Lenovo® XClarity™ Administrator Updating Firmware on Lenovo HX Series Appliances

August 2020

Contents

Introduction

Perform these steps to update firmware on Lenovo HX Series appliances.

1. Download and import the appropriate firmware-update package into XClarity Administrator.
2. Create a compliance policy with the imported firmware package, and assign the policy to each server in the cluster.
3. Perform the following steps for each server in the cluster, one at a time.
    a. Place a server in maintenance mode
    b. Update firmware using XClarity Administrator (I'm not actually sure if the systems should be shut down first for this, or if that's not required)
    c. After the update is complete, take server out of maintenance mode.

Download and import the firmware-update package

1. Download the appropriate update package from the Lenovo HX Series Best Recipe webpage to a workstation that has a network connection to the XClarity Administrator host.

    The Lenovo Best Recipe is a list of software and firmware components that were tested together for a Lenovo solution. It is a snapshot in time for what has been tested. As there are many different software and firmware components and, therefore, many possible combinations, the Best Recipe provides you with an effective point of reference. For more information about the Lenovo Best Recipes, see the ThinkAgile HX Series Best Recipes FAQs webpage.

2. From the XClarity Administrator menu bar, click **Provisioning > Firmware Updates: Repository** to display the Firmware Updates Repository page.
3. Click the **Individual Updates** tab.
4. Click the **Import** icon ().
5. Click **Select Files**, and browse to the location of the firmware updates that you just downloaded.
6. Select all package files, and then click **Open**.

    You must import the metadata file (.xml) as well as the image or payload file (.zip, .bin, .uxz, or .tgz), change history file (.chg), and readme file (.txt) for the update. Any files that are selected but are not specified in the .xml file are discarded.

    Attention:

    - Only import these required files. Do not import other files that might be found on the firmware download websites.
    - If you do not include the XML file in the update package, the update is not imported.
    - If you do not include all required files that are associated with the update, the repository shows that the update is not downloaded, which means that it is partially imported. You can then import the missing files by selecting and importing them.

7. Click **Import**.

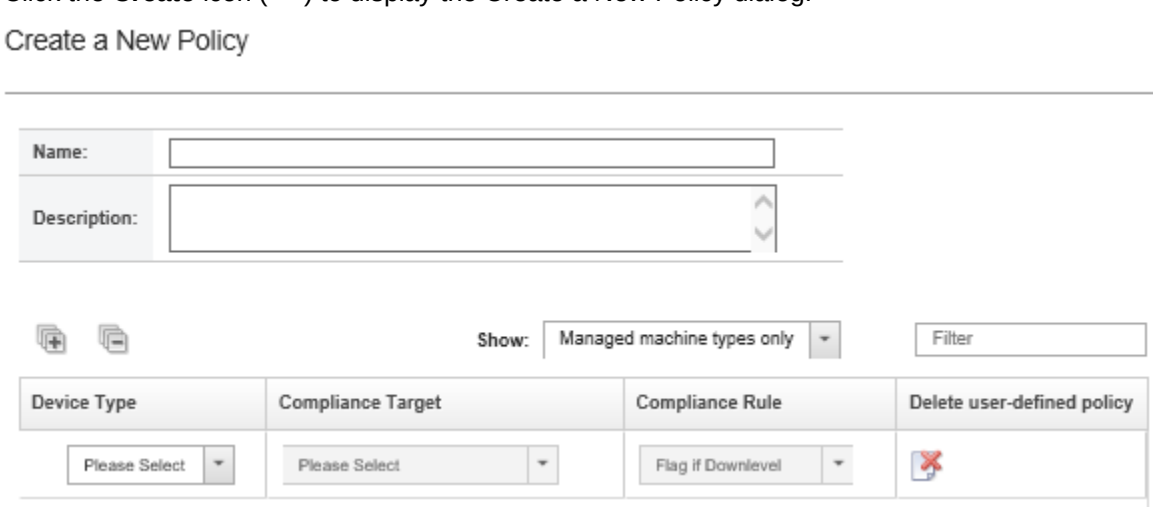
Create a compliance policy using the new firmware package

Firmware-compliance policies ensure that the firmware on certain devices is at the current or specific level by flagging the devices that need attention. Each firmware-compliance policy identifies which devices are monitored and which firmware level must be installed to keep the devices in compliance. XClarity Administrator then uses these policies to check the status of managed devices and to identify devices that are out of compliance.

XClarity Administrator comes with a predefined firmware-compliance policy named “Latest firmware in repository.” When new firmware is downloaded or imported into the repository and when XClarity Administrator is restarted, this policy is updated to include latest available versions of firmware in the repository. You can choose to use the “Latest firmware in repository” policy, or you can create custom policy.

Complete the following steps to create custom firmware-update compliance policy.

1. From the XClarity Administrator menu bar, click **Provisioning > Firmware Updates: Compliance Policies**. The Compliance Policy page is displayed with a list of all existing firmware-compliance policies.
2. Click the **Create** icon ( ) to display the Create a New Policy dialog.



3. Fill in the name and description for the firmware-compliance policy.

4. Fill in the table on the following criteria for each device:
    - **Device Type**. Choose a type of device for which this policy is to apply.

      Tip: If you choose a server, the compliance level is done at the UXSP level. However, you can also expand the server to specify specific firmware levels for each component, such as the baseboard management controller or UEFI.
    - **Compliance Target**. Select one of the following values the compliance target for the applicable server and subcomponents.
        - **Default**. Changes the firmware level of each subcomponent to the default level (such as the latest firmware in the repository for that server type).
        - **Custom**. Allows you to assign a specific firmware level to each subcomponent. Expand the system type to see a list of applicable subcomponents, and select the firmware level that you want to use for each subcomponent.
        - **Do not update**. Prevents the component from being updated.
    - **Compliance Rule**. Select when a device is to be flagged as "not compliant" in the Installed Version column on the Firmware Updates: Apply/Activate.
        - **Flag if Downlevel**. If the firmware level that is installed on a device is earlier than the level that is specified in the firmware-compliance policy, the device is flagged as not compliant. For example, if you replace a network adapter in a compute node, and the firmware on that network adapter is earlier than the level identified in the firmware-compliance policy, the compute node is flagged as not compliance.
        - **Flag if Not Exact Match**. If the firmware level that is installed on a device is not an exact match with the firmware-compliance policy, the device is flagged as not compliant. For example, if you replace a network adapter in a compute node, and the firmware on that network adapter is different than the level identified in the firmware-compliance policy, then the compute node is flagged as not compliance.
        - **No Flag**. Devices that are out of compliance are not flagged.
5. Click **Create**.

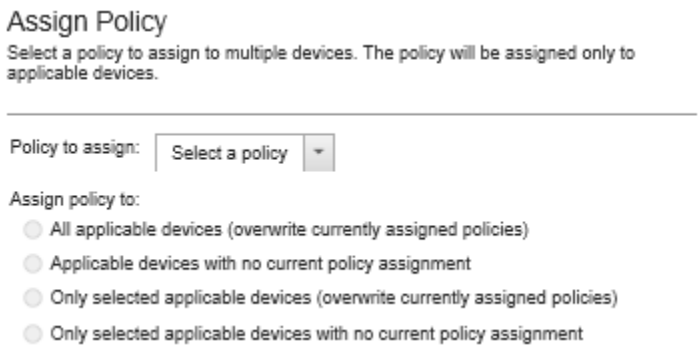
Assign the compliance policy to each node in the cluster

When a device is managed, XClarity Administrator automatically assigns the last-edited firmware-compliance policy that can be applied to that device. You can manually assign a different policy to a device.

Complete the following steps to assign the firmware-compliance policy that you just created to each node in the cluster.

1. From the XClarity Administrator menu bar, click **Provisioning > Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed with a list of managed devices.
2. Select each node in the cluster.

3. Click the **Assign policy** icon ( ) to display the Assign Policy dialog.



4. Select the firmware-compliance policy that you just created from the **Policy to assign** drop-down menu.
5. Select scopes for the policy assignment.
   - All applicable devices
   - All applicable devices with no current policy assignment
   - Only selected applicable devices
   - Only selected applicable devices with no current policy assignment
6. Click **OK**.

Place the node in maintenance mode

Check the cluster status and resiliency before proceeding. You can only place one node in maintenance mode for each cluster.

Complete the following steps to place the node in maintenance mode.

1. Log on to the Controller VM (CVM) or host using SSH.

   Note: For Hyper-V, you can use PowerShell.

2. Place CVM into maintenance mode.

   a. Get the CVM host ID by running the following command.

      ```
      ncli host ls
      ```

      The host ID is represented by the set of characters to the right of the double colon. For example, if the command returns `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx::11`, then the host ID is `11`.

   b. Change the CVM to maintenance mode by running the following command.

      ```
      ncli host edit id=<host_id> enable-maintenance-mode=true
      ```

3. Place the hypervisor in maintenance mode.
   - **ESXI**

     a. Place the hypervisor in maintenance mode by running the following command.

        ```
        esxcli system maintenanceMode set --enable true
        ```

     b. Verify the maintenance mode status by running the following command.

```
esxcli system maintenanceMode get
```

- **Nutanix AHV**
  a. Get the hypervisor host address by running the following command.
     ```
     acli host.list
     ```
  b. Place the hypervisor in maintenance mode by running the following command.
     ```
     acli host.enter_maintenance_mode <hypervisor_address>
     wait=true
     ```
- **Hyper-V using SCVMM**
  a. In the VMM console, click **Fabric > Fabric Resources > Servers > All Hosts**.
  b. Select the host to place in maintenance mode.
  c. In the Host group, select **Start Maintenance Mode** and then select:
     - **Move all virtual machines to other hosts in the cluster.** Moves all highly available VMs to other hosts in the cluster. Note that the host must be in a cluster that's capable of live migration.
     - **Place all running virtual machines into a saved state**. Note that list causes a loss of service for users currently using the VM.
  d. You can verify that host is in maintenance mode by checking its status in **Fabric > Hosts**.
- **Hyper-V not using SCVMM**
  a. Pause the Hyper-V host in a failover cluster running the following PowerShell command.
     ```
     Suspend-ClusterNode
     ```
  b. Verify the maintenance mode status by running the following PowerShell command.
     ```
     Get-ClusterNode
     ```

Updating firmware on the node

After Lenovo XClarity Administrator identifies a device as not compliant, you can manually apply and activate the firmware updates on these managed devices. You can choose to apply and activate all firmware updates that apply to a firmware-compliance policy or only specific firmware updates in a policy.

Before you begin, read the firmware-update considerations before you attempt to update firmware on your managed devices (see Firmware-update considerations).

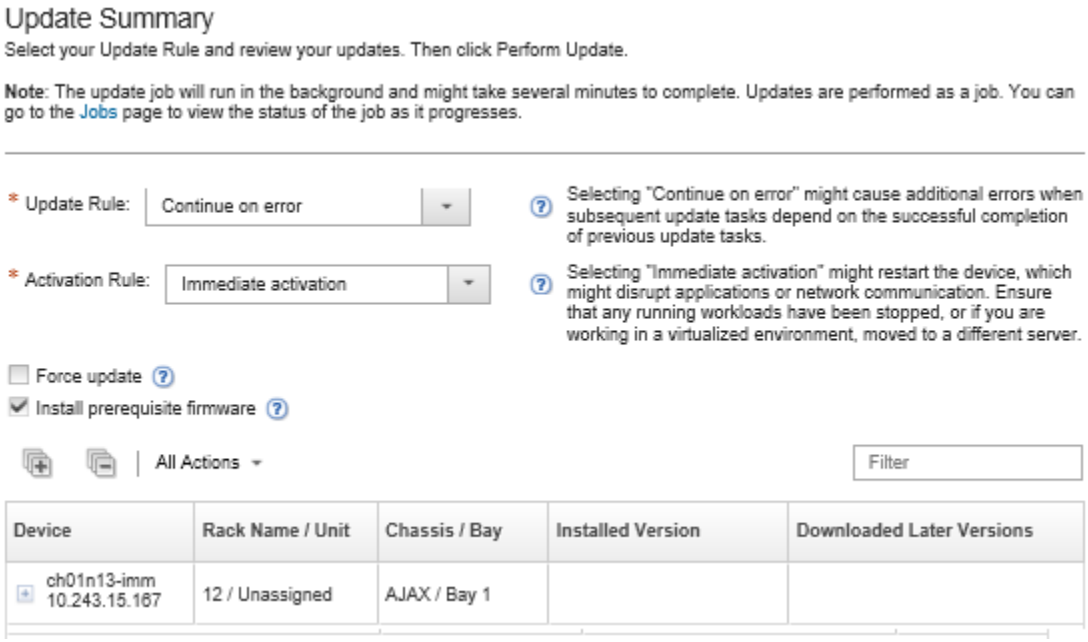
Complete the following steps to apply and activate updates on managed devices.

1. From the XClarity Administrator menu bar, click **Provisioning > Firmware Updates: Apply/Activate**. The Firmware Updates: Apply/Activate page is displayed.
2. Click the **Update with Policy** tab.

3. Select the node that you just placed in maintenance mode.

   You can sort the table columns to make it easier to find specific servers. In addition, you can filter the list of displayed devices by selecting an option in the Show menu to list only devices in a specific chassis, rack, or group, by entering text (such as a name or IP address) in the Filter field, or by clicking a status icon to list only devices with a specific status.

4. Click the **Perform Updates** icon ( ). The Update Summary dialog is displayed.



5. Select one of the following update rules.

   - **Stop all updates on error**. If an error occurs while updating any of the components (such as an adapter or management controller) in the target device, the firmware-update process stops for all selected devices in the current firmware-update job. In this case, none of the updates in the update package for the device are applied. The current firmware that is installed on all selected systems remains in effect.
   - **Continue on error**. If an error occurs while updating any of the devices in the device, the firmware-update process does not update the firmware for that specific device; however, the firmware-update process continues to update the other devices in the device and continues to update all other devices in the current firmware-update job.
   - **Continue to next system on error**. If an error occurs while updating any of the devices in the device, the firmware-update process stops all attempts to update the firmware for that specific device, so the current firmware that is installed on that device remains in effect. The firmware-update process continues to update all other devices in the current firmware-update job.

6. Select one of the following activation rules.

    - **Immediate activation**. During the update process, the device might be restarted automatically a number of times until the entire update process is complete. Ensure that you quiesce all applications on the device before you proceed.
    - **Delayed activation**. Some but not all update operations are performed. Devices must be restarted manually to continue the update process. Additional restarts are then performed until the update operation completes. If a device restarts for any reason, the delayed update process completes.
    - **Prioritized activation**. Firmware updates on the baseboard management controller are activated immediately; all other firmware updates are firmware updates are activated the next time the device is restarted. Additional restarts are then performed until the update operation completes. This rule is supported only for servers.

    Note: When enabled, the Wake-on-LAN boot option can interfere with XClarity Administrator operations that power off the server, including firmware updates if there is a Wake-on-LAN client in your network that issues "Wake on Magic Packet" commands.

7. **Optional:** Clear Install prerequisite firmware if you do not want to install prerequisite firmware. Prerequisite firmware is installed by default.

    Note: When using Delayed Activation or Prioritized Activation for prerequisite firmware updates, you might need to restart the server to activate the prerequisite firmware. After the initial restart, the remaining firmware updates are installed using Immediate Activation.

8. **Optional:** Select Force update to update firmware on the selected components even if the firmware level is up to date or to apply a firmware update that is earlier than the one currently installed on the selected components.

    Note: You cannot apply earlier levels of firmware to device options, adapters, or disk drivers.

9. Click Perform Update to update immediately, or click Schedule to schedule this update to run at a later time.

    If needed, you can perform power actions on the managed devices. The power actions are useful when Delayed Activation is selected and you want the updates to continue when the device is waiting in the "Pending Maintenance" state. To perform a power action on a managed device from this page, click All Actions > Power Actions, and then click one of the following power actions.

    - **Power on**
    - **Power down OS and power off**
    - **Power off**
    - **Shut down OS and restart**
    - **Restart**

Take the node out of maintenance mode

Complete the following steps to take the node out of maintenance mode.

1. Take the hypervisor out of maintenance mode.
   - **ESXi.** Run the following command**.**

     ```
     esxcli system maintenanceMode set --enable false
     ```

   - **Nutanix AHV.** Run the following command.

     ```
     acli host.enter_maintenance_mode <hypervisor_address>
     wait=true
     ```

   - **Hyper-V using SCVMM.** Select the host, and click **Stop Maintenance Mode**. Note that VMM does not automatically restart the VM, and doesn't automatically migrate VMs back to the host
   - **Hyper-V not using SCVMM.** Run the following command.

     ```
     Resume-ClusterNode
     ```

2. Take CVM out of maintenance mode by running the following command from a CVM that is not in maintenance mode.

   ```
   nutanix@cvm$ ncli host edit id=<host_id> enable-maintenance-
   mode=false
   ```