



# Upgrade compute node firmware

## HCI

Dave Bagwell, Michael Wallis, amitha  
December 14, 2020

This PDF was generated from [https://docs.netapp.com/us-en/hci/docs/task\\_hcc\\_upgrade\\_compute\\_node\\_firmware.html](https://docs.netapp.com/us-en/hci/docs/task_hcc_upgrade_compute_node_firmware.html) on December 14, 2020. Always check docs.netapp.com for the latest.

# Table of Contents

- Upgrade compute node firmware. . . . . 1
  - Use NetApp Hybrid Cloud Control UI to upgrade a compute node . . . . . 2
  - Use NetApp Hybrid Cloud Control API to upgrade a compute node . . . . . 7
  - Use a USB drive with the latest compute node firmware ISO downloaded. . . . . 13
  - Use the Baseboard Management Controller (BMC) user interface (UI). . . . . 14

# Upgrade compute node firmware

For H-series compute nodes, you can upgrade the firmware for hardware components such as the BMC, BIOS, and NIC. To upgrade compute node firmware, you can use the NetApp Hybrid Cloud Control UI, REST API, a USB drive with the latest firmware image, or the BMC UI.

After the upgrade, the compute node boots into ESXi and works as before, retaining the configuration.

### What you'll need

- **Compute drivers:** You have upgraded your compute node drivers. If compute node drivers are not compatible with the new firmware, the upgrade will not start. See the [Interoperability Matrix Tool \(IMT\)](#) for driver and firmware compatibility information, and check the latest [compute node firmware release notes](#) for important late-breaking firmware and driver details.
- **Admin privileges:** You have cluster administrator and BMC administrator permissions to perform the upgrade.
- **System ports:** If you are using NetApp Hybrid Cloud Control for upgrades, you have ensured that the necessary ports are open. See [Network ports](#) for more information.
- **Minimum BMC and BIOS versions:** The node you intend to upgrade using NetApp Hybrid Cloud Control meets the following minimum requirements:

Model	Minimum BMC version	Minimum BIOS version
H300E, H500E, H700E	6.84.00	NA2.1
H410C	All versions supported (no upgrade required)	All versions supported (no upgrade required)
H610C	3.96.07	3B01
H615C	4.68.07	3B08.CO



H615C compute nodes must update BMC firmware to version 4.68 using the [compute firmware bundle 2.27](#) to enable NetApp Hybrid Cloud Control to perform future firmware upgrades.



A Redfish license is required for H300E, H500E, and H700E compute nodes to enable NetApp Hybrid Cloud Control to perform future firmware upgrades. Contact NetApp Support to get the license installed manually until a new compute firmware bundle automates this process in a follow-on release.



For a complete matrix of firmware and driver firmware for your hardware, see [this KB article](#) (login required).

- **BIOS boot order:** Manually change the boot order in the BIOS setup for each node to ensure [USB CD/DVD](#) appears in the boot list. See this [article](#) for more information.
- **BMC credentials:** Update the credentials NetApp Hybrid Cloud Control uses to connect to the compute node BMC. You can do this using either the NetApp Hybrid Cloud Control [UI](#) or [API](#). Updating BMC information prior to upgrade refreshes the inventory and ensures that management node services are aware of all hardware parameters needed to complete the upgrade.
- **Attached media:** Disconnect any physical USB or ISO before starting a compute node upgrade.
- **KVM ESXi console:** Close all open Serial-Over-LAN (SOL) sessions and active KVM sessions in the BMC UI before starting a compute node upgrade.
- **Witness Node requirements:** In two- and three-node storage clusters, one [Witness Node](#) must be running in the NetApp HCI installation at all times.
- **Compute node health check:** You have verified that the node is ready to be upgraded. See [Run compute node health checks prior to upgrading compute firmware](#).

#### *About this task*

In production environments, upgrade the firmware on one compute node at a time.

For NetApp Hybrid Cloud Control UI or API upgrades, your ESXi host will be automatically placed in maintenance mode during the upgrade process if you have the DRS feature and required licensing. The node will be rebooted and after the upgrade process is complete, the ESXi host will be taken out of maintenance mode. For USB and BMC UI options, you will need to place the ESXi host in maintenance mode manually, as described in each procedure.

#### *Upgrade options*

Choose the option that is relevant to your upgrade scenario:

- [Use NetApp Hybrid Cloud Control UI to upgrade a compute node](#) (Recommended)
- [Use NetApp Hybrid Cloud Control API to upgrade a compute node](#)
- For compute node image 12.0: [Use a USB drive with the latest compute node firmware ISO downloaded](#)
- For compute firmware 12.2.109: [Use the Baseboard Management Controller \(BMC\) user interface \(UI\)](#)

## Use NetApp Hybrid Cloud Control UI to upgrade a compute node

Starting with management services 2.14, you can upgrade a compute node using the NetApp Hybrid Cloud Control UI. From the list of nodes, you must select the node to upgrade. The **Current Versions** tab shows the current firmware versions and the **Proposed Versions** tab shows the available upgrade versions, if any.



For a successful upgrade, ensure that the health check on the vSphere cluster is successful.



For dark site upgrades, you can reduce upload time if the upgrade package and the management node are both local.



Upgrading the NIC, BIOS, and BMC can take approximately 60 minutes per node depending on the speed of network connectivity between the management node and the BMC host.

### *What you'll need*

- If your management node is not connected to the internet, you have downloaded the compute node firmware package from the [NetApp Support Site](#).



You should extract the **TAR.GZ** file to a **TAR** file, and then extract the **TAR** file to the ISO.




### *Steps*

1. Open a web browser and browse to the IP address of the management node:

```
https://<ManagementNodeIP>
```

2. Log in to NetApp Hybrid Cloud Control by providing the storage cluster administrator credentials.
3. Click **Upgrade** near the top right of the interface.
4. On the **Upgrades** page, select **Compute firmware**.
5. Choose from the following options and perform the set of steps that are applicable to your cluster:



Option	Steps
<p>Your management node has external connectivity.</p>	<ol style="list-style-type: none"> <li data-bbox="857 163 1485 363"> <p>1. Select the cluster you are upgrading.</p> <p>You will see the nodes in the cluster listed along with the current firmware versions and newer versions, if available for upgrade.</p> </li> <li data-bbox="857 394 1258 436"> <p>2. Select the upgrade package.</p> </li> <li data-bbox="857 457 1485 1161"> <p>3. Click <b>Begin Upgrade</b>.</p> <p>After you click <b>Begin Upgrade</b>, the window shows failed health checks, if any.</p> <div data-bbox="938 867 995 940">  </div> <div data-bbox="1076 657 1461 1150"> <p>The upgrade cannot be paused after you begin. Firmware will be updated sequentially in the following order: NIC, BIOS, and BMC. Do not log in to the BMC UI during upgrade. Logging into the BMC terminates the Hybrid Cloud Control Serial-Over-LAN (SOL) session that monitors upgrade process.</p> </div> </li> <li data-bbox="857 1203 1485 2001"> <p>4. If the health checks at the cluster or node level passed with warnings, but without critical failures, you will see <b>Ready to be Upgraded</b>. Click <b>Upgrade Node</b>.</p> <div data-bbox="889 1518 954 1581">  </div> <div data-bbox="1027 1413 1461 1696"> <p>While the upgrade is in progress, you can leave the page and come back to it later to continue monitoring the progress. During the upgrade, the UI shows various messages about the status of the upgrade.</p> </div> <div data-bbox="898 1843 946 1906">  </div> <div data-bbox="1027 1759 1461 2001"> <p>While upgrading the firmware on H610C compute nodes, do not open the Serial-Over-LAN (SOL) console through the BMC web UI. This might cause the upgrade to fail.</p> </div> </li> </ol>

The UI displays a message after the upgrade is

Option	Steps
Your management node is within a dark site without external connectivity.	<ol style="list-style-type: none"> <li>1. Select the cluster you are upgrading.</li> <li>2. Click <b>Browse</b> to upload the upgrade package that you downloaded from the <a href="#">NetApp Support Site</a>.</li> <li>3. Wait for the upload to complete. A progress bar shows the status of the upload.</li> </ol> <div>  <p>The file upload will happen in the background if you navigate away from the browser window.</p> </div> <p>An on-screen message is displayed after the file is successfully uploaded and validated. Validation might take several minutes.</p> <p>You can download logs after the upgrade is complete. For information about the various upgrade status changes, see <a href="#">Upgrade status changes</a>.</p>



If a failure happens during the upgrade, NetApp Hybrid Cloud Control will reboot the node, take it out of maintenance mode, and display the failure status with a link to the error log. You can download the error log, which contains specific instructions or links to KB articles, to diagnose and correct any issue. For additional insight into compute node firmware upgrade issues using NetApp Hybrid Cloud Control, see this [KB](#) article.

## Upgrade status changes

Here are the different states that the UI shows before, during, and after the upgrade process:

Upgrade state	Description
Node failed one or more health checks. Expand to view details.	One or more health checks failed.
Error	An error has occurred during the upgrade. You can download the error log and send it to NetApp Support.



Upgrade state	Description
Unable to Detect	NetApp Hybrid Cloud Control does not have external connectivity to reach the online software repository. This status is also displayed if NetApp Hybrid Cloud Control is unable to query the compute node when the compute node asset does not have the hardware tag.
Ready to be Upgraded.	All the health checks passed successfully, and the node is ready to be upgraded.
An error has occurred during the upgrade.	The upgrade fails with this notification when a critical error occurs. Download the logs by clicking the <b>Download Logs</b> link to help resolve the error. You can try upgrading again after you resolve the error.
Node upgrade is in progress.	The upgrade is in progress. A progress bar shows the upgrade status.

## Use NetApp Hybrid Cloud Control API to upgrade a compute node

You can use APIs to upgrade each compute node in a cluster to the latest firmware version. You can use an automation tool of your choice to run the APIs. The API workflow documented here uses the REST API UI available on the management node as an example.

### *What you'll need*

Compute node assets, including vCenter and hardware assets, must be known to management node assets. You can use the inventory service APIs to verify assets ([https://\[management node IP\]/inventory/1/](https://[management node IP]/inventory/1/)).

### *Steps*

1. Do one of the following depending on your connection:

Option	Steps
<p>Your management node has external connectivity.</p>	<ol style="list-style-type: none"> <li>1. Verify the repository connection: <ol style="list-style-type: none"> <li>a. Open the package service REST API UI on the management node: <div data-bbox="938 331 1487 470" data-label="Text" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> https://[management node IP]/package-repository/1/ </div> </li> <li>b. Click <b>Authorize</b> and complete the following: <ol style="list-style-type: none"> <li>i. Enter the cluster user name and password.</li> <li>ii. Enter the client ID as <code>mnode-client</code>.</li> <li>iii. Click <b>Authorize</b> to begin a session.</li> <li>iv. Close the authorization window.</li> </ol> </li> <li>c. From the REST API UI, click <b>GET /packages/remote-repository/connection</b>.</li> <li>d. Click <b>Try it out</b>.</li> <li>e. Click <b>Execute</b>.</li> <li>f. If code 200 is returned, go to the next step. If there is no connection to the remote repository, establish the connection or use the dark site option.</li> </ol> </li> <li>2. Find the upgrade package ID: <ol style="list-style-type: none"> <li>a. From the REST API UI, click <b>GET /packages</b>.</li> <li>b. Click <b>Try it out</b>.</li> <li>c. Click <b>Execute</b>.</li> <li>d. From the response, copy and save the upgrade package name ("<code>packageName</code>") and package version ("<code>packageVersion</code>") for use in a later step.</li> </ol> </li> </ol>

Option	Steps
<p>Your management node is within a dark site without external connectivity.</p>	<ol style="list-style-type: none"> <li data-bbox="852 163 1485 325"> <p>Go to the NetApp HCI software <a href="#">download page</a> and download the latest compute node firmware image to a device that is accessible to the management node.</p> <div data-bbox="938 359 1485 590"> <div data-bbox="943 443 992 510"></div> <div data-bbox="1073 373 1461 575"> <p>For dark site upgrades, you can reduce upload time if the upgrade package and the management node are both local.</p> </div> </div> </li> <li data-bbox="852 625 1485 1984"> <p>Upload the compute firmware upgrade package to the management node:</p> <ol style="list-style-type: none"> <li data-bbox="901 724 1485 800"> <p>Open the management node REST API UI on the management node:</p> <div data-bbox="938 835 1485 972"> <pre>https://[management node IP]/package-repository/1/</pre> </div> </li> <li data-bbox="901 1008 1485 1354"> <p>Click <b>Authorize</b> and complete the following:</p> <ol style="list-style-type: none"> <li data-bbox="954 1108 1485 1184">Enter the cluster user name and password.</li> <li data-bbox="954 1207 1485 1241">Enter the client ID as <code>mnode-client</code>.</li> <li data-bbox="954 1264 1485 1297">Click <b>Authorize</b> to begin a session.</li> <li data-bbox="954 1320 1485 1354">Close the authorization window.</li> </ol> </li> <li data-bbox="901 1377 1485 1453"> <p>From the REST API UI, click <b>POST /packages</b>.</p> </li> <li data-bbox="901 1476 1485 1509"> <p>Click <b>Try it out</b>.</p> </li> <li data-bbox="901 1533 1485 1608"> <p>Click <b>Browse</b> and select the upgrade package.</p> </li> <li data-bbox="901 1631 1485 1665"> <p>Click <b>Execute</b> to initiate the upload.</p> </li> <li data-bbox="901 1688 1485 1764"> <p>From the response, copy and save the package ID ("<code>id</code>") for use in a later step.</p> </li> </ol> </li> <li data-bbox="852 1787 1485 1984"> <p>Verify the status of the upload.</p> <ol style="list-style-type: none"> <li data-bbox="901 1850 1485 1984"> <p>From the REST API UI, click <b>GET /packages/{id}/status</b>.</p> <p>Click <b>Try it out</b>.</p> <p>Enter the package ID you copied in the previous step in <code>id</code>.</p> </li> </ol> </li> </ol>

2. Locate the compute controller ID and node hardware ID for the node you intend to upgrade:

- a. Open the inventory service REST API UI on the management node: **Click Execute** to initiate the status request

```
https://[management node IP]/inventory/1/
```

when complete.

- b. Click **Authorize** and complete the following:
- Enter the cluster user name and password.
  - Enter the client ID as `mnode-client`.
  - Click **Authorize** to begin a session.
  - Close the authorization window.
- c. From the REST API UI, click **GET /installations**.
- d. Click **Try it out**.
- e. Click **Execute**.
- f. From the response, copy the installation asset ID ("`id`").
- g. From the REST API UI, click **GET /installations/{id}**.
- h. Click **Try it out**.
- i. Paste the installation asset ID into the `id` field.
- j. Click **Execute**.
- k. From the response, copy and save the cluster controller ID ("`controllerId`") and node hardware ID ("`hardwareId`") for use in a later step:

```
"compute": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterId": "Test-1B",
        "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
```

```
"nodes": [  
  {  
    "bmcDetails": {  
      "bmcAddress": "10.111.0.111",  
      "credentialsAvailable": true,  
      "credentialsValidated": true  
    },  
    "chassisSerialNumber": "111930011231",  
    "chassisSlot": "D",  
    "hardwareId": "123a4567-01b1-1243-a12b-11ab11ab0a15",  
    "hardwareTag": "00000000-0000-0000-0000-ab1c2de34f5g",  
    "id": "e1111d10-1a1a-12d7-1a23-ab1cde23456f",  
    "model": "H410C",  
  },  
]
```

3. Run the compute node firmware upgrade:

- a. Open the hardware service REST API UI on the management node:

```
https://[management node IP]/hardware/2/
```

- b. Click **Authorize** and complete the following:

- i. Enter the cluster user name and password.
- ii. Enter the client ID as `mnode-client`.
- iii. Click **Authorize** to begin a session.
- iv. Close the authorization window.

- c. Click **POST /nodes/{hardware\_id}/upgrades**.

- d. Click **Try it out**.

- e. Enter the hardware host asset ID ("`hardwareId`" saved from a previous step) in the parameter field.

- f. Do the following with the payload values:

- i. Retain the values "`force`: `false`" and "`maintenanceMode`: `true`" so that health checks are performed on the node and the ESXi host is set to maintenance mode.
- ii. Enter the cluster controller ID ("`controllerId`" saved from a previous step).
- iii. Enter the package name and package version you saved from a previous step.

```
{
  "config": {
    "force": false,
    "maintenanceMode": true
  },
  "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
  "packageName": "compute-firmware-12.2.109",
  "packageVersion": "12.2.109"
}
```

g. Click **Execute** to initiate the upgrade.



The upgrade cannot be paused after you begin. Firmware will be updated sequentially in the following order: NIC, BIOS, and BMC. Do not log in to the BMC UI during upgrade. Logging into the BMC terminates the Hybrid Cloud Control Serial-Over-LAN (SOL) session that monitors upgrade process.

h. Copy the upgrade task ID that is part of the resource link ("**resourceLink**") URL in the response.

4. Verify the upgrade progress and results:

a. Click **GET /task/{task\_id}/logs**.

b. Click **Try it out**.

c. Enter the task ID from the previous step in **task\_Id**.

d. Click **Execute**.

e. Do one of the following if there are problems or special requirements during the upgrade:

Option	Steps
You need to correct cluster health issues due to <b>failedHealthChecks</b> message in the response body.	<ol style="list-style-type: none"> <li>1. Go to the specific KB article listed for each issue or perform the specified remedy.</li> <li>2. If a KB is specified, complete the process described in the relevant KB article.</li> <li>3. After you have resolved cluster issues, reauthenticate if needed and click <b>POST /nodes/{hardware_id}/upgrades</b>.</li> <li>4. Repeat the steps as described previously in the upgrade step.</li> </ol>
The upgrade fails and the mitigation steps are not listed in upgrade log.	<ol style="list-style-type: none"> <li>1. See this <a href="#">KB article (login required)</a>.</li> </ol>

f. Run the **GET /task/{task\_id}/logs** API multiple times, as needed, until the process is complete.

During the upgrade, the `status` indicates `running` if no errors are encountered. As each step finishes, the `status` value changes to `completed`.

The upgrade has finished successfully when the status for each step is `completed` and the `percentageCompleted` value is `100`.

5. (Optional) Confirm upgraded firmware versions for each component:

- a. Open the hardware service REST API UI on the management node:

```
https://[management node IP]/hardware/2/
```

- b. Click **Authorize** and complete the following:

- i. Enter the cluster user name and password.
- ii. Enter the client ID as `mnode-client`.
- iii. Click **Authorize** to begin a session.
- iv. Close the authorization window.

- c. From the REST API UI, click **GET /nodes/{hardware\_id}/upgrades**.

- d. (Optional) Enter date and status parameters to filter the results.

- e. Enter the hardware host asset ID ("`hardwareId`" saved from a previous step) in the parameter field.

- f. Click **Try it out**.

- g. Click **Execute**.

- h. Verify in the response that firmware for all components has been successfully upgraded from the previous version to the latest firmware.

## Use a USB drive with the latest compute node firmware ISO downloaded

You can insert a USB drive with the latest compute node firmware ISO downloaded to a USB port on the compute node. As an alternative to using the USB thumb drive method described in this procedure, you can mount the ISO on the compute node using the **Virtual CD/DVD** option in the Virtual Console in the Baseboard Management Controller (BMC) interface. The BMC method takes considerably longer than the USB thumb drive method. Ensure that your workstation or server has the necessary network bandwidth and that your browser session with the BMC does not time out.

### Steps

1. Browse to the [NetApp software downloads](#) page, click **NetApp HCI**, and click the download link for correct version of NetApp HCI.
2. Accept the End User License Agreement.

3. Under the **Compute and Storage Nodes** section, download the compute node image.
4. Use the Etcher utility to flash the compute node firmware ISO to a USB drive.
5. Place the compute node in maintenance mode using VMware vCenter, and evacuate all virtual machines from the host.



If VMware Distributed Resource Scheduler (DRS) is enabled on the cluster (this is the default in NetApp HCI installations), virtual machines will automatically be migrated to other nodes in the cluster.

6. Insert the USB thumb drive into a USB port on the compute node and reboot the compute node using VMware vCenter.
7. During the compute node POST cycle, press **F11** to open the Boot Manager. You may need to press **F11** multiple times in quick succession. You can perform this operation by connecting a video/keyboard or by using the console in **BMC**.
8. Select **One Shot > USB Flash Drive** from the menu that appears. If the USB thumb drive does not appear in the menu, verify that USB Flash Drive is part of the legacy boot order in the BIOS of the system.
9. Press **Enter** to boot the system from the USB thumb drive. The firmware flash process begins.

After firmware flashing is complete and the node reboots, it might take a few minutes for ESXi to start.

10. After the reboot is complete, exit maintenance mode on the upgraded compute node using vCenter.
11. Remove the USB flash drive from the upgraded compute node.
12. Repeat this task for other compute nodes in your ESXi cluster until all compute nodes are upgraded.

## Use the Baseboard Management Controller (BMC) user interface (UI)

You must perform the sequential steps to load the compute node firmware ISO and reboot the node to the ISO to ensure that the upgrade is successful. The ISO should be located on the system or virtual machine (VM) hosting the web browser. Ensure that you have downloaded the ISO before you start the process.



The recommendation is to have the system or VM and the node on the same network.



It takes approximately 25 to 30 minutes for the upgrade via the BMC UI.

- [Upgrade firmware on H410C and H300E/H500E/H700E nodes](#)
- [Upgrade firmware on H610C/H615C nodes](#)



## Upgrade firmware on H410C and H300E/H500E/H700E nodes

If your node is part of a cluster, you must place the node in maintenance mode before the upgrade, and take it out of maintenance mode after the upgrade.



Ignore the following informational message you see during the process: **Untrusty Debug Firmware Key is used, SecureFlash is currently in Debug Mode**

### Steps

1. If your node is part of a cluster, place it in maintenance mode as follows. If not, skip to step 2.
  - a. Log in to the VMware vCenter web client.
  - b. Right-click the host (compute node) name and select **Maintenance Mode > Enter Maintenance Mode**.
  - c. Click **OK**.  
VMs on the host will be migrated to another available host. VM migration can take time depending on the number of VMs that need to be migrated.



Ensure that all the VMs on the host are migrated before you proceed.

2. Navigate to the BMC UI, <https://BMCIP/#login>, where BMCIP is the IP address of the BMC.
3. Log in using your credentials.
4. Select **Remote Control > Console Redirection**.
5. Click **Launch Console**.



You might have to install Java or update it.

6. When the console opens, click **Virtual Media > Virtual Storage**.
7. On the **Virtual Storage** screen, click **Logical Drive Type**, and select **ISO File**.



8. Click **Open Image** to browse to the folder where you downloaded the ISO file, and select the ISO file.
9. Click **Plug In**.
10. When the connection status shows **Device#: VM Plug-in OK!!**, click **OK**.
11. Reboot the node by pressing **F12** and clicking **Restart** or clicking **Power Control > Set Power Reset**.
12. During reboot, press **F11** to select the boot options and load the ISO. You might have to press F11 a few times before the boot menu is displayed.

You will see the following screen:

```
ISOLINUX 6.04 6.04-pre1 ETCD Copyright (C) 1994-2015 H.
Enter Linux Installation LiveCD

Enter to boot: F1 for kernels  F2 for options.
Booting enber
boot:
```

13. On the above screen, press **Enter**. Depending on your network, it might take a few minutes after you press **Enter** for the upgrade to begin.



NOTE: Some of the firmware upgrades might cause the console to disconnect and/or cause your session on the BMC to disconnect. You can log back into the BMC, however some services, such as the console, may not be available due to the firmware upgrades. After the upgrades have completed, the node will perform a cold reboot, which can take approximately five minutes.

14. Log back in to the BMC UI and click **System** to verify the BIOS version and build time after booting to the OS. If the upgrade completed correctly, you see the new BIOS and BMC versions.



The BIOS version will not show the upgraded version until the node has finished fully booting.

15. If the node is part of a cluster, complete the steps below. If it is a standalone node, no further action is needed.
  - a. Log in to the VMware vCenter web client.
  - b. Take the host out of maintenance mode. This might show a disconnected red flag. Wait until all statuses are cleared.
  - c. Power on any of the remaining VMs that were powered off.

## Upgrade firmware on H610C/H615C nodes

The steps vary depending on whether the node is standalone or part of a cluster. The procedure can take approximately 25 minutes and includes powering the node off, uploading the ISO, flashing the devices, and powering the node back on after the upgrade.

### Steps

1. If your node is part of a cluster, place it in maintenance mode as follows. If not, skip to step 2.
  - a. Log in to the VMware vCenter web client.
  - b. Right-click the host (compute node) name and select **Maintenance Mode > Enter Maintenance Mode**.
  - c. Click **OK**.

VMs on the host will be migrated to another available host. VM migration can take time depending on the number of VMs that need to be migrated.



Ensure that all the VMs on the host are migrated before you proceed.

2. Navigate to the BMC UI, <https://BMCIP/#login>, where BMC IP is the IP address of the BMC.
3. Log in using your credentials.
4. Click **Remote Control > Launch KVM (Java)**.
5. In the console window, click **Media > Virtual Media Wizard**.



6. Click **Browse** and select the compute firmware **.iso** file.

7. Click **Connect**.

A popup indicating success is displayed, along with the path and device showing at the bottom. You can close the **Virtual Media** window.



8. Reboot the node by pressing **F12** and clicking **Restart** or clicking **Power Control > Set Power Reset**.

9. During reboot, press **F11** to select the boot options and load the ISO.

10. Select **AMI Virtual CDROM** from the list displayed and click **Enter**. If you do not see AMI Virtual CDROM in the list, go into the BIOS and enable it in the boot list. The node will reboot after you save. During the reboot, press **F11**.



11. On the screen displayed, click **Enter**.



Some of the firmware upgrades might cause the console to disconnect and/or cause your session on the BMC to disconnect. You can log back into the BMC, however some services, such as the console, might not be available due to the firmware upgrades. After the upgrades have completed, the node will perform a cold reboot, which can take approximately five minutes.

12. If you get disconnected from the console, select **Remote Control** and click **Launch KVM** or **Launch KVM (Java)** to reconnect and verify when the node has finished booting back up. You might need multiple reconnects to verify that the node booted successfully.



During the powering on process, for approximately five minutes, the KVM console displays **No Signal**.

13. After the node is powered on, select **Dashboard > Device Information > More info** to verify the BIOS and BMC versions. The upgraded BIOS and BMC versions are displayed. The upgraded version of the BIOS will not be displayed until the node has fully booted up.
14. If you placed the node in maintenance mode, after the node boots to ESXi, right-click the host (compute node) name, and select **Maintenance Mode > Exit Maintenance Mode**, and migrate the VMs back to the host.
15. In vCenter, with the host name selected, configure and verify the BIOS version.

## Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [NetApp HCI Resources Page](#)

## Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.