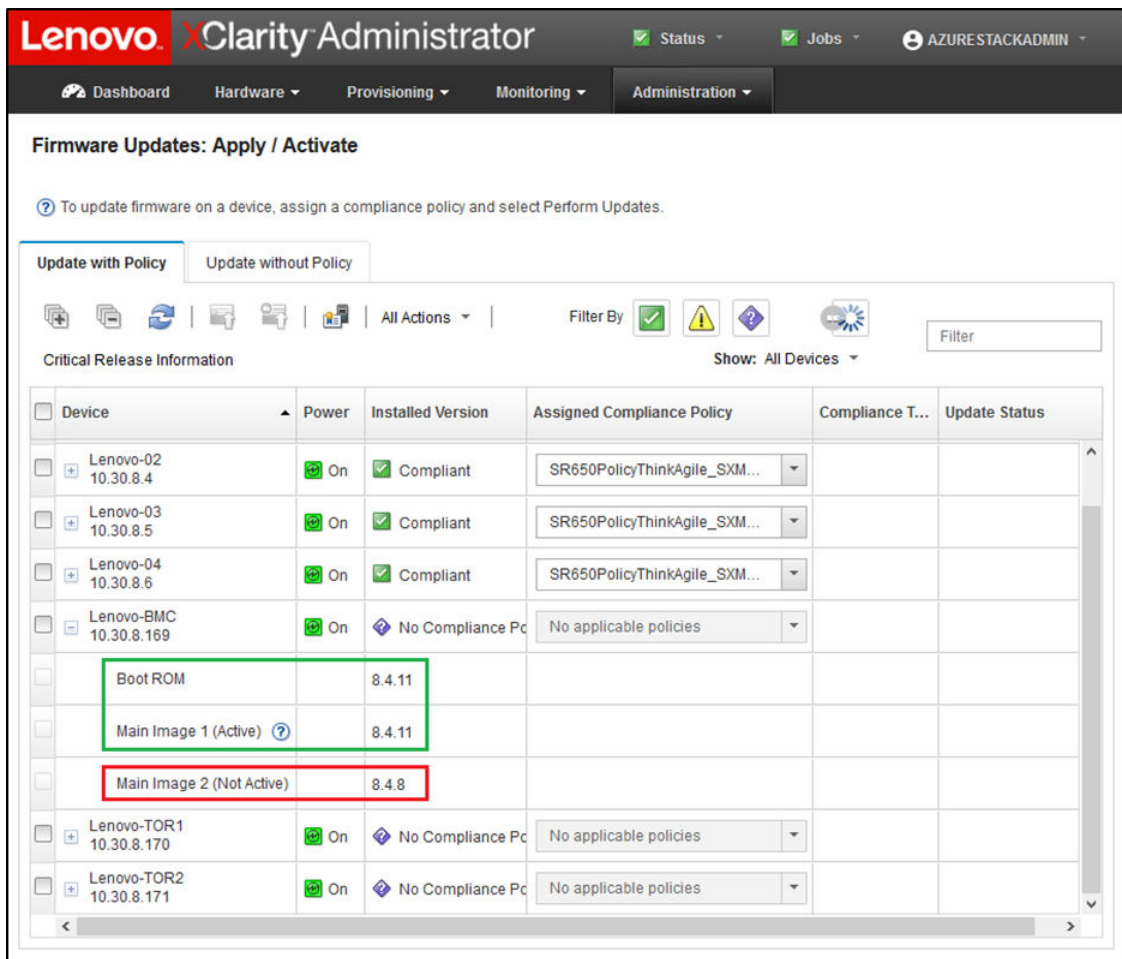


Figure 48. Verifying new BMC firmware running in active image

Note: For a Lenovo BMC switch running ENOS, XClarity Administrator updates only the non-active image and then makes this image the active image before reloading the switch. Therefore, the N-1 switch firmware version from a Best Recipe perspective is always available as the standby image. In the screenshot above, the boot ROM and active image (Main Image 1) are running the new firmware (shown in the green box). The non-active image (Main Image 2) still holds the previous firmware (shown in the red box).

Step 7. From an SSH session with the BMC switch (you can use PuTTY, which is available on the HLH), issue the following command to save the running configuration to the startup configuration.

```
copy running-config startup-config
```

Verify BMC switch functionality

After updating the BMC switch, ensure that the switch is fully functional, based on the solution configuration.

In addition to comparing the running configuration of the switch to the backup configuration file saved before updating the switch firmware, these suggested validation procedures help to verify that:

- Switch NOS is updated and set to boot to it
- All links are up and IP addresses are assigned
- BGP connections are up and sessions are established

- ACLs are in place and counters are incrementing

Perform each of the following tasks to ensure that the updated BMC switch is working properly before proceeding.

Verify BMC switch update

To verify that the switch NOS update has been applied and the switch is set to boot to the updated image, sign in to the BMC switch and run the following command:

```
show boot
```

Example

```
Lenovo-BMC#show boot
Current running image version: 8.4.11
Currently set to boot software image1, active config block.
NetBoot: disabled, NetBoot tftp server: , NetBoot cfgfile:
Current boot Openflow protocol version: 1.0
USB Boot: disabled
Currently profile is default, set to boot with default profile next time.
Current FLASH software:
  image1: version 8.4.11, downloaded 12:52:04 Mon Jan 14, 2019
           NormalPanel, Mode Stand-alone
  image2: version 8.4.8, downloaded 10:26:19 Mon Jan 14, 2019
           NormalPanel, Mode Stand-alone
  boot kernel: version 8.4.11
              NormalPanel
  bootloader : version 8.4.11
Currently scheduled reboot time: none
```

Verify links

To verify that all links are up and IP addresses are assigned, run the following command:

```
show interface link state up
```

Example

```
Lenovo-BMC#show interface link state up
-----
Alias  Port Speed  Duplex  Flow Ctrl  Link  Description
----- --TX-----RX-----
1      1    1000    full     no        no    up    BMC Mgmt Ports
2      2    1000    full     no        no    up    BMC Mgmt Ports
3      3    1000    full     no        no    up    BMC Mgmt Ports
4      4    1000    full     no        no    up    BMC Mgmt Ports
8      8    1000    full     no        no    up    BMC Mgmt Ports
46     8    1000    full     no        no    up    BMC Mgmt Ports
47     47   1000    full     no        no    up    Switch Mgmt Ports
48     48   1000    full     no        no    up    Switch Mgmt Ports
XGE1   49   10000   full     no        no    up    BMC Mgmt Ports
XGE2   50   10000   full     no        no    up    BMC Mgmt Ports
XGE3   51   10000   full     no        no    up    P2P_Rack1/TOR1_To_Rack1/BMC TOR Port 46
XGE4   52   10000   full     no        no    up    P2P_Rack1/TOR2_To_Rack1/BMC TOR Port 46
```

Note: The state of ports 1 through 16 depends on the number of nodes in the solution. The above example is from a 4-node solution.

Another useful command to verify IP configuration and state:

```
show interface ip
```

Example

```
Lenovo-BMC#show interface ip
Interface information:
5:      IP4 10.30.8.169      255.255.255.248 10.30.8.175,    vlan 5, up
6:      IP4 10.30.1.1       255.255.255.128 10.30.8.151,    vlan 6, up

Routed Port Interface Information:
XGE3: IP4 10.30.8.146      255.255.255.252 10.30.8.147    , routed , up
XGE4: IP4 10.30.8.150      255.255.255.252 10.30.8.151    , routed , up

Loopback interface information:
lo1: 10.30.30.26          255.255.255.255 10.30.30.26,    up
```

Verify BGP is operational

To verify that the BGP connections are up and sessions are established, run the following command:

```
show ip bgp neighbor summary
```

Example

```
Lenovo-BMC#show ip bgp neighbor summary
BGP ON
BGP router identifier 10.30.8.154, local AS number 64675
BGP thid 21, allocs 1168, frees 301, current 147124, largest 5784
BGP Neighbor Summary Information:
  Peer          V   AS   MsgRcvd  MsgSent  Up/Down  State
-----
1: 10.30.8.145  4   64675   106      104 01:41:23 established
2: 10.30.8.149  4   64675   106      104 01:41:23 established
```

Verify ACLs are present and operational

To verify that ACLs are in place and counters are incrementing, run the following command:

```
show access-control
show access-control group
show access-control counters
```

Example

```
Lenovo-BMC#show access-control
Current access control configuration:
```

```
Filter 200 profile:
```

```
IPv4
```

- SRC IP : 10.20.3.0/255.255.255.192
- DST IP : 10.20.3.0/255.255.255.192

```
Meter
```

- Set to disabled
- Set committed rate : 64
- Set max burst size : 32

```
Re-Mark
```

- Set use of TOS precedence to disabled

```
Actions : Permit
```

```
Statistics : enabled
```

```
Installed on vlan 125 in
```

```
ACL remark note
```

- "Permit R01-bmc (10.20.3.0/26)_TO_R01-bmc (10.20.3.0/26)"

```
Filter 202 profile:
```

```
IPv4
```

- SRC IP : 10.20.3.0/255.255.255.192
- DST IP : 10.20.30.40/255.255.255.248

```
Meter
```

- Set to disabled
- Set committed rate : 64
- Set max burst size : 32

```
Re-Mark
```

- Set use of TOS precedence to disabled

```
Actions : Permit
```

```
Statistics : enabled
```

```
Installed on vlan 125 in
```

```
ACL remark note
```

- "Permit R01-bmc (10.20.3.0/26)_TO_R01-SwitchMgmt (10.20.30.40/29)"

```
Filter 204 profile:
```

```
IPv4
```

- SRC IP : 10.20.3.61/255.255.255.255
- DST IP : 0.0.0.0/0.0.0.0

```
...
```


Example

```
Lenovo-BMC#show access-control group
Current ACL group Information:
-----
ACL group 1 (14 filter level consumed):

- ACL 200
- ACL 202
- ACL 204
- ACL 206
- ACL 208
- ACL 210
- ACL 212
- ACL 214
- ACL 216
- ACL 218
- ACL 220
- ACL 222
- ACL 224
- ACL 226
ACL group 2 (50 filter level consumed):

- ACL 228
- ACL 230
- ACL 232

...
```

Example

```
Lenovo-BMC#show access-control counters
ACL stats:
Hits for ACL 200  vlan 125  in      1357392
Hits for ACL 202  vlan 125  in      60229537
Hits for ACL 204  vlan 125  in     237099377
Hits for ACL 206  vlan 125  in         0
Hits for ACL 208  vlan 125  in         0
Hits for ACL 210  vlan 125  in         0
Hits for ACL 212  vlan 125  in         0
Hits for ACL 214  vlan 125  in         24
Hits for ACL 216  vlan 125  in         0
Hits for ACL 218  vlan 125  in     573818
Hits for ACL 220  vlan 125  in     800950
Hits for ACL 222  vlan 125  in         0
Hits for ACL 224  vlan 125  in         0
Hits for ACL 226  vlan 125  in     447369
Hits for ACL 228  vlan 125  in     1389622
Hits for ACL 230  vlan 125  in     59570795
Hits for ACL 232  vlan 125  in     174516137

...
```

Verify solution network connectivity

Once the basic system convergence is verified in the updated BMC switch, test connectivity for the following:

- Ping from BMC switch to connected TOR switch IP interfaces

Example

```
Lenovo-BMC#ping 10.30.8.130
[host 10.30.8.130, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.130: #1 ok, RTT 7 msec.
10.30.8.130: #2 ok, RTT 0 msec.
10.30.8.130: #3 ok, RTT 0 msec.
10.30.8.130: #4 ok, RTT 0 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.134
[host 10.30.8.134, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.134: #1 ok, RTT 0 msec.
10.30.8.134: #2 ok, RTT 0 msec.
10.30.8.134: #3 ok, RTT 0 msec.
10.30.8.134: #4 ok, RTT 0 msec.
Ping finished.
```

- Ping from BMC switch to TOR Mgmt IP addresses

Example

```
Lenovo-BMC#ping 10.30.8.170
[host 10.30.8.170, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.170: #1 ok, RTT 1 msec.
10.30.8.170: #2 ok, RTT 0 msec.
10.30.8.170: #3 ok, RTT 0 msec.
10.30.8.170: #4 ok, RTT 0 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.171
[host 10.30.8.171, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.171: #1 ok, RTT 0 msec.
10.30.8.171: #2 ok, RTT 0 msec.
10.30.8.171: #3 ok, RTT 0 msec.
10.30.8.171: #4 ok, RTT 0 msec.
Ping finished.
```

- Ping from BMC switch to node IMM/XCCs

Example

```
Lenovo-BMC#ping 10.30.8.3
[host 10.30.8.3, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.3: #1 ok, RTT 1 msec.
10.30.8.3: #2 ok, RTT 0 msec.
10.30.8.3: #3 ok, RTT 0 msec.
10.30.8.3: #4 ok, RTT 0 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.4
[host 10.30.8.4, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.4: #1 ok, RTT 0 msec.
10.30.8.4: #2 ok, RTT 1 msec.
10.30.8.4: #3 ok, RTT 1 msec.
10.30.8.4: #4 ok, RTT 1 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.5
[host 10.30.8.5, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.5: #1 ok, RTT 0 msec.
10.30.8.5: #2 ok, RTT 1 msec.
10.30.8.5: #3 ok, RTT 0 msec.
10.30.8.5: #4 ok, RTT 1 msec.
Ping finished.
Lenovo-BMC#ping 10.30.8.6
[host 10.30.8.6, max tries 4, delay 1000 msec, length 0, ping source N/S, ttl 255, tos 0]
10.30.8.6: #1 ok, RTT 1 msec.
10.30.8.6: #2 ok, RTT 1 msec.
10.30.8.6: #3 ok, RTT 1 msec.
10.30.8.6: #4 ok, RTT 1 msec.
Ping finished.
```

Fallback

If an issue prevents any of the switches from being updated, all switches must be returned to their initial state.

The following fallback process includes high-level steps to accomplish this. In general, the same commands specified in this document to perform the switch updates can be used to return the switches to their original state.

1. If one of the switch updates fails, do not proceed to another switch. If XClarity Administrator reports an error when attempting to transfer the image files to the switch, refer to [Appendix B “Updating ThinkAgile SXM Series switches using the CLI \(Lenovo switches only\)” on page 91](#) for instructions on using the switch CLI method to update switch firmware.
2. The original switch firmware is available in the “standby” image slot for all switches in the ThinkAgile SXM Series solution except the RackSwitch G8052 BMC switch. For this switch, the original firmware is available in the non-active image slot, which could be “image1” or “image2.” If a switch update fails, the switch can be reverted to the original firmware using the following command syntax:

All switches except the G8052: `boot image <standby | active`

RackSwitch G8052 BMC switch: `boot image <image1 | image2`

Important: Do not allow the TOR switches to run different versions of firmware except during the period in which TOR1 has been updated and the TOR2 update is pending. That is, if TOR1 fails to update properly, do not update TOR2. Also, if TOR2 fails to update properly, TOR1 must be reverted to the previous firmware until the update issue can be resolved.

3. The configuration file from each switch is backed up before updating the switches. These files are also saved to `D:\Lenovo\SwitchConfigBackups` on the HLH. Any switch can be restored to its backup configuration to restore the switch to its previous configuration.

Updated CNOS command syntax

With the release of Lenovo switch firmware CNOS v10.7.1.0, several CLI command keywords have changed for consistency.

The left table column shows the keyword used in CNOS versions 10.6.x and earlier. The right column shows the updated keyword used in CNOS versions 10.7.x and later.

Previous CLI Keyword	New CLI Keyword
configure device	configure terminal
routing-protocol	router
bridge-port	switchport
port-aggregation	port-channel
aggregation-group	channel-group
cancel	abort
startup	boot
remove	clear
cp	copy
apply	set
display	show
save	write
dbg	debug

Beginning with CNOS v10.7.1.0, the NOS advertised only new formats (end-user documentation, help strings, and so on). However, the NOS accepts and processes both old and new formats for a limited time. Therefore, the new NOS images contain messages that the old format will be deprecated in a future release.

Also note that although CNOS v10.7.1.0 and later accepts and processes old CLI commands, the information display shows only the new syntax. For example, any “routing-protocol” settings now display in the “router” section when looking at the switch running or startup configurations.

The information in a saved configuration file is not affected and remains intact with the old commands. To store the commands in a file in the new format, after reloading the switch to the v10.7.1.0 or later image, you must explicitly run `save/write` for each TOR switch.

Copy the newly saved configuration from all switches to the HLH for future reference. In addition, if XClarity Administrator v2.1 or later is installed and configured to manage the switches, back up all switch configurations using XClarity Administrator.

Chapter 4. Component service and replacement considerations

The ThinkAgile SXM Series components are precisely configured to provide the necessary solution-level functionality. Before attempting to service, replace, or reinstall any hardware and software component, you should review the relevant topic to ensure that you are aware of any specific procedures or requirements.

Replacing servers

ThinkAgile SXM Series solutions require specific configuration of the HLH and scale unit nodes. Use the following tips to help ensure successful server replacement.

HLH system replacement

When replacing the HLH system, do the following:

1. If Lenovo XClarity Administrator is still accessible, unmanage all Azure Stack Hub scale unit nodes and network switches.
2. If the HLH OS is still accessible, copy the D:\lenovo folder to a USB thumb drive for restoration.
3. After replacing the HLH hardware, ensure that the firmware level and UEFI settings are configured according to the ThinkAgile SXM Best Recipe. See [“Firmware maintenance and Best Recipe” on page 5](#) for more information.
4. Apply all platform security settings.
5. Configure the IMM or XCC IPv4 address according to the worksheet generated during the initial deployment.
6. Reconfigure the Supervisor-level account.
7. Remove the default USERID account from the IMM or XCC.
8. If available, copy the files from the backup USB thumb drive (from [2 on page 53](#) above) to D:\Lenovo on the replacement HLH system.
9. Reinstall Lenovo XClarity Administrator. See [Appendix A “XClarity Administrator deployment and configuration” on page 55](#).

Azure Stack Hub scale unit node replacement

When replacing an Azure Stack Hub scale unit node , do the following:

1. If the system is still responsive, use the Azure Stack Hub Administrator Portal to Drain the scale unit node that will be replaced.
2. In LXCA, unmanage the node.
3. Replace the scale unit node hardware.
4. Reconnect the network and power cables.
5. Configure the IMM/XCC IPv4 address according to the worksheet generated during the initial deployment.
6. Reconfigure the Supervisor-level account on the IMM/XCC to be managed by LXCA using the same credentials currently used for the other nodes.
7. Remove the default USERID account from the IMM/XCC.
8. Ensure that the firmware levels on the replacement node are configured according to the ThinkAgile SXM Best Recipe that is currently in use for the solution.

See [“Firmware maintenance and Best Recipe” on page 5](#) for more information.

9. Use Lenovo XClarity Administrator to apply the Microsoft Azure Stack Hub pattern UEFI settings. See [“Import and apply server pattern” on page 87](#) for more information.
10. Configure the boot volume as a RAID-1 mirror.

Replacing server parts

ThinkAgile SXM Series solutions require specific server configuration. Use the following tips to help ensure successful part replacement.

Requirement for product-specific server motherboard

In order to meet functional requirements, ThinkAgile SXM Series solutions require a specific motherboard Field Replaceable Unit (FRU) for the scale unit nodes and the HLH system. When attempting to service the scale unit nodes, make sure that your Support Engineer is aware of the following:

- Do not use common server motherboard spares.
- Always check the ThinkAgile SXM Series support information on the Web for the correct motherboard FRU part number.

Server hot-swap fans

The ThinkAgile SXM Series racks do not have cable management arms. To replace a hot-swap fan on the HLH or scale unit node, the server must be powered off and pulled out of the rack. Always make sure to Drain a scale unit node using the Azure Stack Hub Administrator Portal before powering it off for any reason.

RAID adapter for boot volume

The RAID adapter supports only the OS boot volume and not the storage devices that make up the solution storage pool.

1. Use Lenovo XClarity Administrator to update the adapter firmware to the same Best Recipe level that is currently in use for the solution. See [“Firmware maintenance and Best Recipe” on page 5](#).
2. Restore the RAID configuration to the drives.

Mellanox network adapter

1. Reconnect the cables according to the point-to-point diagrams and tables found in the appropriate topic:
 - For SXM4400/SXM6400 solutions, refer to https://pubs.lenovo.com/thinkagile-sxm/sxm_r2_network_cabling
 - For SXM4600 solutions, refer to https://pubs.lenovo.com/thinkagile-sxm/sxm_r3_network_cabling
2. Use Lenovo XClarity Administrator to update the adapter firmware to the same Best Recipe level that is currently in use for the solution. See [“Firmware maintenance and Best Recipe” on page 5](#).

Memory

No solution-specific configuration is required after replacement.

CPU

No solution-specific configuration is required after replacement.

Appendix A. XClarity Administrator deployment and configuration

Although it is typically not necessary to reinstall and configure XClarity Administrator (LXCA) from scratch for use with ThinkAgile SXM Series solutions, this document contains instructions to do so if it becomes necessary for any reason. This document also includes instructions to update LXCA to the version contained in the current ThinkAgile SXM Series Best Recipe.

Retire the current LXCA installation

If LXCA v2.x or later is deployed on the HLH, it is typically not necessary to retire LXCA. In this case, simply update LXCA to the version specified in the current Best Recipe. However, if LXCA v1.x is deployed on the HLH, perform the tasks shown here to retire the existing installation of LXCA. Then proceed to deploy LXCA from scratch in the next topics.

If LXCA v1.x is deployed on the HLH, perform these tasks to retire the existing installation of LXCA.

- Step 1. On the HLH, use Internet Explorer to sign in to LXCA.
- Step 2. Using the LXCA menu bar near the top of the screen, navigate to **Administration → Network Access**.
- Step 3. To prepare for configuring a fresh deployment of LXCA later, record the IPv4 settings of the current LXCA environment using the highlighted parameters in the following illustration. If for some reason LXCA is not accessible, these parameters are available in the Customer Deployment Summary document left with the customer after initial solution deployment.

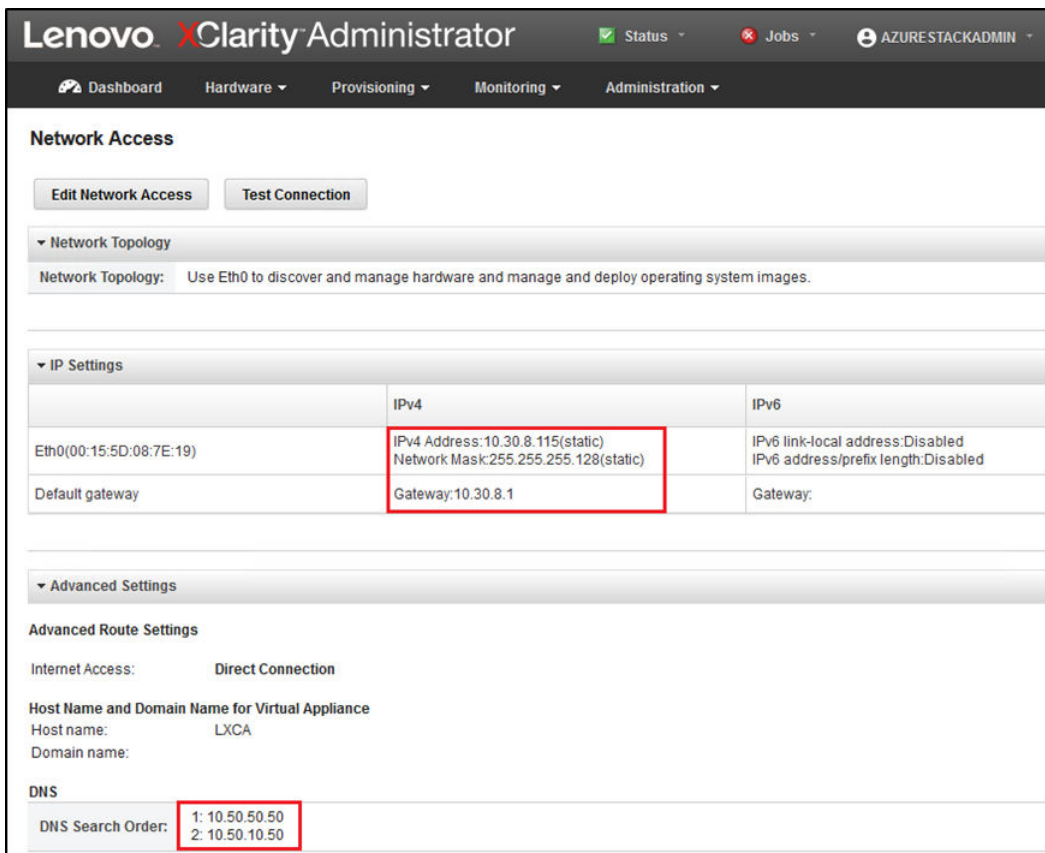



Figure 49. LXCA IPv4 settings to record

Record the settings in the following table:

	Lenovo LXCA IPv4 Settings
IPv4 Address	
Network Mask	
Gateway	
DNS Server 1	
DNS Server 2 (optional)	

Step 4. Using the LXCA menu bar near the top of the screen, navigate to **Provisioning** → **Server Profiles**.

Step 5. Select all server profiles shown, and click the **Deactivate Server Profiles** icon ()

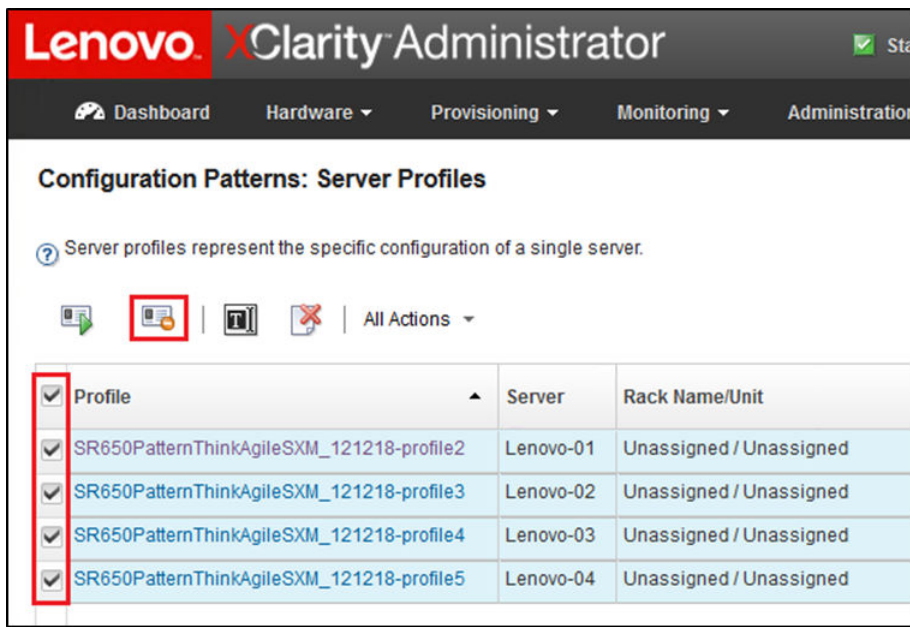


Figure 50. Selecting LXCA server profiles to deactivate

Step 6. In the window that is displayed, deselect (uncheck) the Reset BMC identity settings option if it is checked, and click **Deactivate**.

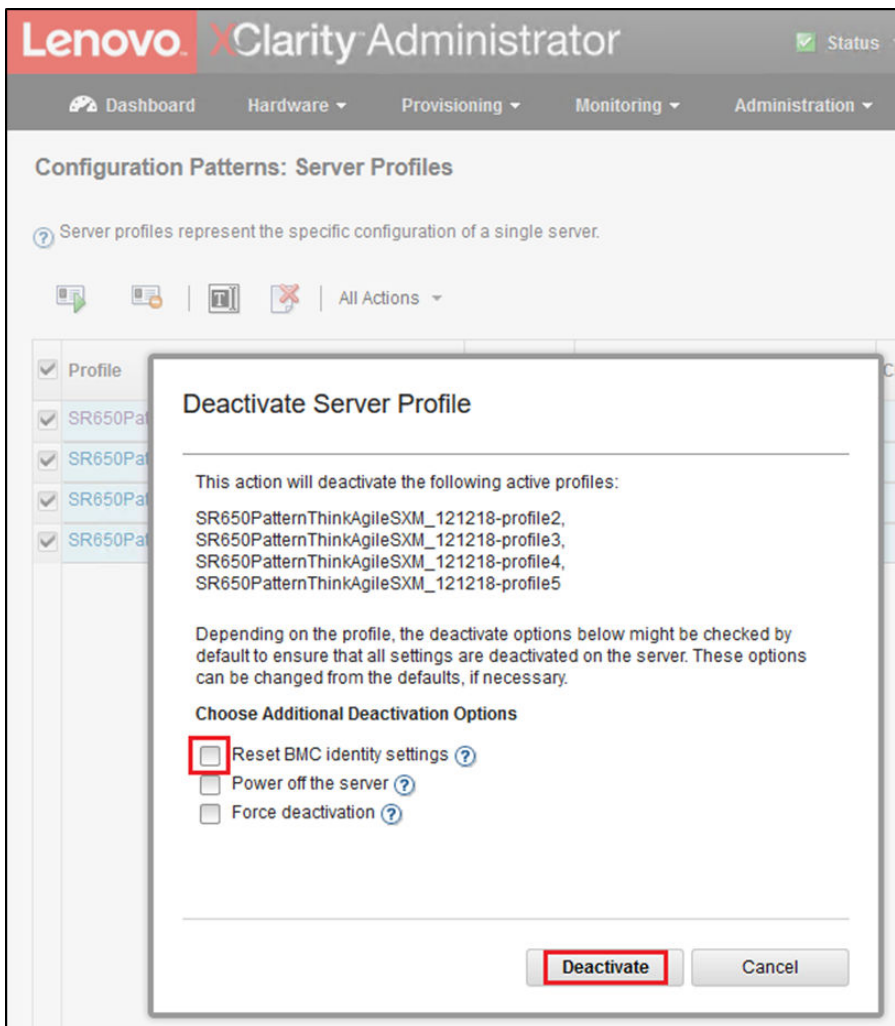


Figure 51. Resetting BMC identity settings

- Step 7. Using the LXCA menu bar near the top of the screen, navigate to **Hardware → Servers**.
- Step 8. Select all nodes and click **Unmanage**.

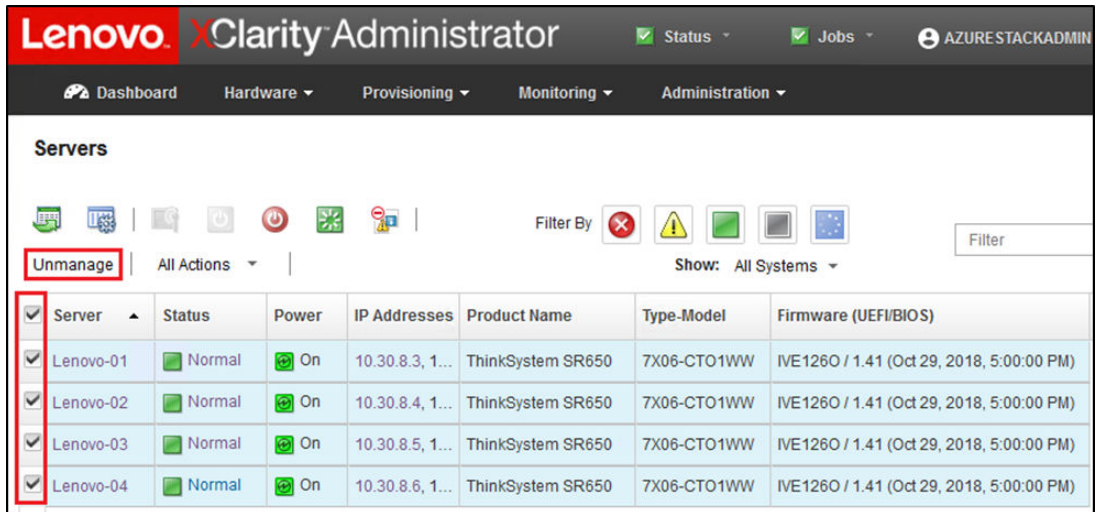


Figure 52. Unmanaging the nodes

Step 9. In the window that opens, select **Force unmanage even if the device is not reachable**, and click **Unmanage**.

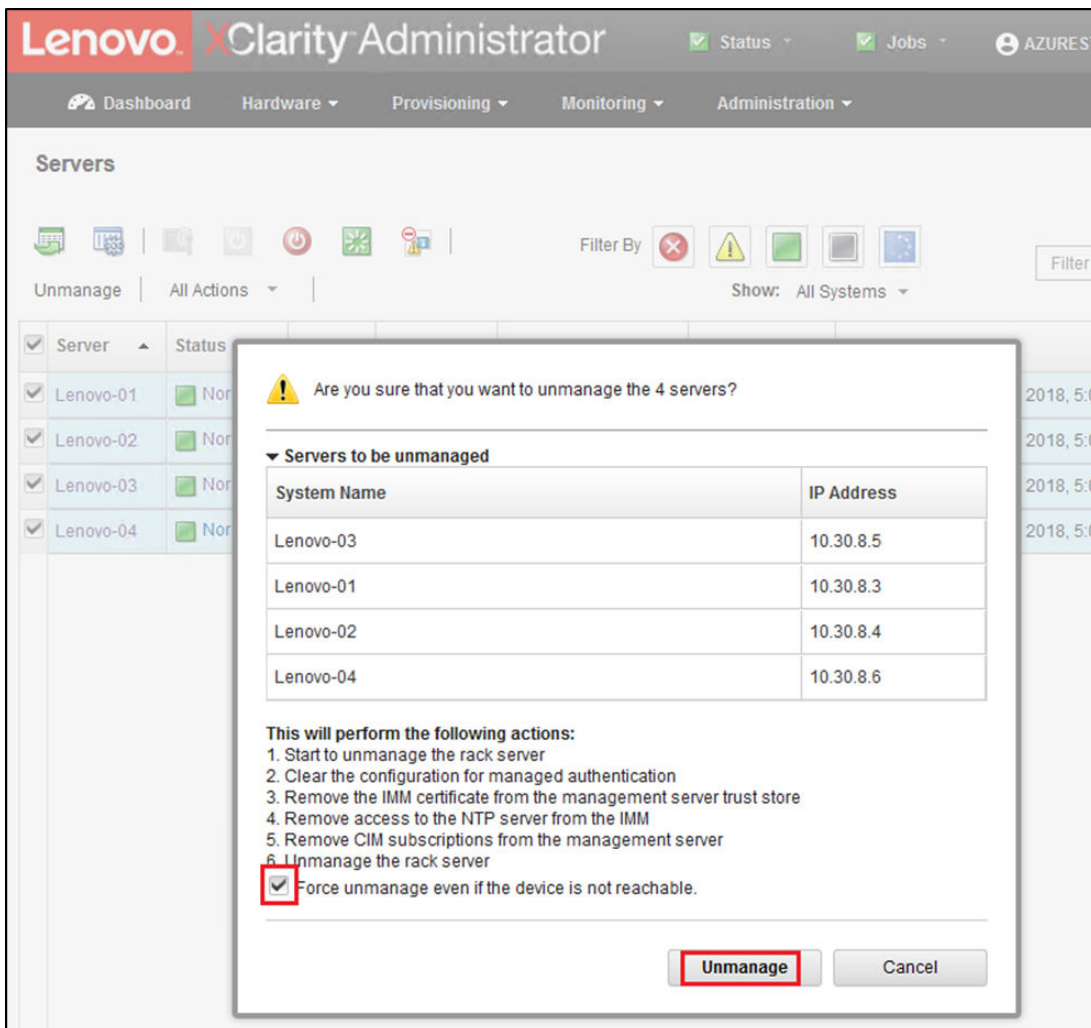


Figure 53. Selecting option to force unmanage nodes

- Step 10. Using the LXCA menu bar near the top of the screen, navigate to **Hardware → Switches**.
- Step 11. If any switches display, select all switches and click **Unmanage**.
- Step 12. In the window that opens, select **Force unmanage even if the device is not reachable**, and click **Unmanage**.
- Step 13. Once all managed servers and switches have been unmanaged, shut down the LXCA Server by using the menu bar to select **Administration → Shut Down Management Server**.
- Step 14. In the window that opens, ensure that there are no active jobs, and click **Shutdown**.
- Step 15. In the confirmation window, click **OK**.
- Step 16. On the HLH, open Hyper-V Manager and wait for the LXCA virtual machine to show a state of Off.

Once the LXCA virtual machine is powered off, work can begin to deploy and configure a new version of LXCA on the HLH.

Deploy and configure LXCA

To prepare for a new deployment of LXCA, the appropriate files need to be downloaded from the [ThinkAgile SXM Series Updates Repository](#). This includes the "LXCA_SXMBR<xyy>.zip" archive file and the LXCA full

VHD image file, which will have a file name in the format “Invgv_sw_lxca_<version>_winsrvr_x86-64.vhd” and will be found in the current Best Recipe directory on the site.



Lenovo ThinkAgile SXM Series Updates Repository

September 2023 ThinkAgile SXM Series update release (SXMBR2309)

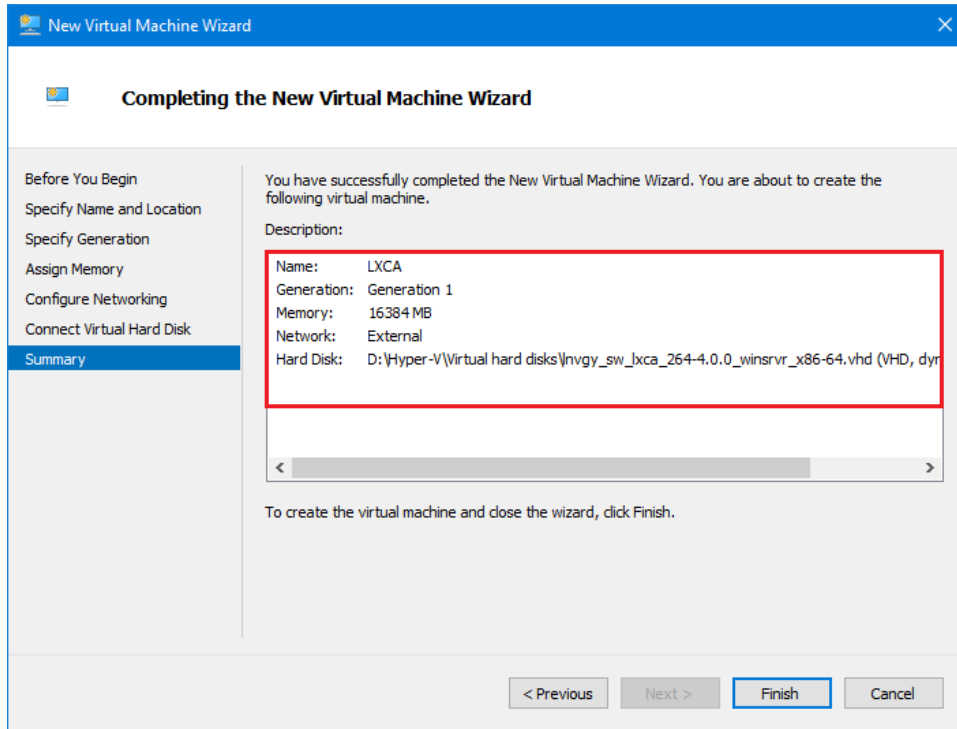
Important: The OEM Extension Packages in this Best Recipe include functionality to perform an attempt to update to this OEM Extension Package until LXCA has been prepared to perform system Administrator for a specific Best Recipe topic in the [ThinkAgile SXM Series Information Center](#) for

File Name	Date Modified
Parent Directory	
HelperScripts.zip	09/29/2023
Invgv_sw_lxca_264-4.0.0_winsrvr_x86-64.vhd	09/29/2023
LXCA_SXMBR2309.zip	
SHA256 Hash: fc833a189538e3b930270d3fa70a794bc77ac4b7d0ee7eb6c581df892a2bdae7 MD5 Hash: 114f1376d28d3242f2141d89d2dc9bda	09/29/2023
OEMv2.2_SXMBR2309-EGS.zip	
SHA256 Hash:	

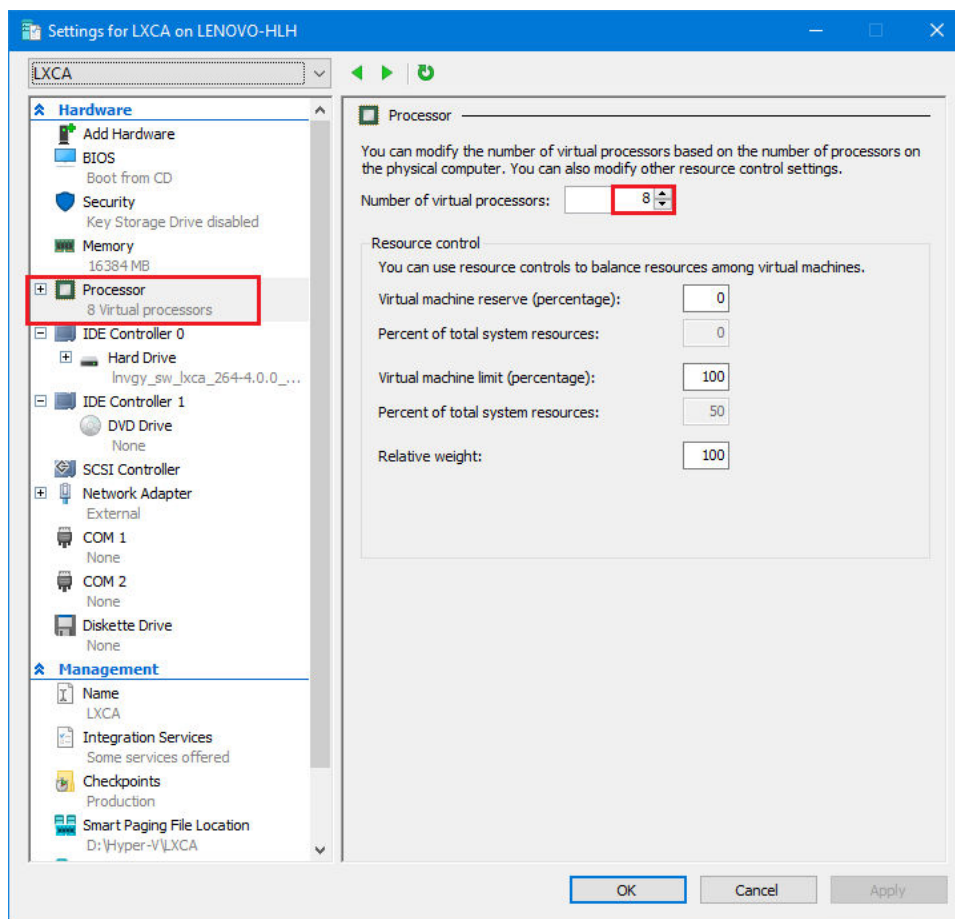
Once all files have been downloaded from the ThinkAgile SXM Series Updates Repository and copied to a USB thumb drive, follow these steps:

- Step 1. Expand the “LXCA_SXMBR<xyy>.zip” archive onto the thumb drive.
- Step 2. Copy the VHD file and expanded archive content (not the directory itself) to D:\LXCA on the hardware lifecycle host (HLH). Replace any files or directories with the same names that are already in the directory.
- Step 3. Copy the LXCA VHD file from **D:\Lenovo\LXCA** to **D:\Hyper-V\Virtual hard disks** on the HLH, creating the specified directories if necessary. Make sure to copy, not move, the file so the original can serve as a backup in case LXCA must be reinstalled in the future.
- Step 4. Open Hyper-V Manager, select **Lenovo-HLH** in the left navigation pane.
- Step 5. In the Actions pane on the right, click **New → Virtual Machine...**
- Step 6. On the Before You Begin page, click **Next**.
- Step 7. On the Specify Name and Location page, enter a Name for the VM, such as “LXCA”, click to check the Store the virtual machine in a different location checkbox, enter “D:\Hyper-V” as the Location, and then click **Next**.
- Step 8. On the Specify Generation page, leave Generation 1 selected and click **Next**.
- Step 9. On the Assign Memory page, enter “16384” for Startup memory and then click **Next**.

- Step 10. On the Configure Networking page, use the Connection dropdown list to select “External” and then click **Next**.
- Step 11. On the Connect Virtual Hard Disk page, click the option to Use an existing virtual hard disk, click **Browse...** and navigate to the LXCA VHD file located at **D:\Hyper-V\Virtual hard disks** on the HLH. Once the VHD file has been selected, click Next.
- Step 12. On the Summary page, verify that all parameters are shown correctly before clicking **Finish** to create the virtual machine.




- Step 13. Once the VM is created, it will appear in the Virtual Machines pane of Hyper-V Manager. Select the VM and then click **Settings...** in the right pane.
- Step 14. In the page that opens, select Processor in the left pane, increase the Number of virtual processors to “8”, and then click OK.



Configure LXCA static IP address

Perform this procedure to configure the LXCA static IP address for your ThinkAgile SXM Series solution.

- Step 1. In Hyper-V Manager, select the LXCA virtual machine in the center pane, and click **Connect...** in the right pane.
- Step 2. In the Virtual Machine Connection window, click the **Start** button () to start the LXCA virtual machine.
- Step 3. Watch the boot process until the following displays, then type "1" and press Enter.

```
-----
Lenovo LXCA - Version 4.0.0 build 264
-----

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 metric 1
      inet6 fe80::215:5dff:fe2a:b416 prefixlen 64 scopeid 0x20<link>
      ether 00:15:5d:2a:b4:16 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
```

Figure 54. Virtual Machine Connection window

Step 4. Enter the requested parameters, as shown in the yellow boxes in the following illustration. Refer to the table that you completed in [“Retire the current LXCA installation”](#) on page 55.


```

=====
=====
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

... .. [ 50.079250] hv_balloon: Received INFO_TYPE_MAX_PAGE_CNT
[ 50.083244] hv_balloon: Data Size is 8
1

ATTENTION: ***
Perform this action only when the Lenovo XClarity Administrator virtual
appliance is initially deployed. If you change the virtual appliance IP
address after managing devices, Lenovo XClarity Administrator will not be
able to connect to those managed devices and the devices will appear to
be offline.

For more information, see 'Configuring network settings' in the Lenovo
XClarity Administrator online documentation.

Gather all required IP information before proceeding. You have 60 secs
to enter the infomation for each prompt.
- For ipv4 protocol: IP address, subnetmask and gateway IP address
- For ipv6 protocol: IP address and prefix length.

Do you want to continue? (enter y or Y for Yes, n for No) Y

Enter the appropriate static IP settings for the XClarity virtual
appliance eth0 port when prompted and then press Enter, OR just press
Enter to proceed to next prompt without providing any input to the
current prompt.

IP protocol(specify ipv4 or ipv6): ipv4
IP address: 10.30.8.115
netmask: 255.255.255.128
gateway: 10.30.8.1
DNS1 IP (optional): 10.50.50.50
DNS2 IP (optional): 10.50.10.50

Processing ... ..
IP protocol: ipv4
IP addr: 10.30.8.115
netmask: 255.255.255.128
gateway: 10.30.8.1
DNS1: 10.50.50.50
DNS2: 10.50.10.50
Do you want to continue? (enter y or Y for Yes, n for No) Y
Status: Running

```

Figure 55. Virtual machine parameters

Step 5. Verify that all parameters have been entered correctly, and then type “Y” and press Enter.

Step 6. Open Internet Explorer and access the LXCA Initial Setup page: <https://<IPv4Address>/ui/login.html>

where <IPv4Address> is the LXCA IP address that was just configured.

The Initial Setup page displays. When you access LXCA for the first time, you must complete several initial setup steps.

To execute the initial setup of LXCA, work through each of the seven tasks shown on the Initial Setup page and complete them as instructed in the following topics.

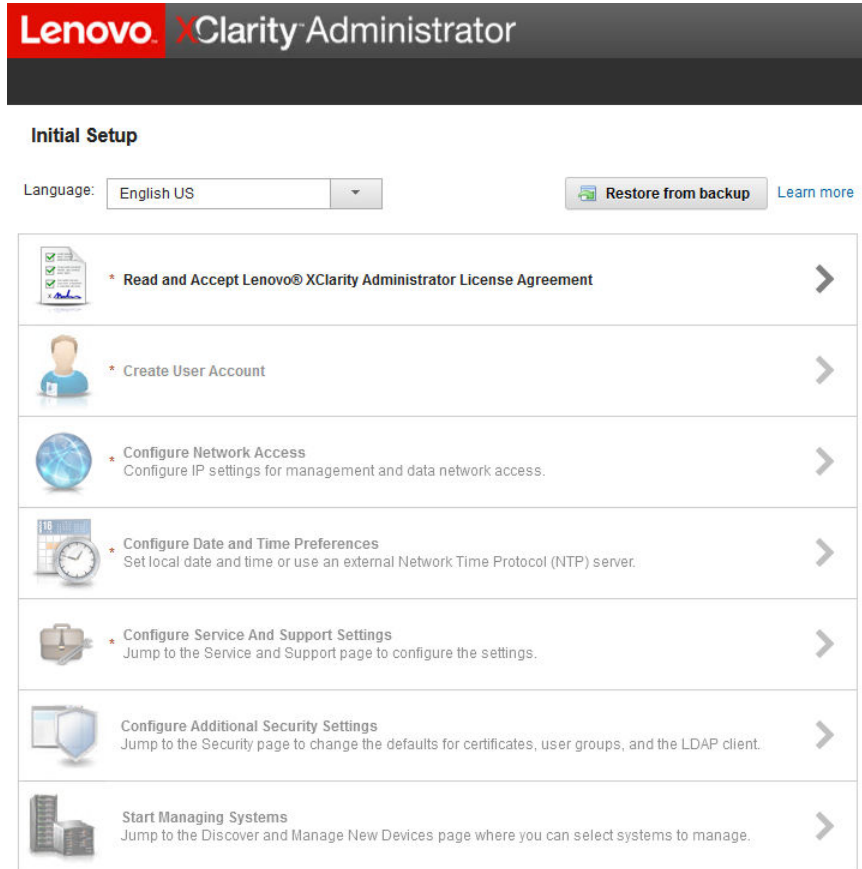


Figure 56. LXCA Initial Setup page

Read and Accept Lenovo XClarity Administrator License Agreement task

Procedure for performing the license agreement task as part of LXCA initial setup.

- Step 1. In the Initial Setup window, click **Read and Accept Lenovo® XClarity Administrator License Agreement**. The license agreement displays.



Figure 57. Read and Accept Lenovo XClarity Administrator License Agreement task window

Step 2. Click **Accept**. The initial startup page now shows a green checkmark on this task.

Proceed to the [“Create User Account task”](#) on page 67.

Create User Account task

Procedure for performing the user account creation task as part of LXCA initial setup.

Step 1. In the Initial Setup window, click **Create User Account**.

The Create New Supervisor User window displays.

Create New Supervisor User

* Username: AzureStackAdmin

Description: Supervisor account used to m:

* New password: ●●●●●●

* Confirm new password: ●●●●●●

Password and password confirm values must match

Create Cancel

Figure 58. Create New Supervisor User window

- Step 2. Create a supervisor account to access LXCA and manage the Azure Stack Hub physical nodes. Include the following parameters:
- **Username:** AzureStackAdmin (or your preferred user name)
 - **Description:** <Description of your choice> (optional)
 - **Password:** <Password>
- Step 3. Click **Create**. The Local User Management page displays with the new user shown. The current active session is now running under this account (upper right corner of screenshot below).

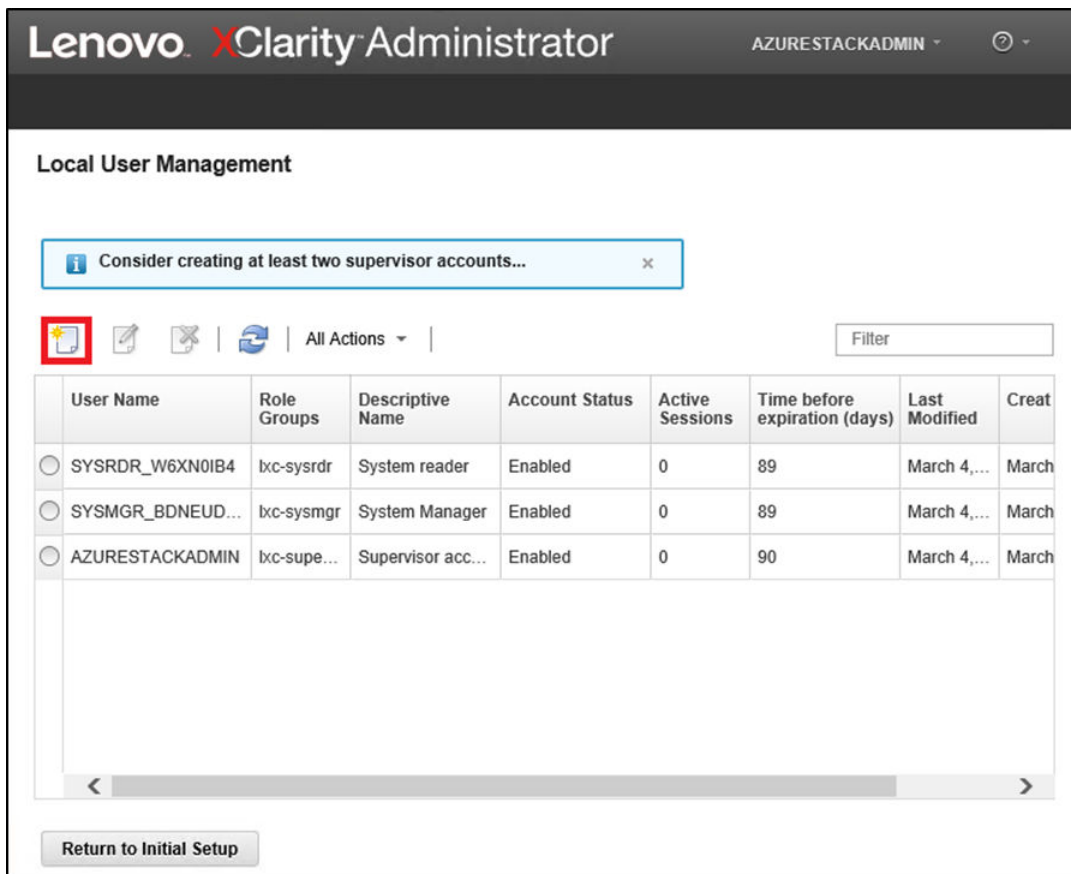



Figure 59. Local User Management window

- Step 4. It is good practice to create at least two supervisor accounts. In the event that the password of the account just created is lost or forgotten, the “failsafe” account can be used to sign in to LXCA and reset the lost password. To create a second account, click the **Create New User** icon () shown in the red box in the screenshot above.
- Step 5. Repeat step 2 to create a second supervisor account. Include the following parameters:
- **Username:** Backup (or your preferred user name)
 - **Description:** <Description of your choice> (optional)
 - **Password:** <Password>
- Step 6. Click **Create**. The Local User Management page displays with the second new user. The two other accounts listed are internal system accounts used by LXCA. Do not be modify or remove these accounts.

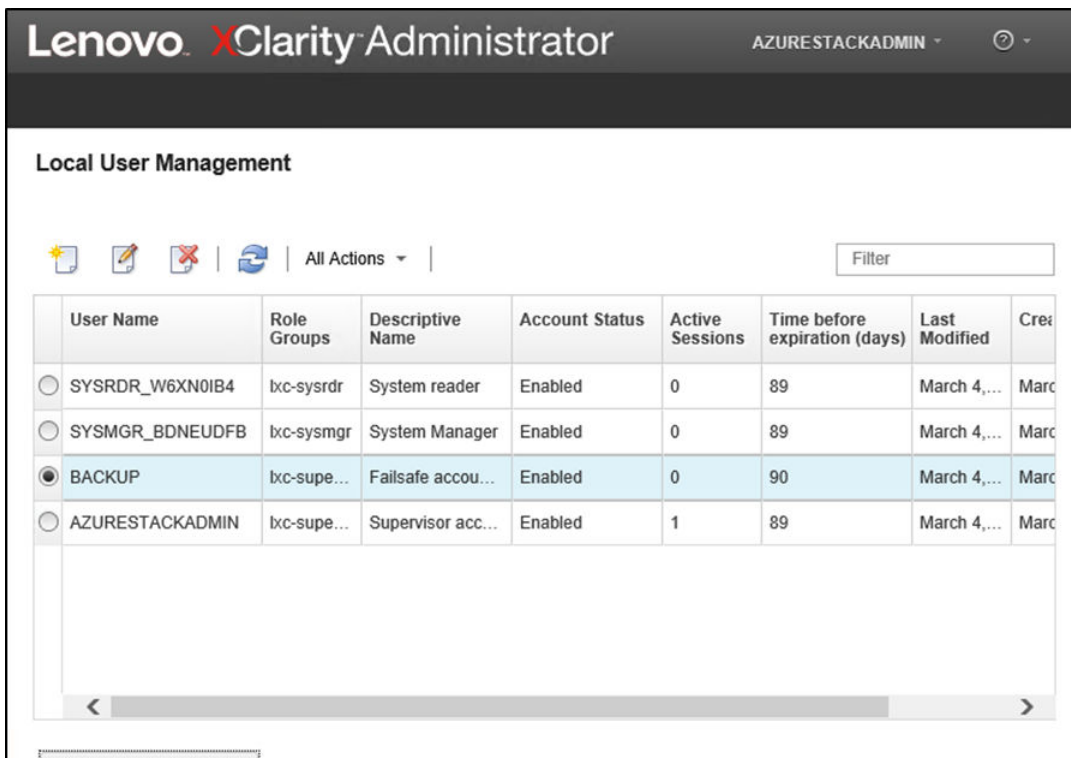


Figure 60. Local User Management window with backup user

Step 7. Record all LXCA credentials in the following table to add to your records later.

	User Name	Password
Primary account		
Secondary account		

Step 8. Back in LXCA, click **Return to Initial Setup** to finish the Create User Account task and return to the Initial Setup page.

Proceed to the [“Configure Network Access task” on page 70](#).

Configure Network Access task

Procedure for configuring network access as part of LXCA initial setup.

Step 1. In the Initial Setup window, click **Configure Network Access**.

The Edit Network Access window displays.

Edit Network Access

IP Settings Advanced Routing DNS & Proxy

IP Settings

If you use DHCP and an external security certificate, make sure that the address leases for the management server on the DHCP server are permanent to avoid communication issues with managed resources when the management server IP address changes.

One network interface detected:

Eth0: Enabled - used to discover and manage hardware only. ?
 You will not be able to manage or deploy operating system images and update operating system drivers.

	IPv4	IPv6
	Use statically assigned IP address	Use stateful address configuration (DHCPv6)
Eth0:	* IP address: 10.30.8.52 Network Mask: 255.255.255.192	IP address: 0::0 Prefix Length: 64
Default gateway:	Gateway: 10.30.8.1	Gateway: DHCP

Save IP Settings Restart Return to Initial Setup

Figure 61. Edit Network Access window

- Step 2. On the Edit Network Access page with the IP Settings tab visible, verify that the correct IPv4 parameters display in the **IP address**, **Network Mask**, and **Gateway** fields.
- Step 3. Go to the DNS & Proxy tab and verify that the DNS Server(s) were entered correctly.
- Step 4. On the same page, enter “LXCA” in the **Host name** field, as shown in the following illustration.

Edit Network Access

IP Settings Advanced Routing **DNS & Proxy**

Names for this Virtual Appliance

Host name:
Domain name:

DNS Servers

DNS Operating Mode: ?

Order	DNS Server
<input type="text" value="1"/>	<input type="text" value="10.241.80.5"/>

Proxy Setting

Internet Access :

Figure 62. DNS & Proxy settings tab

- Step 5. Click **Save DNS & Proxy**, then click **Save** in the confirmation window , and then click **Close** in the Internet/DNS Settings window.
- Step 6. Return to the IP Settings tab of the Edit Network Access page.
- Step 7. Under the IPv6 column heading, select **Disable IPv6** in the dropdown list. Click **Close** to dismiss the pop-up window, and then click **Save IP Settings**.

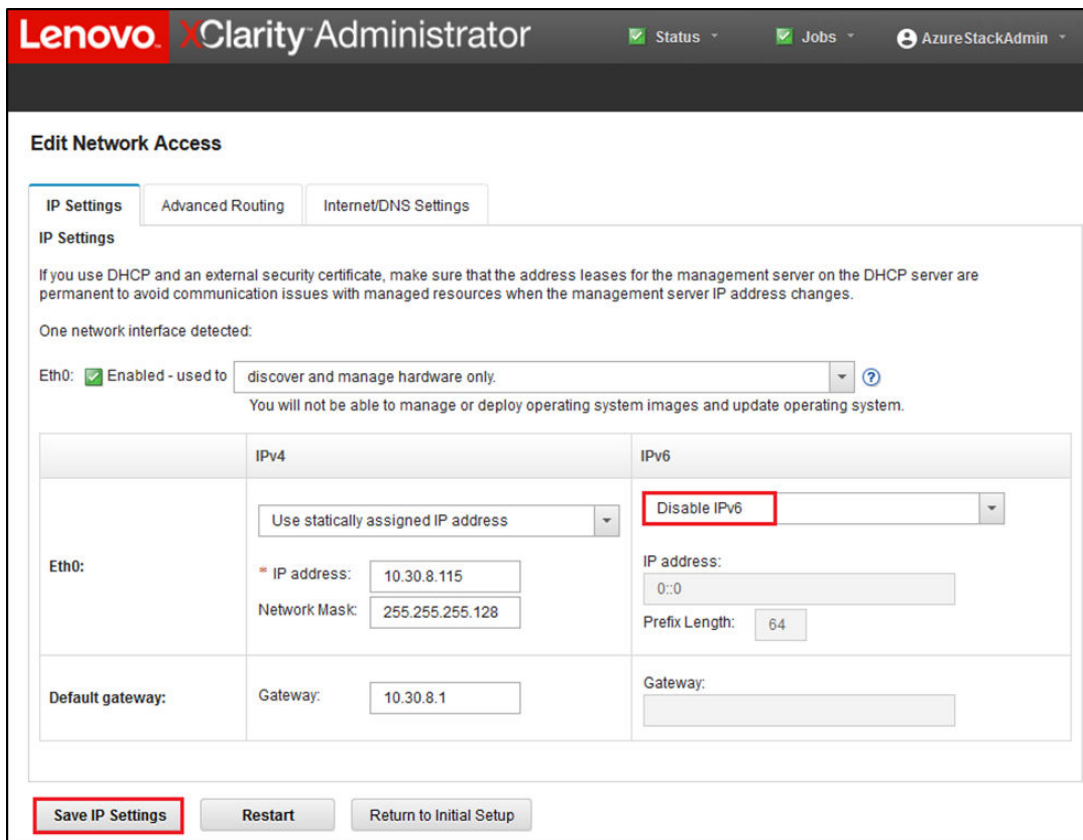


Figure 63. Disabling IPv6 settings

- Step 8. Click **Save** in the confirmation pop-up window.
- Step 9. A window appears prompting you to restart the management server to apply these changes. Click **Restart** and then click **Close** in the confirmation window that displays.

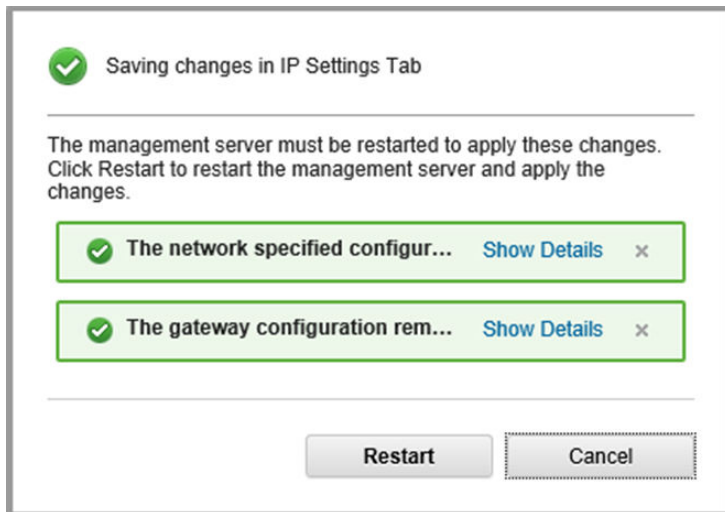


Figure 64. Saving IP Settings tab changes

- Step 10. Wait for the management server to restart, approximately five minutes. During this time, a pop-up window displays that reads “The connection to the management server was lost. A connection to

the server could not be established.” This message is normal when restarting the management server and can be ignored. When this pop-up displays, click **Close**. For LXCA v4.0 and later, a login screen should be presented once the LXCA management server has restarted.

Step 11. If necessary, refresh the browser to return to the LXCA login page, then log in using the primary supervisor account created earlier. The Initial Setup page displays, this time with the first three tasks checked.

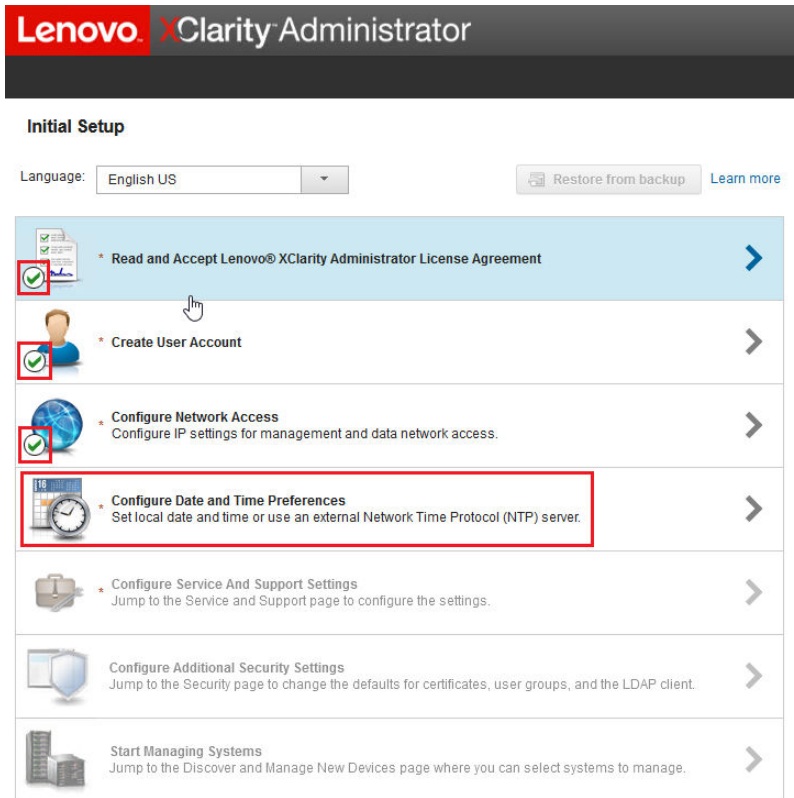


Figure 65. Initial Setup page with completed tasks checked

Proceed to the “[Configure Date and Time Preferences task](#)” on page 74.

Configure Date and Time Preferences task

Procedure for configuring date and time preferences as part of LXCA initial setup.

Step 1. In the Initial Setup window, click **Configure Date and Time Preferences**.

The Edit Date and Time window displays.

Edit Date and Time

Date and time will be automatically synchronized with the NTP server.

Time zone: ▾
Daylight saving time is not observed in this time zone.

Edit clock settings (12 or 24 hours format):

NTP server host name or IP address:

NTP v3 Authentication:

Figure 66. Edit Date and Time window

Step 2. On the Edit Date and Time page, specify the **Time zone** as “UTC -0:00, Coordinated Universal Time Etc/UCT” and **NTP server host name or IP address** that is suitable for your location.

Note: LXCA does not support Windows time servers. If you normally use a Windows time server, substitute an address appropriate for your location.

Step 3. Once you have entered the parameters, click **Save** to return to the Initial Setup page.

Proceed to the [“Configure Service and Support Settings task” on page 75.](#)

Configure Service and Support Settings task

Procedure for configuring service and support settings as part of LXCA initial setup.

Step 1. In the Initial Setup window, click the **Configure Service and Support Settings** task. The Lenovo Privacy Statement is displayed. Click Accept to dismiss this window and move to the Service and Support page.

Step 2. On the Periodic Data Upload tab, select the options you prefer, and click **Apply**.

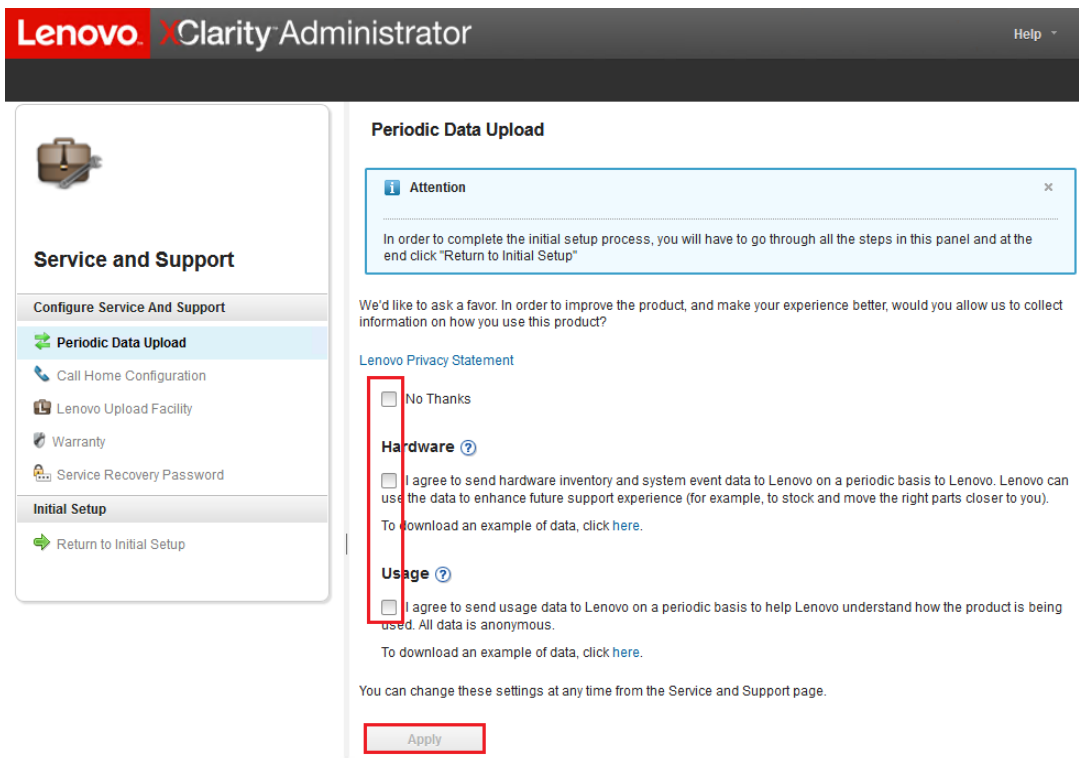


Figure 67. Service and Support Periodic Data Upload tab

- Step 3. On the Call Home Configuration tab, scroll to the bottom of the page if necessary and select **Skip Step** (the Call Home feature is not used for ThinkAgile SXM Series solutions).

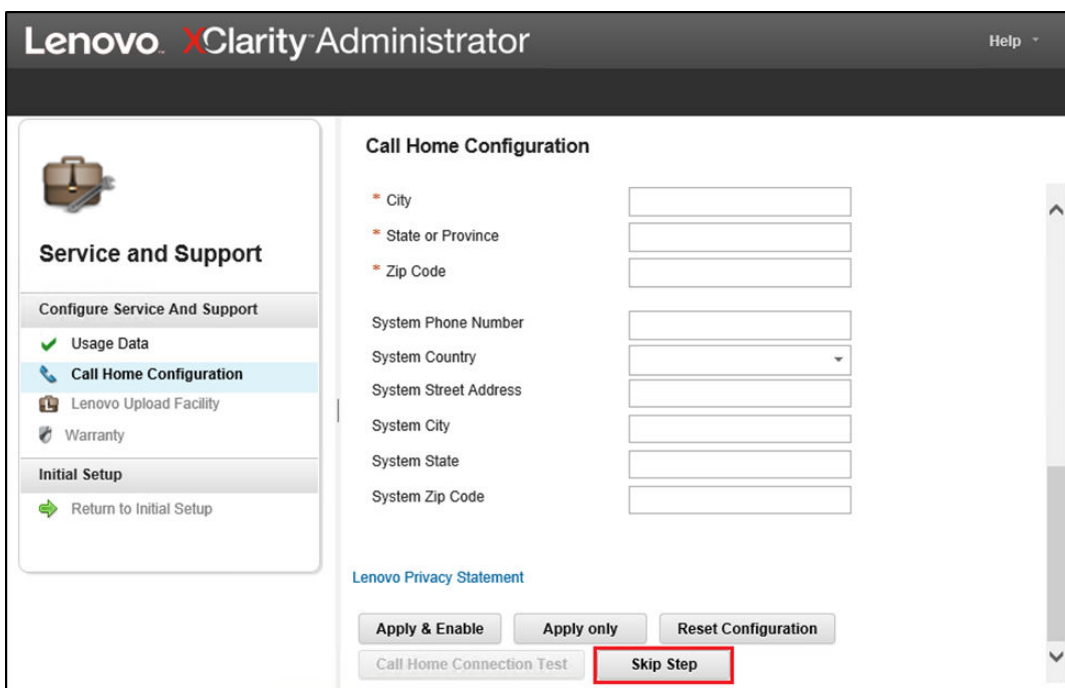


Figure 68. Service and Support Call Home Configuration tab

Step 4. On the Lenovo Upload Facility tab, scroll to the bottom of the page and click **Skip Step**.

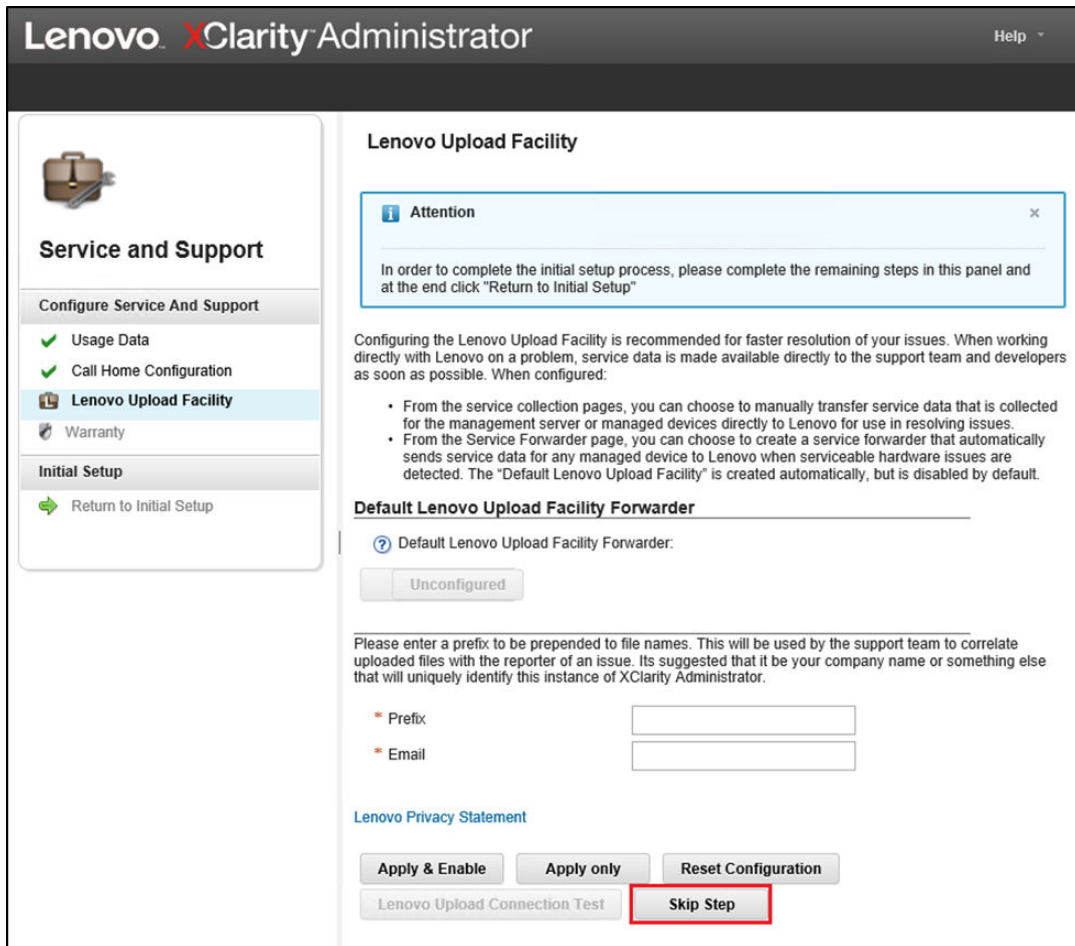


Figure 69. Service and Support Lenovo Upload Facility tab

Step 5. On the Warranty tab, ensure that all drop-down lists are set to **Disabled**, and then click **Apply**. Since ThinkAgile SXM Series solution warranty entitlement is based on the rack serial number, this LXCA feature is not supported.

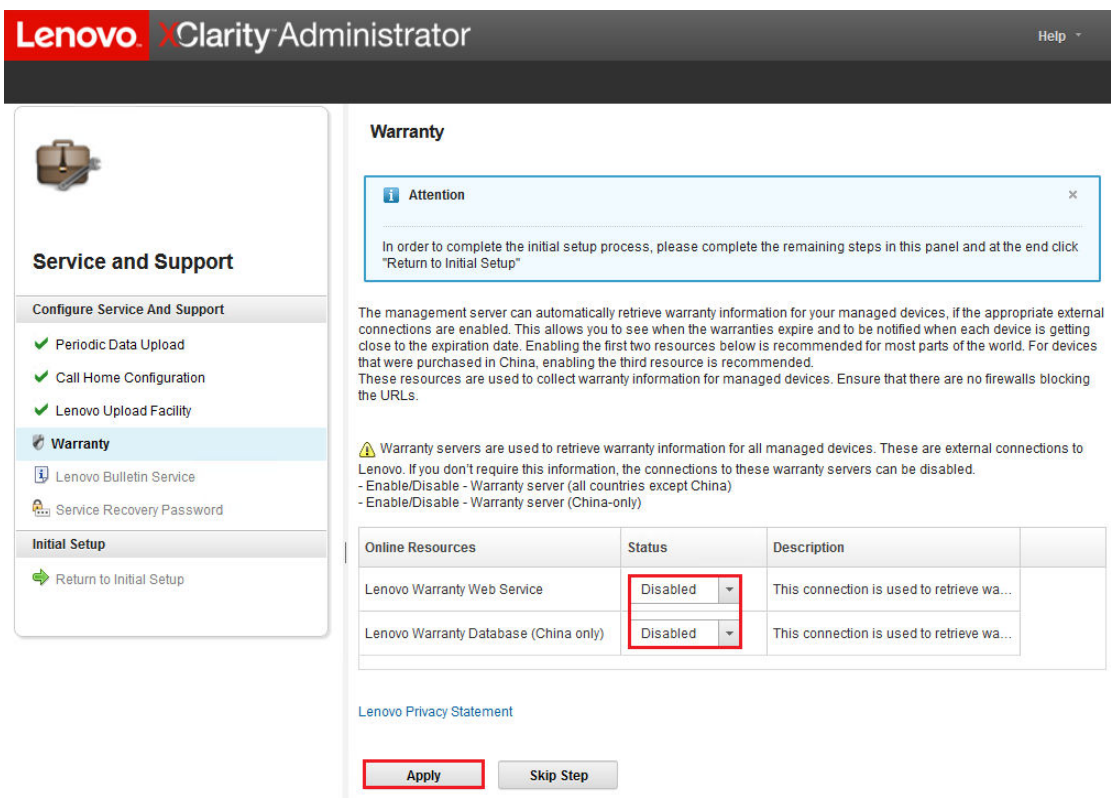


Figure 70. Service and Support Warranty tab

- Step 6. Click **Close** in the Success window that displays, choose whether to receive bulletins from Lenovo, and then click **Apply**.
- Step 7. On the Service Recovery Password tab, enter and confirm a password for LXCA recovery, and click **Apply**. Record this password for future reference.

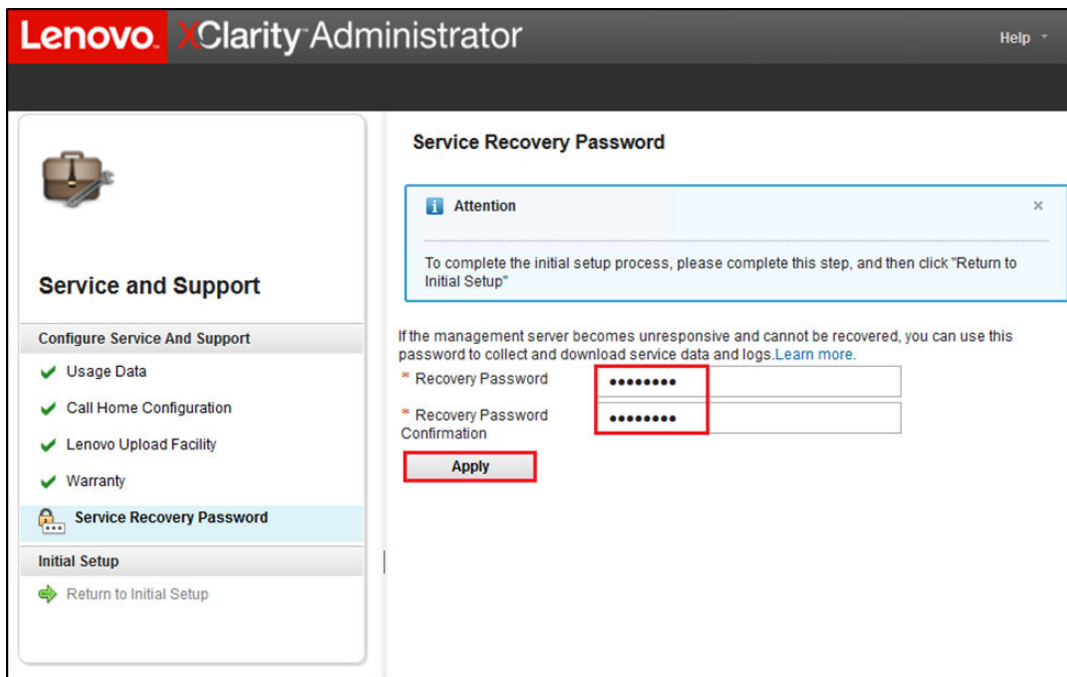


Figure 71. Service Recovery Password page

Step 8. Click **Close** in the Success window that displays, and then click **Return to initial setup**.

Proceed to the “[Configure Additional Security Settings task](#)” on page 79.

Configure Additional Security Settings task

Procedure for configuring additional security settings as part of LXCA initial setup.

- Step 1. In the Initial Setup window, click **Configure Additional Security Settings**. The Security page displays.
- Step 2. Since nothing needs to be modified here, click **Return to Initial Setup**.
- Step 3. At this point, LXCA is ready to start managing systems. Verify that all steps on the Initial Setup page display a green checkmark except for the last one, as shown in the screenshot below.

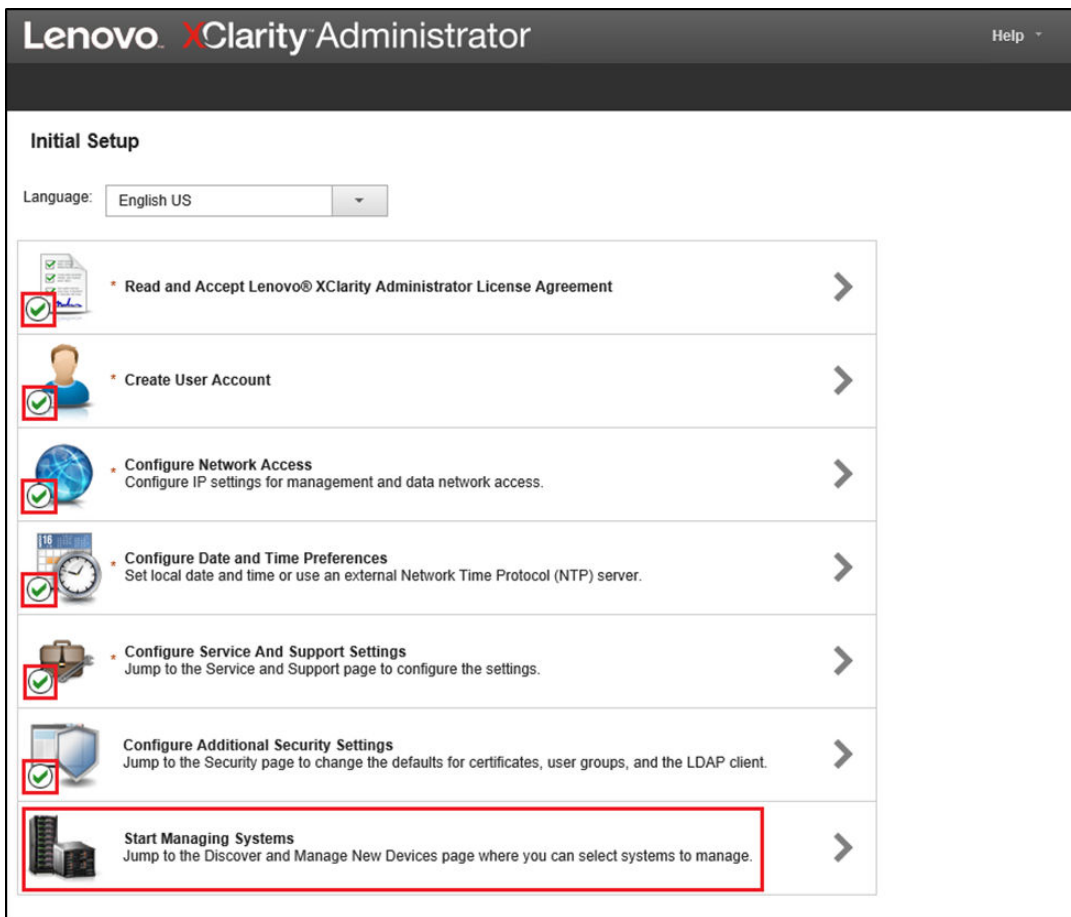


Figure 72. Initial Setup window with one task remaining

Proceed to [“Start Managing Systems task” on page 80.](#)

Start Managing Systems task

Procedure for managing systems in LXCA.

- Step 1. In the Initial Setup window, click **Start Management Systems**. The Start Management Systems page displays.
- Step 2. Click **No, don't include Demo Data**.

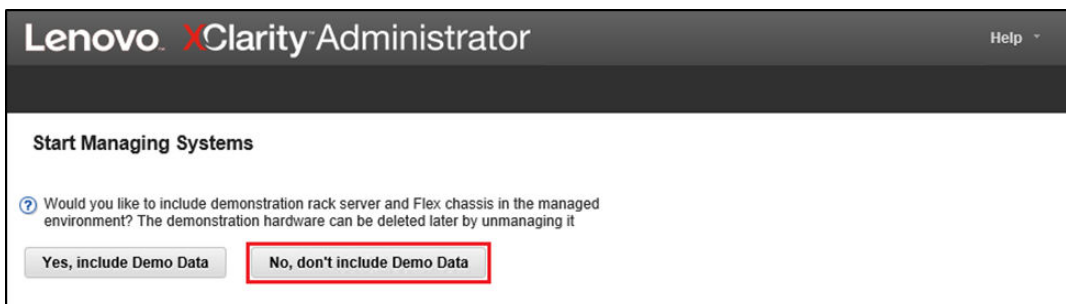


Figure 73. Selecting No, don't include Demo Data in Start Managing Systems window


- Step 3. Click **No thanks** in the pop-up window.
- Step 4. The Discover and Manage New Devices page displays. Automatic discovery takes place for the subnet on which LXCA resides. Since the BMCs in the systems that will become nodes in the Azure Stack Hub scale unit have IP addresses on the same subnet, they should display in the table. If your solution uses Lenovo TOR switches, they may also be listed.

We will not manage any systems or switches at this point. We will return to manage systems after the LXCA Pro license key has been enabled and LXCA has been updated to the version specified by the current [ThinkAgile SXM Best Recipe](#).

Proceed to [“Apply LXCA Pro license” on page 81](#).

Apply LXCA Pro license

Before using LXCA to manage systems, you must import and apply the LXCA Pro License key. This key is specifically for long-term use of the Pattern functionality. To import and apply the license key, follow these steps:

- Step 1. Using the top menu of LXCA, navigate to **Administration → Licenses**.
- Step 2. On the License Management page, click the **Import** icon ()
- Step 3. Click Accept License on the License Agreement window that opens, and then click **Select Files....**
- Step 4. Navigate to D:\Lenovo\LXCA\LXCA License Files, select the file in the directory, and then click **Open**.
- Step 5. In the Import and apply window, click **Import and apply**, and then click **Yes** in the confirmation window that appears.
- Step 6. Click **Close** in the Success window that appears.
- Step 7. Back on the License Management page, confirm that the LXCA Pro license key has been applied successfully and the Status is “Valid”.

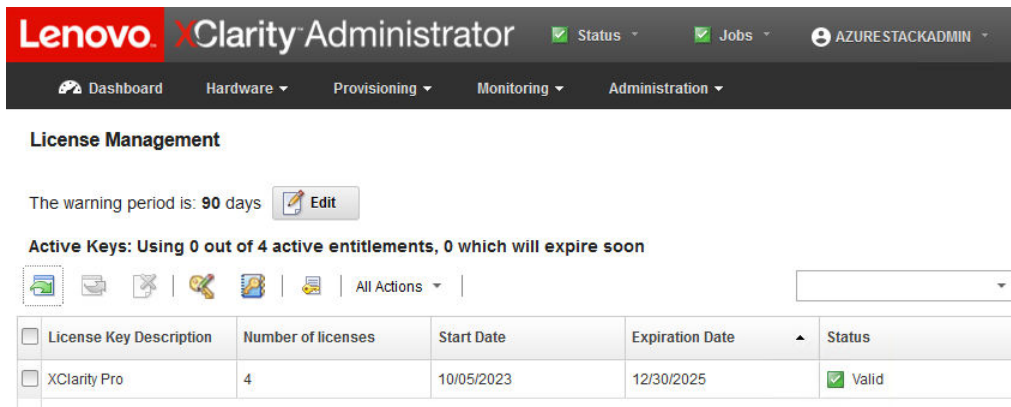


Figure 74. License Management page with valid LXCA Pro license shown

Apply LXCA update package

Two types of LXCA updates are typically available. An LXCA Update Package is applied to a base VHD image to update to the latest major release (for example, from v3.0.0 to v3.1.0 or v3.2.0 or v3.3.0, etc.). An LXCA FixPack is applied to a major release to update LXCA to the latest minor release (for example, from v3.6.0 to v3.6.8). To apply an update to LXCA, follow these steps:

Step 1. Using the top menu of LXCA , navigate to **Administration → Update Management Server**.

Step 2. Click the **Import** icon () and then **Select Files....**

Step 3. Navigate to the appropriate Update Package or FixPack directory inside D:\Lenovo\LXCA\LXCA Update Packages. For example, if updating LXCA base VHD v3.4.5 to v3.6.8, use the content of the “LXCA v3.6.0 Update” directory to update to v3.6.0 and then use the content of the “LXCA v3.6.8 FixPack” directory to update to v3.6.8. In our example below, we update LXCA v4.0.0 to v4.0.14, which does not require an LXCA Update Package, but does require an LXCA FixPack.

Step 4. Select all four files in the directory, and click **Open**.

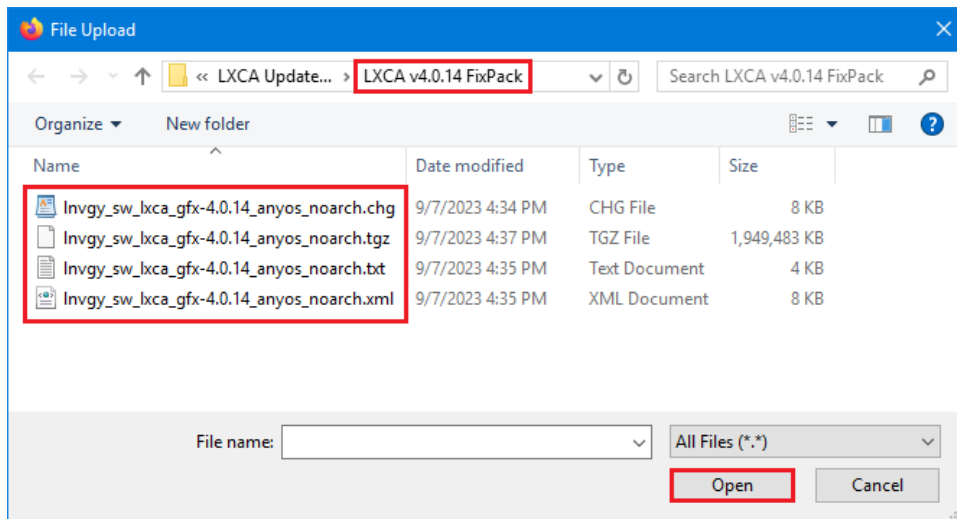



Figure 75. Selecting LXCA FixPack files

Step 5. In the Import window, click **Import**. Progress displays until import and validation of the update content completes. The Import window will close when complete.

Step 6. In the Update Management Server page, select the Update Name for the update that was just imported, and then click the **Perform Update** () button.

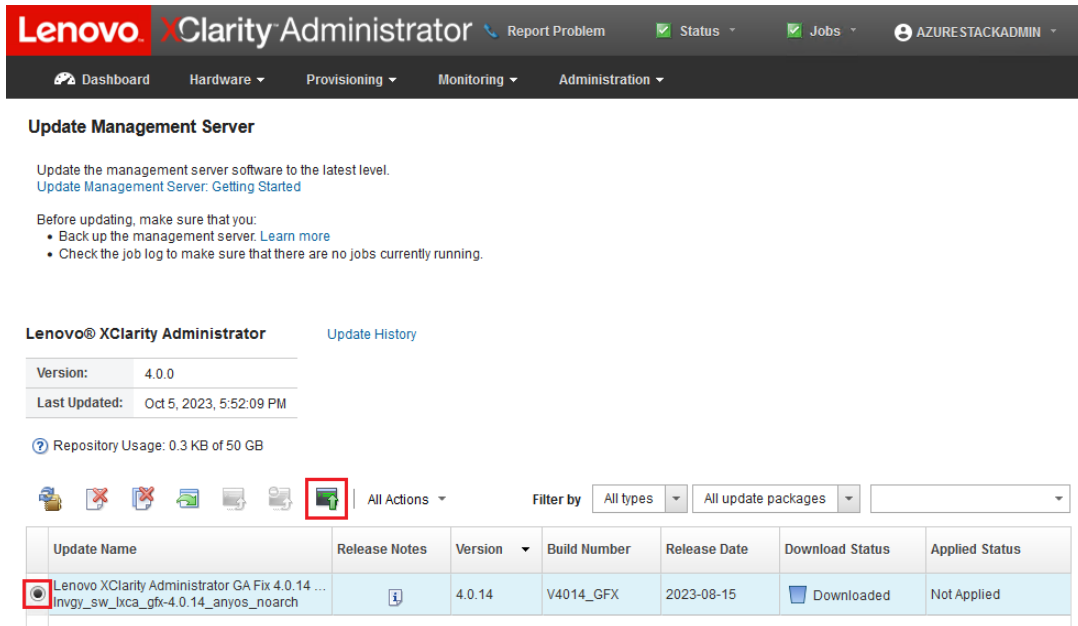


Figure 76. Selecting the update package and performing update

- Step 7. In the confirmation pop-up window, click **Restart**.
- Step 8. Wait for the management server to restart, which can take several minutes. If necessary, refresh the browser to return to the LXCA sign-in page, then sign in using the primary supervisor account created earlier.
- Step 9. Return to the Update Management Server page and wait for the download status to become “Cleaned Up” and applied status to become “Applied” before proceeding. You may need to refresh the page to get the final status to update.

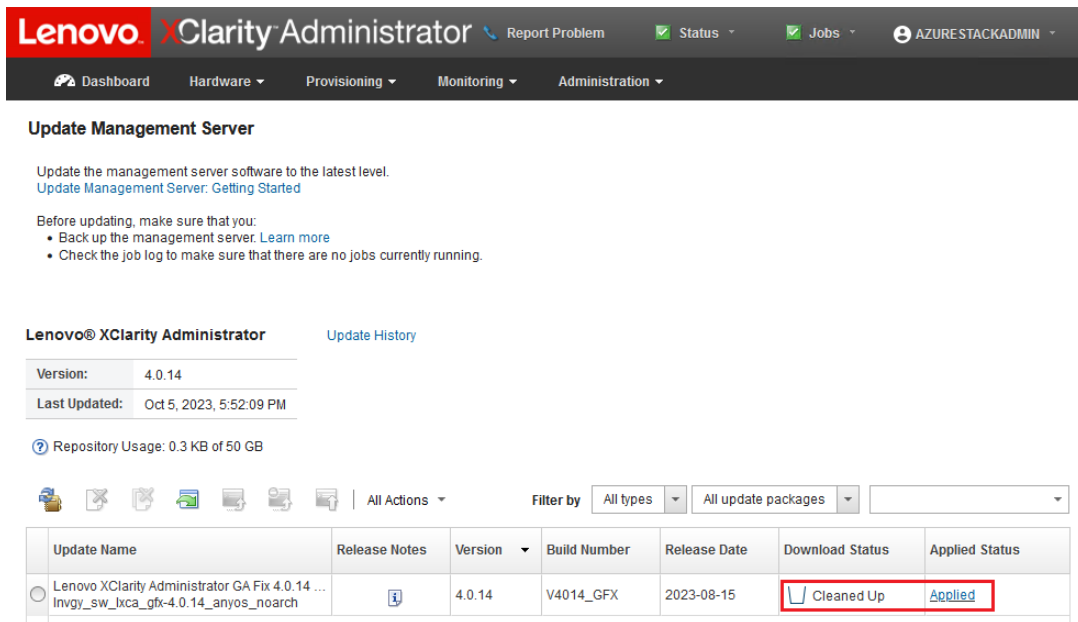
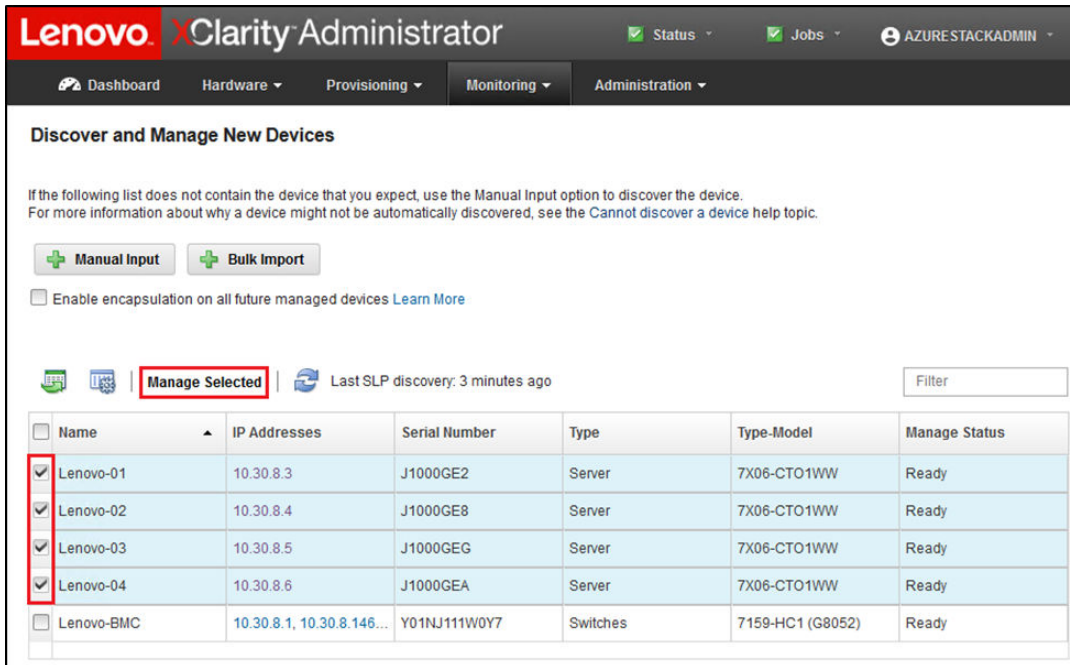


Figure 77. Update package final statuses

Manage the nodes

Now that LXCA configuration is complete, it can manage the nodes and network switches in the Azure Stack Hub scale unit. To manage the nodes in the Azure Stack Hub scale unit, follow these steps:

- Step 1. At the top menu of LXCA, select **Hardware → Discover and Manage New Devices**.
- Step 2. To manage the Lenovo servers, select the checkbox to the left of each of them and click **Manage Selected**. Leave any switches and the HLH unselected if they are listed.



The screenshot shows the 'Discover and Manage New Devices' page in the Lenovo XClarity Administrator. The page includes a navigation bar with 'Dashboard', 'Hardware', 'Provisioning', 'Monitoring', and 'Administration'. Below the navigation bar, there are buttons for 'Manual Input' and 'Bulk Import', and a checkbox for 'Enable encapsulation on all future managed devices'. A table of discovered devices is shown, with the 'Manage Selected' button highlighted in red. The table contains the following data:

<input type="checkbox"/>	Name	IP Addresses	Serial Number	Type	Type-Model	Manage Status
<input checked="" type="checkbox"/>	Lenovo-01	10.30.8.3	J1000GE2	Server	7X06-CTO1WW	Ready
<input checked="" type="checkbox"/>	Lenovo-02	10.30.8.4	J1000GE8	Server	7X06-CTO1WW	Ready
<input checked="" type="checkbox"/>	Lenovo-03	10.30.8.5	J1000GEG	Server	7X06-CTO1WW	Ready
<input checked="" type="checkbox"/>	Lenovo-04	10.30.8.6	J1000GEA	Server	7X06-CTO1WW	Ready
<input type="checkbox"/>	Lenovo-BMC	10.30.8.1, 10.30.8.146...	Y01NJ111W0Y7	Switches	7159-HC1 (G8052)	Ready

Figure 78. Four nodes selected to be managed

- Step 3. In the Manage window, uncheck **Managed Authentication**, and click **Manage stored credentials**.

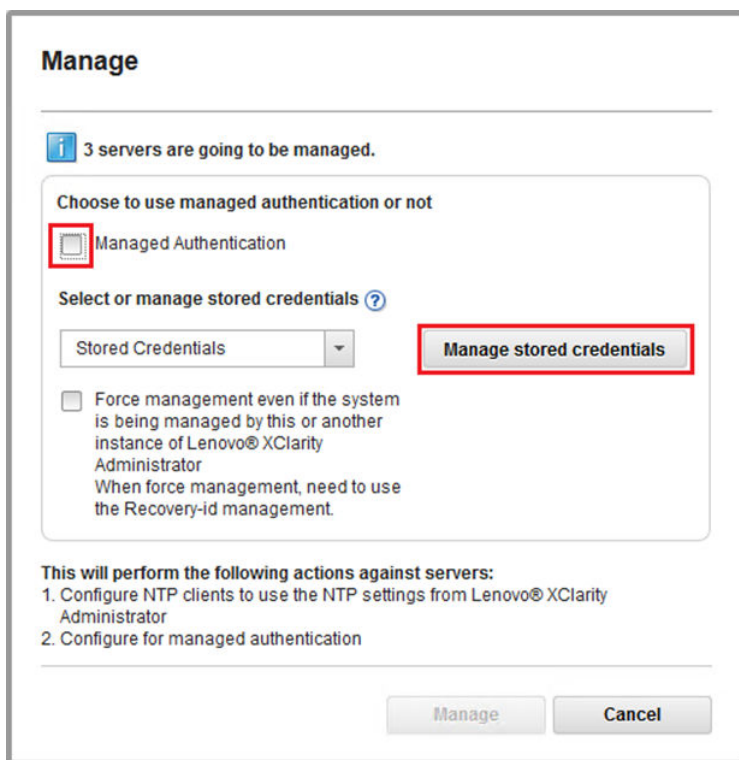



Figure 79. Manage stored credentials

- Step 4. Click **Create new stored credentials** ().
- Step 5. Enter the credentials that LXCA will use to communicate with the XClarity controllers on the nodes. These credentials should be recorded in the Customer Deployment Summary document that was left with the customer after initial solution deployment. Since the credentials are identical between nodes, they only need to be entered once. Enter a description that makes it obvious that LXCA uses this credential set to manage the nodes. After entering the credentials, click **Create Stored Credential**.

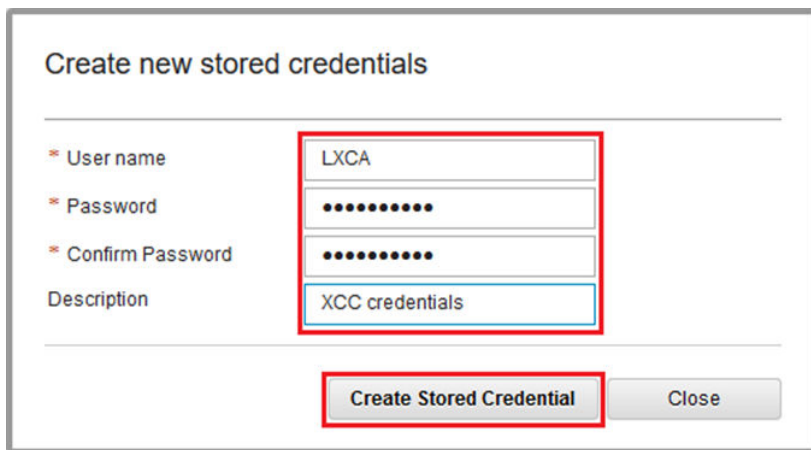


Figure 80. Create a new stored credential

Step 6. Back in the Stored credentials management window, select the credentials that were just created, and click **Select**.

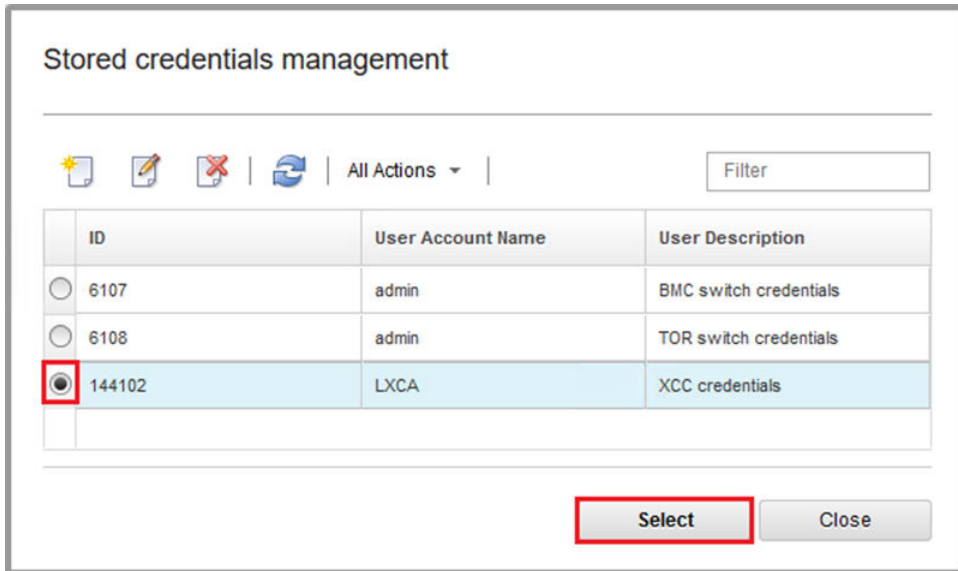


Figure 81. Selecting new stored credential for management

Step 7. In the Manage window, click **Manage**.

Step 8. A status window displays the process of establishing a management connection with each XClarity controller.

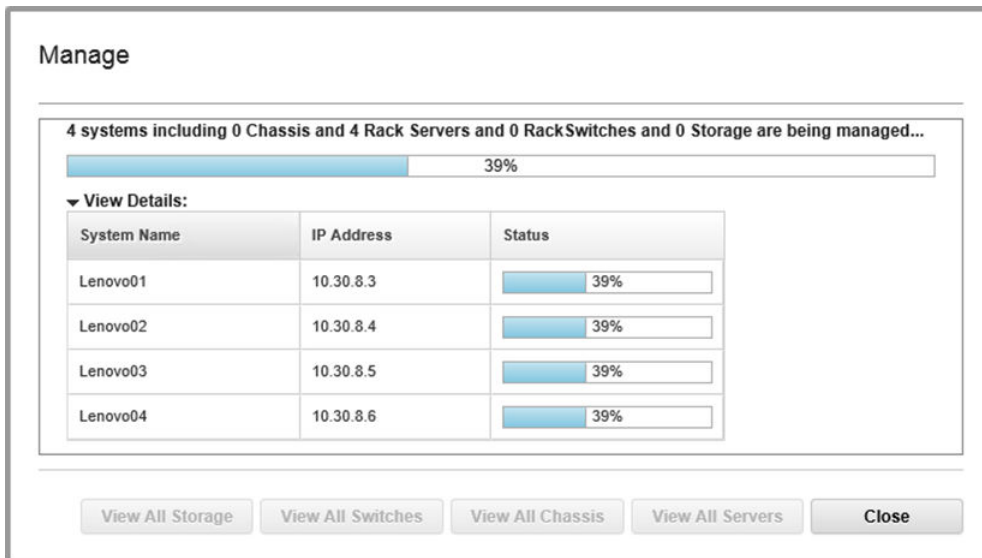


Figure 82. Establishing management connections with each XClarity controller

Step 9. Once the process completes, click **View All Servers** to close the Manage window and return to the LXCA main window.

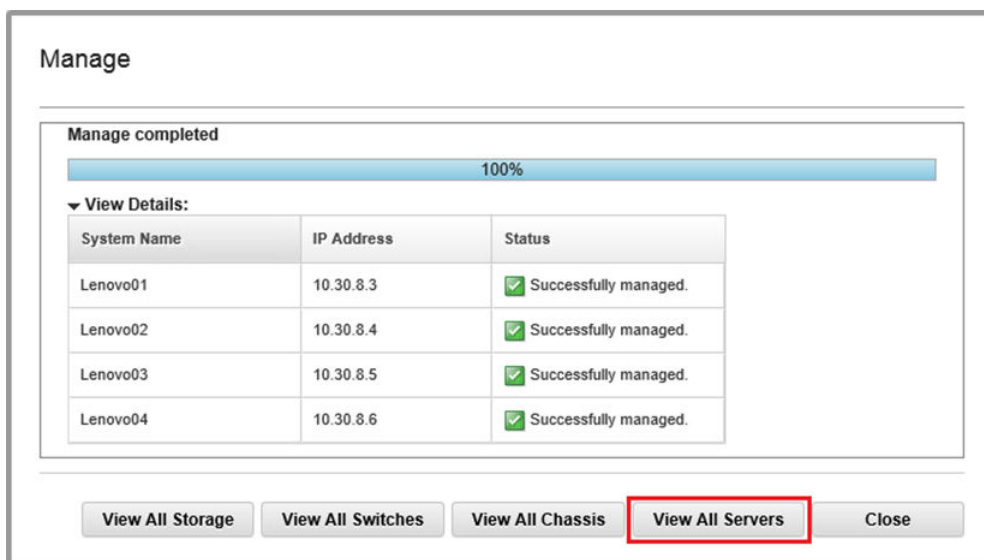


Figure 83. View All Servers

Even though the job completes successfully, inventory collection from the nodes may take 20 minutes or more to complete. During this time, some tasks (such as applying a server pattern or policy) may not be allowed. A Pending status indicates that inventory collection is in progress.

Eventually, the status of all nodes displays as Normal.

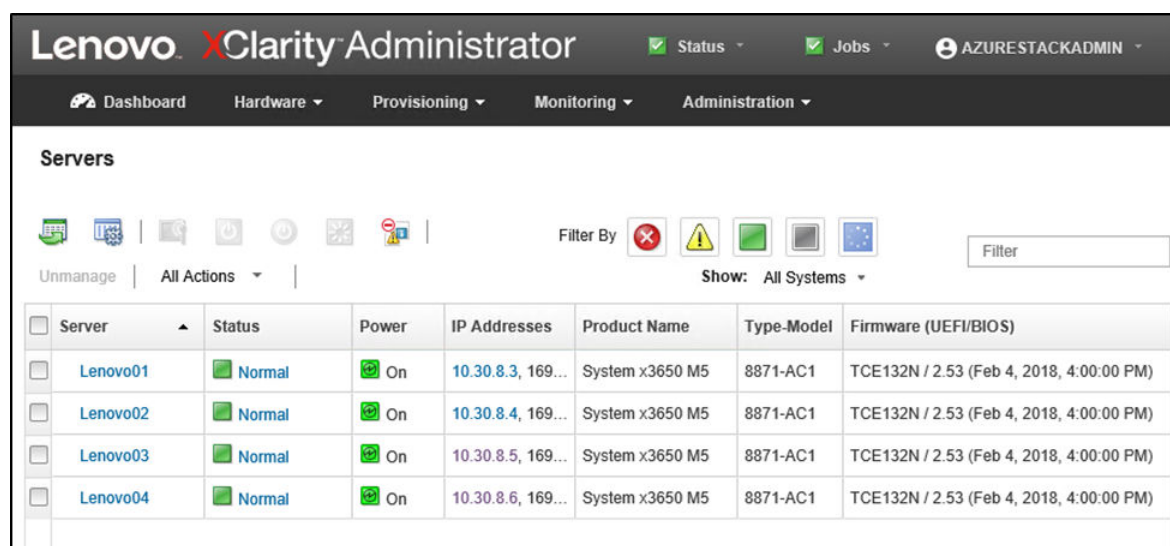




Figure 84. Inventory collection completed

Import and apply server pattern

A server pattern represents a bare-metal server configuration and can be applied to multiple servers at a time.

The appropriate server pattern is available in the `D:\Lenovo\XClarity` directory on the HLH.

To import the Lenovo ThinkAgile SXM Series server pattern, follow these steps:

- Step 1. At the top menu of the LXCA browser interface, select **Provisioning → Patterns**.
- Step 2. On the Configuration Patterns: Patterns page, click the **Import** icon () , and then **Select Files....**
- Step 3. Navigate to D:\Lenovo\LXCA, select the LXCA pattern file appropriate for your solution, and then click **Open**.
- Step 4. Click **Import**. When the import success window displays, click **Close**.
- Step 5. To deploy the pattern, select the checkbox to the left of the pattern that was just imported and click the **Deploy Pattern** icon () .

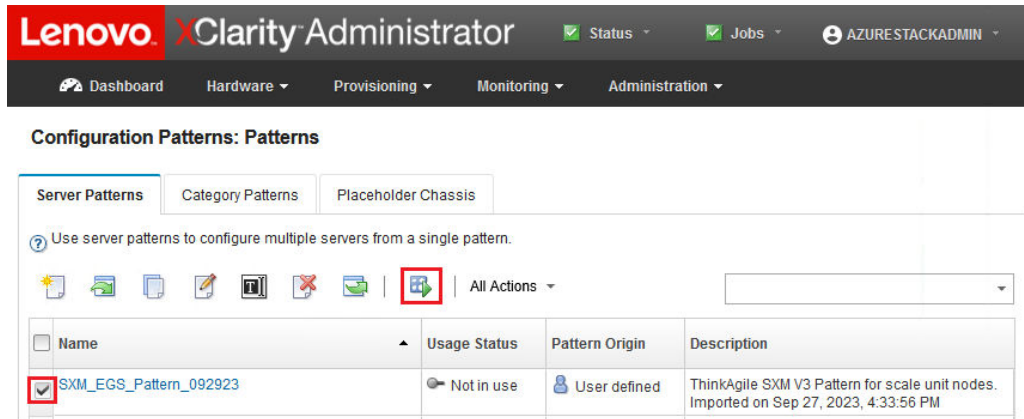


Figure 85. Deploying a pattern

- Step 6. Ensure that the **Partial – Activate BMC settings but do not restart the server...** radio button is selected, then select all Azure Stack Hub scale unit nodes and click **Deploy**.

Important: Make sure that the **Partial...** option is selected, since we do NOT want all the nodes to restart at the same time.

Deploy Server Pattern - SR650PatternThinkAgileSXM_121218

Deploy the server pattern to one or more individual servers or groups of servers (for example, a chassis). During deployment, one server profile is created for each individual server.

* Pattern To Deploy:

* Activation ? Full — Activate all settings and restart the server now.
 Partial — Activate BMC settings but do not restart the server. UEFI and server settings will be active after the next restart.
 Deferred — Generate a profile with the settings for review, but do not activate settings on the server.

Choose one or more servers to which to deploy the selected pattern.

Any Deploy Status

<input checked="" type="checkbox"/>	Name	Rack Name/Unit	Chassis/Bay	Deploy Status
<input checked="" type="checkbox"/>	Lenovo-01	Unassigned / Un		✓ Ready
<input checked="" type="checkbox"/>	Lenovo-02	Unassigned / Un		✓ Ready
<input checked="" type="checkbox"/>	Lenovo-03	Unassigned / Un		✓ Ready
<input checked="" type="checkbox"/>	Lenovo-04	Unassigned / Un		✓ Ready

Figure 86. Deploy pattern with full activation

Step 7. In the pop-up window that is displayed, select **Jump to Profiles page**.

✓ Deployment request was submitted.

Job "Server Profile activation: Feb 27, 2018" has been created and started successfully. Changes are being propagated to the following servers or bays: Lenovo01, Lenovo02, Lenovo03, Lenovo04

You can monitor job progress from the Jobs pod in the banner above.

You can view the profile creation progress from the Server Profiles link that is located under the Provisioning menu in the menu bar. Profiles will not show up in the Server Profiles table until the profile has been created.

Figure 87. Jump to Profiles control

Step 8. Wait for all profiles to become active, as shown in the Profile Status column.

The screenshot shows the 'Configuration Patterns: Server Profiles' section of the Lenovo Clarity Administrator. It includes a navigation bar with 'Dashboard', 'Hardware', 'Provisioning', 'Monitoring', and 'Administration'. Below the navigation, there is a header for 'Configuration Patterns: Server Profiles' and a sub-header explaining that server profiles represent the specific configuration of a single server. A toolbar contains icons for help, refresh, print, and delete, along with an 'All Actions' dropdown. A filter dropdown is set to 'All Systems' with a 'Filter' button. The main content is a table with the following data:

Profile	Server	Rack Name/Unit	Chassis/Bay	Profile Status	Pattern
SR650PatternThinkAgileSXM_121218-profile6	Lenovo-01	Unassigned / Un		Active	SR650PatternThinkAgileSXM_121218
SR650PatternThinkAgileSXM_121218-profile7	Lenovo-02	Unassigned / Un		Active	SR650PatternThinkAgileSXM_121218
SR650PatternThinkAgileSXM_121218-profile8	Lenovo-03	Unassigned / Un		Active	SR650PatternThinkAgileSXM_121218
SR650PatternThinkAgileSXM_121218-profile9	Lenovo-04	Unassigned / Un		Active	SR650PatternThinkAgileSXM_121218

Figure 88. Server profiles with Active status

This completes the LXCA deployment and configuration process.

Appendix B. Updating ThinkAgile SXM Series switches using the CLI (Lenovo switches only)

If updating the ThinkAgile SXM Series switch firmware using XClarity Administrator doesn't work (for example, if the current switch firmware version does not allow update via XClarity Administrator), follow this procedure to update the ThinkAgile SXM Series switch firmware using the CLI.

Prerequisites

Follow the instructions in this topic before starting switch firmware update using the CLI.

Before work can begin, make sure you have the following items available:

- Lenovo Specific Serial Cable (Mini-USB-RJ45-Serial) supplied with switch
- USB to Serial cable
- USB thumb drive (must be formatted as FAT32 and must not have a capacity greater than 32GB)
- Appropriate switch firmware images, based on the ThinkAgile SXM Best Recipe

Prepare switch image files

Prepare the switch image files for switch firmware update as instructed in this topic.

The switch firmware image files are contained in the main firmware update archive found in the ThinkAgile SXM Updates Repository. This archive is titled using the format *<Platform>Firmware_SXMBR<yyyy>.zip*, where *<Platform>* is either "Broadwell" or "Purley" and *yyyy* represents the ThinkAgile SXM Best Recipe version. To prepare the switch firmware image files for update using the CLI method, follow these steps:

- Step 1. Extract all content from the main firmware update archive file.
- Step 2. In the extracted directory, look for the appropriate switch firmware update files. The following example shows the firmware update packages for the switches included in Broadwell-based ThinkAgile SXM solutions.

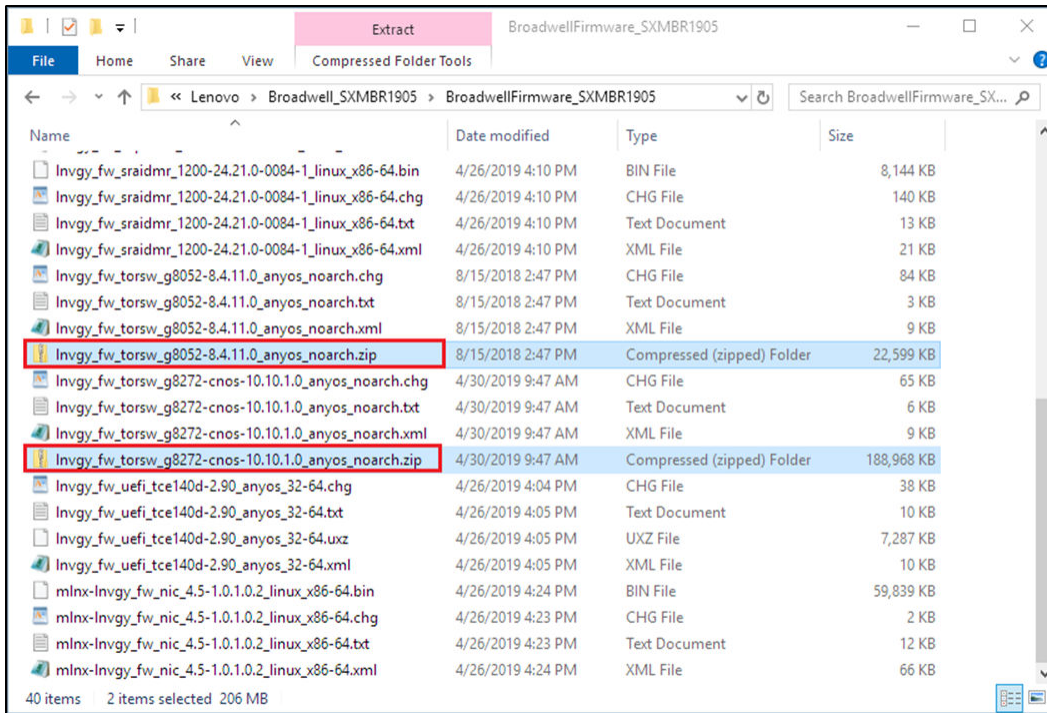


Figure 89. Broadwell-based ThinkAgile SXM switch firmware update packages

Step 3. For each switch to be updated, open the appropriate zip archive file. The following example shows the contents of the archive for the RackSwitch G8272 TOR switches included in Broadwell-based ThinkAgile SXM solutions.

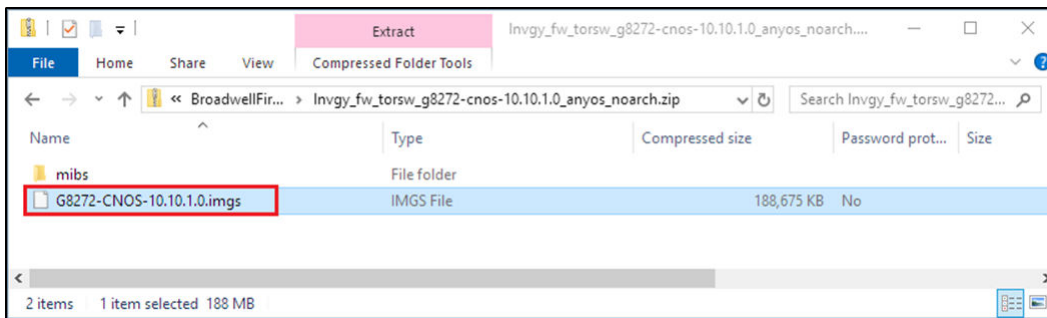


Figure 90. Switch firmware update archive contents

Step 4. Select the IMGS image files and copy the files. Note that for the BMC switch running ENOS, there are two IMGS files, as shown in the following example.

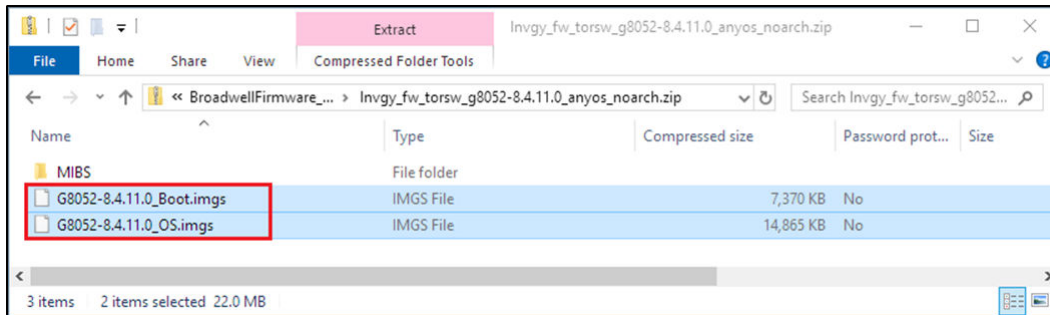


Figure 91. ThinkAgile SXM switch firmware IMGS image files

- Step 5. Paste the image files into the root of the USB thumb drive.
- Step 6. Repeat this procedure to copy any other required switch image files to the USB thumb drive.

Verify Azure Stack Hub health

Before working with any switches, it is important to verify that the Azure Stack Hub environment is healthy.

To do this, sign in to the Azure Stack Hub Administrator Portal and verify that no alerts are being displayed. See the following illustration for an example. We will refer back to the portal throughout this process to check the general health of the solution.

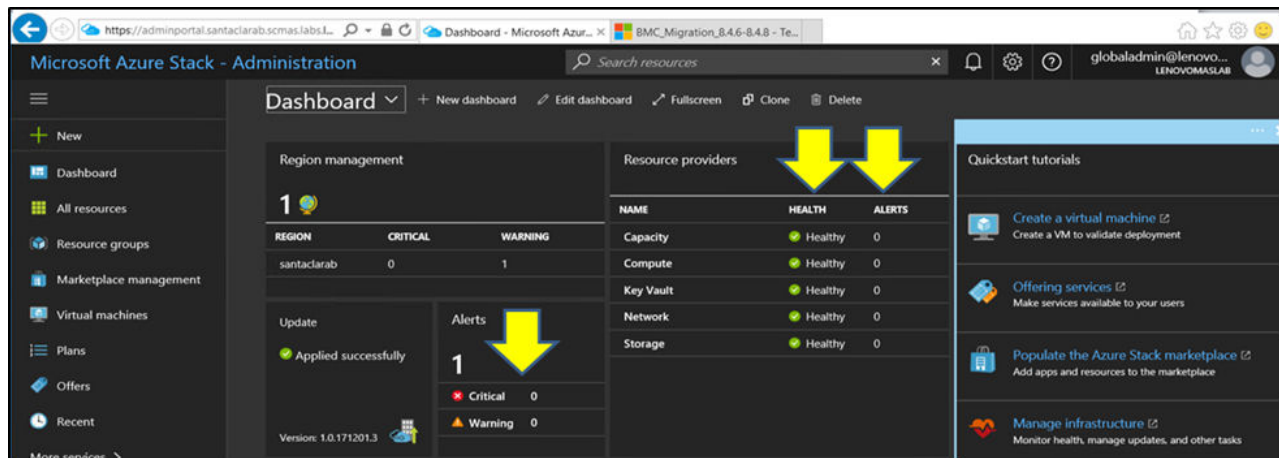


Figure 92. Verifying Azure Stack Hub health

Updating Lenovo TOR switch firmware using the CLI

This topic outlines the sequence of steps required to update the CNOS image of Lenovo TOR switches. The process is the same for the Lenovo G8272 RackSwitch switches found in the Broadwell solutions and the Lenovo ThinkSystem NE2572 RackSwitch switches found in the Purley solutions.

Back up TOR switch configurations

Before beginning the update procedure, ensure that both TOR switch configurations have been backed up.

Although switch configuration backup can be done using XClarity Administrator v2.1 and later, switch CLI commands are provided here since a serial connection and USB thumb drive are used for the steps in this appendix.

For the two TOR switches running CNOS, use these steps:

- Step 1. Connect to the TOR1 switch via serial console from the HLH.
- Step 2. Insert the USB thumb drive into the TOR1 switch.
- Step 3. Sign in to the TOR1 switch using the credentials `admin/<password>`.
- Step 4. Use the following commands to copy the currently running configuration to the startup configuration and save the configuration file to the root of the USB thumb drive:

```
enable
cp running-config startup-config
cp startup-config usb1 TOR1StartupBackup.cfg
system eject-usb
```

- Step 5. You can now remove the USB thumb drive from the TOR1 switch.
- Step 6. Connect to the TOR2 switch via serial console from the HLH.
- Step 7. Insert the USB thumb drive into the TOR2 switch.
- Step 8. Sign in to the TOR2 switch using the credentials `admin/<password>`.
- Step 9. Use the following commands to copy the currently running configuration to the startup configuration and save the configuration file to the root of the USB thumb drive:

```
enable
cp running-config startup-config
cp startup-config usb1 TOR2StartupBackup.cfg
system eject-usb
```

- Step 10. You can now remove the USB thumb drive from the TOR2 switch.

The TOR switch configurations are now backed up to the USB drive in case issues are encountered during switch updating and the switches need to be recovered to the current configuration.

Update CNOS on TOR switches using the CLI

This procedure describes how to update the CNOS on your ThinkAgile SXM Series TOR switches (Lenovo ThinkSystem NE2572 RackSwitch for Purley-based solutions and Lenovo RackSwitch G8272 for Broadwell-based solutions).

Examples in this topic might show slightly different results, depending on the version of CNOS against which the commands are run. Important aspects shown in examples are called out.

To update CNOS on your ThinkAgile SXM Series TOR switches, follow these steps on the TOR1 switch, then verify switch functionality before repeating the process on the TOR2 switch.

- Step 1. Insert the USB thumb drive into the TOR switch.
- Step 2. Connect to the TOR switch using the serial console from the HLH.
- Step 3. Sign in to the TOR switch using the credentials `admin/<password>`.
- Step 4. Use the following commands to copy the new switch firmware image file from the root of the USB thumb drive to the standby image slot on the TOR switch (replace the bracketed item with the actual switch image file name):

```
enable
cp usb1 <ImageFileName>.imgs system-image all
```

Example

```
TOR1 login: admin
Password:
...
TOR1#enable
TOR1#cp usb1 CNOS/G8272-CNOS-10.6.1.0.imgs system-image all
WARNING: This operation will overlay the currently booting image.
Confirm download operation (y/n)? y
TOR1#
```

Step 5. To verify that the switch is set to restart using the new standby image, run the following command:

```
display boot
```

Example

```
TOR1#display boot
Current ZTP State: Enable
Current FLASH software:
  active image: version 10.6.1.0, downloaded 20:49:51 UTC Tue Jan 16 2018
  standby image: version 10.8.1.0, downloaded 10:25:35 UTC Thu Jan 11 2018
  Uboot: version 10.8.1.0, downloaded 07:47:27 UTC Sun Jan 14 2018
  ONIE: empty
Currently set to boot software active image
Current port mode: default mode
Next boot port mode: default mode
Currently scheduled reboot time: none
```

In the above example, two key details are found:

- New switch firmware is available in the standby image.
- Switch is set to boot to the active image; this must be changed.

Step 6. To change the image from which the switch will boot, run the following commands:

```
configure
startup image standby
exit
```

Example

```
TOR1#configure
TOR1(config)# startup image standby
TOR1(config)#exit
TOR1#display boot
Current ZTP State: Enable
Current FLASH software:
  active image: version 10.6.1.0, downloaded 20:49:51 UTC Tue Jan 16 2018
  standby image: version 10.8.1.0, downloaded 10:25:35 UTC Thu Jan 11 2018
  Uboot: version 10.8.1.0, downloaded 07:47:27 UTC Sun Jan 14 2018
  ONIE: empty
Currently set to boot software standby image
Current port mode: default mode
Next boot port mode: default mode
```

In the above example, running the display boot command again shows that the switch is now set to boot from the standby image, which contains the new switch firmware image.

Step 7. Before restarting the TOR switch to implement the changes, it is good practice to shut down all the ports on the switch and confirm that the other TOR switch has taken over and is processing all network traffic. To shut down the ports on the TOR switch that is being updated, run the following commands:

```
configure
interface ethernet 1/1-54
shutdown
exit
```

Step 8. Once the ports have been shut down, verify the failover of traffic to TOR2 by verifying connectivity. Follow these steps:

- a. Use the top menu of the XClarity Administrator browser interface to navigate to **Administration → Network Access**.
- b. Click the **Test Connection** button near the top of the interface.
- c. In the **Host** field, enter 8.8.8.8 and then click **Test Connection**.
- d. A Success window displays. Click **Close** to dismiss this window.
- e. As an additional verification step, sign in to the Azure Stack Hub Administrator Portal.
- f. Check the Azure Stack Hub Administrator Portal to ensure that no alerts are currently visible.

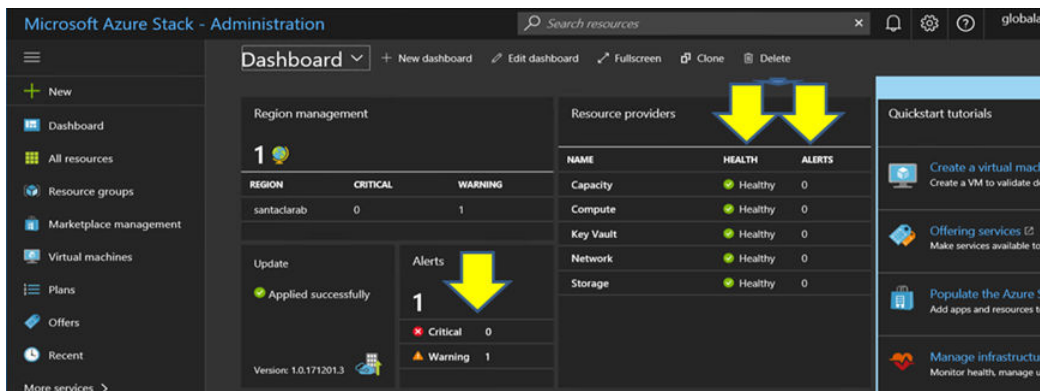


Figure 93. Checking Azure Stack Hub Administrator Portal for alerts

Step 9. Once switch failover is complete, restart the TOR switch that is being updated by issuing the following command: Reload

A warning is displayed since the current running configuration has all ports shut down, which is different from the current startup configuration. Enter **y** and press Enter to continue.

Important: Do NOT save the running configuration at this point or all ports will remain shut down after the switch is reloaded.

```
Example

TOR1(config)#reload
WARNING: The running-config is different to startup-config.
Confirm operation without saving running-config to startup-config (y/n)? y
... After reload ...
TOR1 login: admin
Password:
...
TOR1#enable
```


Step 10. Once the switch has come back online, sign in to the switch using the serial console.

Step 11. Remove the USB thumb drive from the TOR switch.

Refer to [“Verifying TOR switch functionality” on page 33](#) to ensure proper functionality of the updated TOR switch. Once verified, repeat the above process, including verification steps, on the other TOR switch. If the BMC switch also needs to be updated, proceed to [“Updating BMC switch firmware using the CLI” on page 97](#). Otherwise, the switch firmware update process is now complete.

Updating BMC switch firmware using the CLI

This topic outlines the sequence of steps that are required to update the ENOS image and configuration of the BMC switch using the switch CLI method. Although the process is similar to the one used for the TOR switches, the commands executed on the switch are different, since the BMC switch runs a different NOS than the TOR switches.

Back up BMC switch configuration

Before beginning the update procedure, ensure that the BMC switch configuration has been backed up.

To perform a backup of the BMC switch configuration file, follow these steps:

- Step 1. Insert a USB thumb drive into the BMC switch.
- Step 2. Connect to the BMC switch via serial console from the HLH.
- Step 3. Sign in to the BMC switch using the credentials `admin/<password>`.
- Step 4. Use the following commands to copy the currently running configuration to the startup configuration, and then save the startup (boot) configuration to the root of the USB thumb drive.

```
enable
copy running-config startup-config
usbcopy tusb BMCStartupBackup.cfg boot
```

The BMC switch configuration file is now backed up to the USB thumb drive in case issues are encountered during switch updating and the switch needs to be recovered to the current configuration.

Update the BMC switch using the CLI

The procedure describes how to update the Network Operating System on your ThinkAgile SXM Series BMC switch.

To update the BMC switch, follow these steps:

- Step 1. Connect to the BMC switch using the serial console from the HLH.
- Step 2. Sign in to the BMC switch using the credentials `admin/<password>`.
- Step 3. Use the following commands to copy the new switch OS image file from the root of the USB thumb drive to the ‘image2’ slot on the BMC switch, and the new switch boot image file to the ‘boot’ slot on the BMC switch:

```
enable
configure terminal
usbcopy fromusb <ImageFileName>_OS.imgs image2
usbcopy fromusb <ImageFileName>_Boot.imgs boot
```

Example

```
Enter login username: admin
Enter login password:
...
BMC#enable
BMC#configure terminal
BMC(config)#usbcopy fromusb G8052-8.4.8.0_OS.imgs image2
Switch to be booted with image1. (Y/N) : Y
BMC(config)#usbcopy fromusb G8052-8.4.8.0_Boot.imgs boot
```

- Step 4. To set the switch to reboot using the new OS image loaded in the 'image2' slot and the matching boot image, and then verify this setting, run the following commands:

```
boot image image2
exit
show boot
```

Example

```
BMC(config)#boot image image2
BMC(config)#exit
BMC#show boot
Current running image version: 8.4.8
Currently set to boot software image2, active config block.
NetBoot: disabled, NetBoot tftp server: , NetBoot cfgfile:
Current boot Openflow protocol version: 1.0
USB Boot: disabled
Currently profile is default, set to boot with default profile next time.
Current FLASH software:
  image1: version 8.4.8, downloaded 08:04:14 Fri Jan 19, 2018
          NormalPanel, Mode Stand-alone
  image2: version 8.4.11, downloaded 22:20:41 Thu Jan 18, 2018
          NormalPanel, Mode Stand-alone
  boot kernel: version 8.4.11
              NormalPanel
  bootloader : version 8.4.11
Currently scheduled reboot time: none
```

- Step 5. Before restarting the BMC switch to implement the changes, it is good practice to shut down all the ports on the switch. To shut down all ports on the BMC switch, run the following commands:

```
configure terminal
interface port 1-52
shutdown
exit
```

- Step 6. Eject the USB thumb drive from the BMC switch and reboot it by entering the following commands:

```
System usb-eject
reload
```

A warning is displayed since the current running configuration has all ports shut down, which is different from the current startup configuration. Enter *y* and press Enter to continue.

Important: Do NOT save the running configuration at this point or all ports will remain shut down after the switch is reloaded.

- Step 7. Once the switch has come back online, sign in to the switch using the serial console.

Step 8. Remove the USB thumb drive from the BMC switch.

Refer to [“Verifying BMC switch functionality” on page 45](#) to ensure proper functionality of the updated BMC switch. Once verification is complete, the switch firmware update process is complete.

Lenovo