



Upgrade your NetApp HCI or SolidFire system

HCI

NetApp
May 20, 2020

This PDF was generated from https://docs.netapp.com/us-en/hci/docs/concept_hci_upgrade_overview.html on May 20, 2020. Always check docs.netapp.com for the latest.



Table of Contents

- Upgrade your NetApp HCI or SolidFire system 1
 - Upgrades overview 1
 - Upgrade sequences 1
 - System upgrade procedures..... 4
 - vSphere upgrade sequences with vCenter Plug-in..... 47

Upgrade your NetApp HCI or SolidFire system

Upgrades overview

The content in this section introduces recommended upgrade sequences for components in a NetApp HCI system or SolidFire all-flash storage system.

System upgrade sequences content describes the tasks that are needed to complete a NetApp HCI system or SolidFire all-flash storage system upgrade. Ideally these procedures are performed as part of the larger upgrade sequence and not in isolation. If a component-based upgrade or update is needed, see the procedure prerequisites to ensure additional complexities are addressed.

vSphere upgrade sequences including Element Plug-in for vCenter Server content describes additional pre- and post-upgrade steps required to re-install the Element Plug-in for vCenter Server.

System upgrade sequences

Choose one of the following sequences based on your system:

- [Upgrade your NetApp HCI installation for version 1.8.](#)
- [Upgrade your NetApp SolidFire all-flash storage system for Element 12.0.](#)

vSphere upgrade sequences including Element Plug-in for vCenter Server

Choose one of the following sequences based on your system:

- [Upgrade your vSphere components for a NetApp HCI system with the Element Plug-in for vCenter Server.](#)
- [Upgrade your vSphere components for a NetApp SolidFire storage system with the Element Plug-in for vCenter Server.](#)

Find more information

- [NetApp HCI Documentation Center](#)
- [SolidFire and Element Documentation Center](#)

Upgrade sequences

Upgrade your NetApp HCI system for version 1.8

You can keep your NetApp HCI system up-to-date after deployment by sequentially upgrading all NetApp HCI software components.

These components include management services, HealthTools, NetApp Hybrid Cloud Control (HCC), Element software, management node, compute firmware, compute drivers, and the Element Plug-in for vCenter Server.

What you'll need

- You are running management node 11.3 or later. Newer versions of the management node have a modular architecture that provides individual services.



To check the version, log in to your management node and view the Element version number in the login banner. If you do not have 11.3, see [Upgrade your management node](#).

- You have upgraded your management services to at least version 2.1.326.

Upgrades using HCC are not available in earlier service bundle versions.

- You have ensured that the system time on all nodes is synced and that NTP is correctly configured for the storage cluster and nodes. Each node must be configured with a DNS nameserver in the per-node web UI ([https://\[IP address\]:442](https://[IP address]:442)) with no unresolved cluster faults related to time skew.

Steps

1. [Update management services from Hybrid Cloud Control](#).



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.

2. [Upgrade to the latest HealthTools](#).
3. [Run Element storage health checks prior to upgrading storage](#).
4. [Upgrade your Element software version](#).
5. [Upgrade your management node](#).
6. [Upgrade your Element Plug-in for vCenter Server](#).
7. [Run compute node health checks prior to upgrading compute firmware](#).
8. [Update your compute node firmware](#).
9. [Update your compute node drivers](#).

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Upgrade your NetApp SolidFire all-flash storage system for Element 12.0

You can keep your SolidFire Element storage system up-to-date after deployment by sequentially upgrading all NetApp storage components.

These components include management services, HealthTools, NetApp Hybrid Cloud Control (HCC), Element software, management node, and (depending on your installation) the Element Plug-in for vCenter Server.

What you'll need

- You are running management node 11.3 or later. Newer versions of the management node have a modular architecture that provides individual services.



To check the version, log in to your management node and view the Element version number in the login banner. If you do not have 11.3, see [Upgrade your management node](#).

- You have upgraded your management services to at least version 2.1.326.

Upgrades using HCC are not available in earlier service bundle versions.

- You have ensured that the system time on all nodes is synced and that NTP is correctly configured for the storage cluster and nodes. Each node must be configured with a DNS nameserver in the per-node web UI ([https://\[IP address\]:442](https://[IP address]:442)) with no unresolved cluster faults related to time skew.

Steps

1. [Update management services from Hybrid Cloud Control](#).



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.

2. [Upgrade to the latest HealthTools](#).
3. [Run Element storage health checks prior to upgrading storage](#).
4. [Upgrade your Element software version](#).
5. [Upgrade your management node](#).
6. [Upgrade your Element Plug-in for vCenter Server to version 4.4](#).

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

System upgrade procedures

Update management services

You can update your management services to the latest bundle version after you have installed management node 11.3 or later.

Beginning with the Element 11.3 management node release, the management node design has been changed based on a new modular architecture that provides individual services. These modular services provide central and extended management functionality for NetApp HCI and SolidFire all-flash storage systems. Management services include system telemetry, logging, and update services, the QoSSIOC service for Element Plug-in for vCenter Server, NetApp Hybrid Cloud Control (HCC), and more.

You can update management services using the NetApp Hybrid Cloud Control (HCC) UI or the management node REST API:

- [Update management services using Hybrid Cloud Control](#) (Preferred method)
- [Update management services using the management node API](#)
- [Update management services using the management node API for dark sites](#)



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.



(Required for any user who has updated to 2.10.27) Due to an upgrade API issue introduced in 2.10.27, management services cannot be upgraded from that version unless you use the workaround described in [these](#) release notes. You must upgrade to 2.10.29 or a later version using this workaround to resolve the issue and restore management services update capabilities.



For the latest management services release notes describing major services, new features, bug fixes, and workarounds for each service bundle, see [NetApp KB 1087586: Management Services Release Notes](#)

Update management services using Hybrid Cloud Control

You can update your NetApp management services using NetApp Hybrid Cloud Control (HCC).

Management service bundles provide enhanced functionality and fixes to your installation outside of major releases.

Before you begin

- You must be running management node 11.3 or later.

- You must have upgraded your management services to at least version 2.1.326. NetApp Hybrid Cloud Control upgrades are not available in earlier service bundles.



For a list of available services for each service bundle version, see the [Management Services Release Notes](#).

Steps

1. Open a web browser and browse to the IP address of the management node: `<a href="https://<ManagementNodeIP>" class="bare">https://<ManagementNodeIP>;</code>`
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 the **Management Services** tab.

The Management Services tab shows the current and available versions of management services software.



If your installation cannot access the internet, only the current software version is shown.

5. If your installation can access the internet and if a management services upgrade is available, click **Begin Upgrade**.
6. If your installation cannot access the internet, do the following:
 - a. Follow the instructions on the page to download and save a management services upgrade package to your computer.
 - b. Click **Browse** to locate the package you saved and upload it.

After the upgrade begins, you can see the upgrade status on this page.

Update management services using the management node API

Users should ideally perform management services updates from NetApp Hybrid Cloud Control. You can however manually update management services using the REST API UI from the management node.

Before you begin

- You have internet access.
- You have deployed a NetApp Element software management node 11.3 or later.
- Your cluster version is running NetApp Element software 11.3 or later.

Steps

1. Open the REST API UI on the management node: [https://\[management node IP\]/mnode](https://[management node IP]/mnode)

2. Click **Authorize** and complete the following:
 - a. Enter the cluster user name and password.
 - b. Enter the client ID as `mnode-client` if the value is not already populated.
 - c. Copy the token URL string and paste it into another browser tab to initiate a token request.
 - d. Click **Authorize** to begin a session.
 - e. Close the window.
3. (Optional) Confirm available versions of management node services: `GET /services/versions`
4. (Optional) Get detailed information about the latest version: `GET /services/versions/latest`
5. (Optional) Get detailed information about a specific version: `GET /services/versions/{version}/info`
6. Perform one of the following management services update options:
 - a. Run this command to update to the most recent version of management node services: `PUT /services/update/latest`
 - b. Run this command to update to a specific version of management node services: `PUT /services/update/{version}`
7. Run `GET/services/update/status` to monitor the status of the update.

A successful update returns a result similar to the following example:

```
{
  "current_version": "2.10.27",
  "details": "Updated to version 2.10.27",
  "status": "success"
}
```

Update management services using the management node API for dark sites

Users should ideally perform management services updates from NetApp Hybrid Cloud Control. You can however manually upload, extract, and deploy a service bundle update for management services to the management node using the REST API. You can run each command from the REST API UI for the management node.

Before you begin

- You have deployed a NetApp Element software management node 11.3 or later.
- Your cluster version is running NetApp Element software 11.3 or later.
- You have downloaded the service bundle update from the [NetApp Support Site](#) to a device that can be used in the dark site.

Steps

1. Open the REST API UI on the management node: `https://[management node IP]/mnode`

2. Click **Authorize** and complete the following:
 - a. Enter the cluster user name and password.
 - b. Enter the client ID as `mnode-client` if the value is not already populated.
 - c. Copy the token URL string and paste it into another browser tab to initiate a token request.
 - d. Click **Authorize** to begin a session.
 - e. Close the window.
3. Upload and extract the service bundle on the management node using this command: `PUT /services/upload`
4. Deploy the management services on the management node: `PUT /services/deploy`
5. Monitor the status of the update: `GET /services/update/status`

A successful update returns a result similar to the following example:

```
{
  "current_version": "2.10.27",
  "details": "Updated to version 2.10.27",
  "status": "success"
}
```

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Upgrade to the latest HealthTools

Before you begin the Element storage upgrade, you should upgrade your HealthTools suite.

What you'll need

- You are running management node 11.0, 11.1 or later.
- You have upgraded your management services to at least version 2.1.326.

NetApp Hybrid Cloud Control upgrades are not available in earlier service bundle versions.

- You have downloaded the latest version of [HealthTools](#) and copied the installation file to the management node.



You can check the locally installed version of HealthTools by running the `sfupdate-healthtools -v` command.

- To use HealthTools with dark sites, you need to do these additional steps:
 - Download a [JSON file](#) from the NetApp Support Site on a computer that is not the management node and rename it to `metadata.json`.
 - Have the management node up and running at the dark site.

About this task

The commands in the HealthTools suite require escalated privileges to run. Either preface commands with `sudo` or escalate your user to root privileges.



The HealthTools version you use might be more up to date than the sample input and response below.

Steps

1. Run the `sfupdate-healthtools <path to install file>` command to install the new HealthTools software.

Sample input:

```
sfupdate-healthtools /tmp/solidfire-healthtools-2020.03.01.09.tgz
```

Sample response:

```
Checking key signature for file /tmp/solidfirehealthtools-2020.03.01.09/components.tgz
installing command sfupdate-healthtools
Restarting on version 2020.03.01.09
sfupdate-healthtools /sf/bin/sfupdate-healthtools -r 2020.03.01.09
installing command sfupgradecheck
installing command sfinstall
installing command sfresetupgrade
```

2. Run the `sfupdate-healthtools -v` command to verify the installed version has been upgraded.

Sample response:

```
Currently installed version of HealthTools:
2020.03.01.09
```

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Run Element storage health checks prior to upgrading storage

You must run health checks prior to upgrading Element storage to ensure all storage nodes in your cluster are ready for the next Element storage upgrade.

You can run health checks using NetApp Hybrid Cloud Control (HCC) UI, HCC API, or the HealthTools suite:

- [Use NetApp Hybrid Cloud Control to run Element storage health checks prior to upgrading storage](#) (Preferred method)
- [Use API to run Element storage health checks prior to upgrading storage](#)
- [Use HealthTools to run Element storage health checks prior to upgrading storage](#)

You can also find out more about storage health checks that are run by the service:

- [Storage health checks made by the service](#)

What you'll need

- You have updated to the latest management services bundle (2.10.27 or later).



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.

- You are running management node 11.3 or later.
- Your cluster version is running NetApp Element software 11.3 or later.


Use NetApp Hybrid Cloud Control to run Element storage health checks prior to upgrading storage

Using NetApp Hybrid Cloud Control (HCC), you can verify that a storage cluster is ready to be upgraded.

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 the **Storage** tab.
5. Click the health check  for the cluster you want to check for upgrade readiness.

6. On the **Storage Health Check** page, click **Run Health Check**.
7. If there are issues, do the following:
 - a. Go to the specific KB article listed for each issue or perform the specified remedy.
 - b. If a KB is specified, complete the process described in the relevant KB article.
 - c. After you have resolved cluster issues, click **Re-Run Health Check**.

After the health check completes without errors, the storage cluster is ready to upgrade. See [storage node upgrade instructions](#) to proceed.

Use API to run Element storage health checks prior to upgrading storage

You can use REST API to verify that a storage cluster is ready to be upgraded. The health check verifies that there are no obstacles to upgrading, such as pending nodes, disk space issues, and cluster faults.

Steps

1. Locate the storage cluster ID:
 - a. Open the management node REST API UI on the management node:

https://[management node IP]/mnode

- b. Click **Authorize** and complete the following:
 - i. Enter the cluster user name and password.
 - ii. Enter the client ID as `mnode-client` if the value is not already populated.
 - iii. Click **Authorize** to begin a session.
 - c. From the REST API UI, click **GET /assets/storage-clusters**.
 - d. Click **Try it out**.
 - e. Click **Execute**.
 - f. From the response, copy the storage cluster ID ("`id`") of the cluster you intend to check for upgrade readiness.
2. Run health checks on the storage cluster:
- a. Open the storage REST API UI on the management node:

https://[management node IP]/storage/1

- b. Click **Authorize** and complete the following:
 - i. Enter the cluster user name and password.
 - ii. Enter the client ID as `mnode-client` if the value is not already populated.

- iii. Click **Authorize** to begin a session.
- c. Click **POST /health-checks**.
- d. Click **Try it out**.
- e. Enter the storage cluster ID in the parameter field.
- f. Click **Execute** to run a health check on the specified storage cluster.

The response should indicate state as **initializing**:

```
{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccbb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccbb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccbb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}
```

- g. Copy the **healthCheckId** that is part of response.
3. Verify the results of the health checks:
- a. Click **GET /health-checks/healthCheckId**.
 - b. Click **Try it out**.
 - c. Enter the health check ID in the parameter field.
 - d. Click **Execute**.
 - e. Scroll to the bottom of the response body.
4. If the **message** return indicates that there were problems regarding cluster health, do the following:
- a. Go to the specific KB article listed for each issue or perform the specified remedy.
 - b. If a KB is specified, complete the process described in the relevant KB article.
 - c. After you have resolved cluster issues, run **GET /health-checks/healthCheckId** again.

If all health checks are successful, the return is similar to the following example:

```
"message": "All checks completed successfully.",  
"percent": 100,  
"timestamp": "2020-03-06T00:03:16.321621Z"
```

Use HealthTools to run Element storage health checks prior to upgrading storage

You can verify that the storage cluster is ready to be upgraded by using the `sfupgradecheck` command. This command verifies information such as pending nodes, disk space, and cluster faults.

If your management node is at a dark site, the upgrade readiness check needs the `metadata.json` file you downloaded during [HealthTools upgrades](#) to run successfully.

About this task

This procedure describes how to address upgrade checks that yield one of the following results:

- Running the `sfupgradecheck` command runs successfully. Your cluster is upgrade ready.
- Checks within the `sfupgradecheck` tool fail with an error message. Your cluster is not upgrade ready and additional steps are required.
- Your upgrade check fails with an error message that HealthTools is out-of-date.
- Your upgrade check fails because your management node is on a dark site.

Steps

1. Run the `sfupgradecheck` command:

```
sfupgradecheck -u <cluster-user-name> MVIP
```



For passwords that contain special characters, add a backslash (\) before each special character. For example, `mypass!@1` should be entered as `mypass\\!@.`

Sample input command with sample output in which no errors appear and you are ready to upgrade:

```
sfupgradecheck -u admin 10.117.78.244
```

```
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A00000008lt0QQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of available disk
space
Passed node IDs: 1, 2, 3
More information: https://kb.netapp.com/support/s/article/ka11A00000008ltTQAQ/
SolidFire-Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A00000008ltYQAQ/mNodeconnectivity
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and the
management node
Node ID: 1 Upload speed: 90063.90 KBs/sec
Node ID: 3 Upload speed: 106511.44 KBs/sec
Node ID: 2 Upload speed: 85038.75 KBs/sec
```

2. If there are errors, additional actions are required. See the following sub-sections for details.

Your cluster is not upgrade ready

If you see an error message related to one of the health checks, follow these steps:

1. Review the **sfupgradecheck** error message.

Sample response:

The following tests failed:

check_root_disk_space:

Test Description: Verify node root directory has at least 12 GBs of available disk space

Severity: ERROR

Failed node IDs: 2

Remedy: Remove unneeded files from root drive

More information: <https://kb.netapp.com/support/s/article/ka11A000000081tTQAQ/SolidFire-Disk-space-error>

check_pending_nodes:

Test Description: Verify no pending nodes in cluster

More information: <https://kb.netapp.com/support/s/article/ka11A000000081tOQAQ/pendingnodes>

check_cluster_faults:

Test Description: Report any cluster faults

check_root_disk_space:

Test Description: Verify node root directory has at least 12 GBs of available disk space

Passed node IDs: 1, 3

More information: <https://kb.netapp.com/support/s/article/ka11A000000081tTQAQ/SolidFire-Disk-space-error>

check_mnode_connectivity:

Test Description: Verify storage nodes can communicate with management node

Passed node IDs: 1, 2, 3

More information:

<https://kb.netapp.com/support/s/article/ka11A000000081tYQAQ/mNodeconnectivity>

check_files:

Test Description: Verify options file exists

Passed node IDs: 1, 2, 3

check_cores:

Test Description: Verify no core or dump files exists

Passed node IDs: 1, 2, 3

check_upload_speed:

Test Description: Measure the upload speed between the storage node and the management node

Node ID: 1 Upload speed: 86518.82 KBs/sec

Node ID: 3 Upload speed: 84112.79 KBs/sec

Node ID: 2 Upload speed: 93498.94 KBs/sec

In this example, node 1 is low on disk space. You can find more information in the [knowledge base \(KB\)](#) article listed in the error message.

HealthTools is out of date

If you see an error message indicating that HealthTools is not the latest version, follow these instructions:

1. Review the error message and note that the upgrade check fails.

Sample response:


```
sfupgradecheck failed: HealthTools is out of date:
installed version: 2018.02.01.200
latest version: 2020.03.01.09.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/
Or rerun with the -n option
```

2. Follow the instructions described in the response.

Your management node is on a dark site

1. Review the message and note that the upgrade check fails:

Sample response:

```
sfupgradecheck failed: Unable to verify latest available version of healthtools.
```

2. Download a [JSON file](#) from the NetApp Support Site on a computer that is not the management node and rename it to `metadata.json`.
3. Run the following command:

```
sfupgradecheck -l --metadata=<path-to-metadata-json>
```

4. For details, see additional [HealthTools upgrades](#) information for dark sites.
5. Verify that the HealthTools suite is up-to-date by running the following command:

```
sfupgradecheck -u <cluster-user-name> -p <cluster-password> MVIP
```

Storage health checks made by the service

Storage health checks make the following checks per cluster.

| Check Name | Node/Cluster | Description |
|----------------------|--------------|---|
| check_async_results | Cluster | Verifies that the number of asynchronous results in the database is below a threshold number. |
| check_cluster_faults | Cluster | Verifies that there are no upgrade blocking cluster faults (as defined in Element source). |

| Check Name | Node/Cluster | Description |
|--------------------------|--------------|--|
| check_upload_speed | Node | Measures the upload speed between the storage node and the management node. |
| connection_speed_check | Node | Verifies that nodes have connectivity to the management node serving upgrade packages and estimates connection speed. |
| check_cores | Node | Checks for kernel crash dump and core files on the node. The check fails for any crashes in a recent time period (threshold 7 days). |
| check_root_disk_space | Node | Verifies the root file system has sufficient free space to perform an upgrade. |
| check_var_log_disk_space | Node | Verifies that <code>/var/log</code> free space meets some percentage free threshold. If it does not, the check will rotate and purge older logs in order to fall under threshold. The check fails if it is unsuccessful at creating sufficient free space. |
| check_pending_nodes | Cluster | Verifies that there are no pending nodes on the cluster. |

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Upgrade Element software

To upgrade to NetApp Element software 12.0, you must use the `sfinstall` file included in the HealthTools suite of tools. Certain operations are suppressed during an Element software upgrade, such as adding and removing nodes, adding and removing drives, and commands associated with initiators, volume access groups, and virtual networks, among others.

Choose one of the following Element software upgrade options that use HealthTools for the procedure:

- [Upgrade Element software at connected sites](#)
- [Upgrade Element software at dark sites](#)



If you are upgrading an H610S series node to Element 12.0 or later, you will need to upgrade Element software (phase 1) and then perform additional upgrade steps (phase 2) for each storage node. See [Upgrading H610S storage nodes to Element 12.0 or later \(phase 2\)](#) after you complete the `sfinstall` procedure with HealthTools.

What you'll need

- You have updated your management services bundle to the latest version.



You must upgrade to the latest management services bundle before upgrading your Element software to version 12.

- You have checked upgrade path information for the Element version you are upgrading to and verified that the upgrade path is valid.

[NetApp KB 1088254: Upgrade matrix for storage clusters running NetApp Element Software](#)

- You have the latest version of HealthTools.
- You have verified that the cluster is ready to be upgraded. See [Run Element storage health checks prior to upgrading storage](#).
- You have ensured that the system time on all nodes is synced and that NTP is correctly configured for the storage cluster and nodes. Each node must be configured with a DNS nameserver in the per-node web UI ([https://\[IP address\]:442](https://[IP address]:442)) with no unresolved cluster faults related to time skew.
- The management node in your environment is running version 11.0, 11.1 or later.

Upgrade Element software at connected sites

Steps

1. For NetApp HCI systems, go to the NetApp HCI software [download page](#). For SolidFire storage systems, go to the Element software [download page](#).
2. Select the correct software release and download the latest storage node image to a computer that is not the management node.
3. Copy the ISO file to the management node in an accessible location like `/tmp`.



You can do this by using, for example, SCP.

When you upload the ISO file, make sure that the name of the file does not change, otherwise later steps will fail.

4. **Optional:** Download the ISO from the management node to the cluster nodes before the upgrade.

This step reduces the upgrade time by pre-staging the ISO on the storage nodes and running

additional internal checks to ensure that the cluster is in a good state to be upgraded. Performing this operation will not put the cluster into "upgrade" mode or restrict any of the cluster operations.

```
sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO> --stage
```



Omit the password from the command line to allow **sfinstall** to prompt for the information. For passwords that contain special characters, add a backslash (\) before each special character. For example, **mypass!@1** should be entered as **mypass\!\@.**

Example

See the following sample input:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfisodium-11.0.0.345.iso --stage
```

The output for the sample shows that **sfinstall** attempts to verify if a newer version of **sfinstall** is available:

```
sfinstall 10.117.0.244 -u admin
/tmp/solidfire-rtfisodium-11.0.0.345.iso 2018-10-01 16:52:15:
Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/
or rerun with --skip-version-check
```

See the following sample excerpt from a successful pre-stage operation:



When staging completes, the message will display **Storage Node Upgrade Staging Successful** after the upgrade event.

```
flabv0004 ~ # sfinstall -u admin
10.117.0.87 solidfire-rtfi-sodium-patch3-11.3.0.14171.iso --stage
2019-04-03 13:19:58: sfinstall Release Version: 2019.01.01.49 Management Node
Platform:
Ember Revision: 26b042c3e15a Build date: 2019-03-12 18:45
2019-04-03 13:19:58: Checking connectivity to MVIP 10.117.0.87
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.86
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.87
...
2019-04-03 13:19:58: Successfully connected to cluster and all nodes
...
2019-04-03 13:20:00: Do you want to continue? ['Yes', 'No']: Yes
...
2019-04-03 13:20:55: Staging install pack on cluster nodes
2019-04-03 13:20:55: newVersion: 11.3.0.14171
2019-04-03 13:21:01: nodeToStage: nlabp2814, nlabp2815, nlabp2816, nlabp2813
2019-04-03 13:21:02: Staging Node nlabp2815 mip=[10.117.0.87] nodeID=[2] (1 of 4
nodes)
2019-04-03 13:21:02: Node Upgrade serving image at
http://10.117.0.204/rtfi/solidfire-rtfisodium-
patch3-11.3.0.14171/filesystem.squashfs
...
2019-04-03 13:25:40: Staging finished. Repeat the upgrade command without the --stage
option to start the upgrade.
```

The staged ISOs will be automatically deleted after the upgrade completes. However, if the upgrade has not started and needs to be rescheduled, ISOs can be manually de-staged using the command:

```
sfinstall <MVIP> -u <cluster_username> --destage
```

After the upgrade has started, the de-stage option is no longer available.

5. Start the upgrade with the `sfinstall` command and the path to the ISO file:

```
sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO>
```

Example

See the following sample input command:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-11.0.0.345.iso
```

The output for the sample shows that `sfinstall` attempts to verify if a newer version of `sfinstall` is available:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-11.0.0.345.iso
2018-10-01 16:52:15: Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/ or rerun with --skip-version-check
```

See the following sample excerpt from a successful upgrade. Upgrade events can be used to monitor the progress of the upgrade.

```
# sfinstall 10.117.0.161 -u admin solidfire-rtfi-sodium-11.0.0.761.iso
2018-10-11 18:28
Checking connectivity to MVIP 10.117.0.161
Checking connectivity to node 10.117.0.23
Checking connectivity to node 10.117.0.24
...
Successfully connected to cluster and all nodes
#####
You are about to start a new upgrade
10.117.0.161
10.3.0.161
solidfire-rtfi-sodium-11.0.0.761.iso
Nodes:
10.117.0.23 nlabp1023 SF3010 10.3.0.161
10.117.0.24 nlabp1025 SF3010 10.3.0.161
10.117.0.26 nlabp1027 SF3010 10.3.0.161
10.117.0.28 nlabp1028 SF3010 10.3.0.161
#####
Do you want to continue? ['Yes', 'No']: yes
...
Watching for new network faults. Existing fault IDs are set([]).
Checking for legacy network interface names that need renaming
Upgrading from 10.3.0.161 to 11.0.0.761 upgrade method=rtfi
Waiting 300 seconds for cluster faults to clear
Waiting for caches to fall below threshold
...
Installing mip=[10.117.0.23] nodeID=[1] (1 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[7] away from mip[10.117.0.23] nodeID[1] ssid[11] to new ssid[15]
Moving primary slice=[12] away from mip[10.117.0.23] nodeID[1] ssid[11] to new
ssid[15]
...
Installing mip=[10.117.114.24] nodeID=[2] (2 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[5] away from mip[10.117.114.24] nodeID[2] ssid[7] to new
ssid[11]
...
Install of solidfire-rtfi-sodium-11.0.0.761 complete.
Removing old software
No staged builds present on nodeID=[1]
No staged builds present on nodeID=[2]
...
Starting light cluster block service check
```



If you are upgrading an H610S series node to Element 12.0 or later, you will need to perform additional upgrade steps (phase 2) for each storage node. See [Upgrading H610S storage nodes to Element 12.0 or later \(phase 2\)](#).

Upgrade Element software at dark sites

You must use the HealthTools suite of tools to update NetApp Element software at a dark site.

What you'll need

1. For NetApp HCI systems, go to the NetApp HCI software [download page](#). For SolidFire storage systems, go to the Element software [download page](#).
2. Select the correct software release and download the latest storage node image to a computer that is not the management node.
3. Download this [JSON file](#) (https://library.netapp.com/ecm/ecm_get_file/ECMLP2840740) from the NetApp Support Site on a computer that is not the management node and rename it to `metadata.json`.
4. Copy the ISO file to the management node in an accessible location like `/tmp`.



You can do this by using, for example, SCP. When you upload the ISO file, make sure that the name of the file does not change, otherwise later steps will fail.

Steps

1. Run the `sfupdate-healthtools` command:

```
sfupdate-healthtools <path-to-healthtools-package>
```

2. Check the installed version:

```
sfupdate-healthtools -v
```

3. Check the latest version against the metadata JSON file:

```
sfupdate-healthtools -l --metadata=<path-to-metadata-json>
```

4. Ensure that the cluster is ready:

```
sudo sfupgradecheck -u <cluster_username> -p <cluster_password> MVIP --metadata=<path-to-metadata-json>
```


5. Run the **sfinstall** command with the path to the ISO file and the metadata JSON file:

```
sfinstall -u <cluster_username> <MVIP> <path-toinstall-file-ISO> --metadata=<path-to  
-metadata-json-file>
```

See the following sample input command:

```
sfinstall -u admin 10.117.78.244 /tmp/solidfire-rtfi-11.3.0.345.iso  
--metadata=/tmp/metadata.json
```

Optional You can add the **--stage** flag to the **sfinstall** command to pre-stage the upgrade in advance.



If you are upgrading an H610S series node to Element 12.0 or later, you will need to perform additional upgrade steps (phase 2) for each storage node. See [Upgrading H610S storage nodes to Element 12.0 or later \(phase 2\)](#).

What happens if an upgrade fails

If the software upgrade fails, you can pause the upgrade.



You should pause an upgrade only with Ctrl-C. This enables the system to clean itself up.

When **sfinstall** waits for cluster faults to clear and if any failure causes the faults to remain, **sfinstall** will not proceed to the next node.

Steps

1. You should stop **sfinstall** with Ctrl+C.
2. Contact NetApp Support to assist with the failure investigation.
3. Resume the upgrade with the same **sfinstall** command.
4. When an upgrade is paused by using Ctrl+C, if the upgrade is currently upgrading a node, choose one of these options:
 - **Wait:** Allow the currently upgrading node to finish before resetting the cluster constants.
 - **Continue:** Continue the upgrade, which cancels the pause.
 - **Abort:** Reset the cluster constants and abort the upgrade immediately.



Aborting the cluster upgrade while a node is being updated might result in the drives being ungracefully removed from the node. If the drives are ungracefully removed, adding the drives back during an upgrade will require manual intervention by NetApp Support. The node might be taking longer to do firmware updates or post update syncing activities. If the upgrade progress seems stalled, contact NetApp Support for assistance.

Upgrading H610S storage nodes to Element 12.0 or later (phase 2)

If you are upgrading an H610S series node to Element 12.0 or later, the upgrade process involves two phases.

Phase 1, which is performed first, follows the same steps as the standard upgrade to Element 12.0 process. It installs Element Software and all 5 firmware updates in a rolling fashion across the cluster one node at a time. Due to the firmware payload, the process is estimated to take approximately 1.5 to 2 hours per H610S node, including a single cold-boot cycle at the end of the upgrade for each node.

Phase 2 involves completing steps to perform a complete node shutdown and power disconnect for each H610S node that are described in a required [KB](#). This phase is estimated to take approximately one hour per H610S node.



After you complete phase 1, four of the five firmware updates are activated during the cold boot on each H610S node; however, the Complex Programmable Logic Device (CPLD) firmware requires a complete power disconnect and reconnect to fully install. The CPLD firmware update protects against NVDIMM failures and metadata drive eviction during future reboots or power cycles. This power reset is estimated to take approximately one hour per H610S node. It requires shutting down the node, removing power cables or disconnecting power via a smart PDU, waiting approximately 3 minutes, and reconnecting power.

Before you begin

- You have completed phase 1 of the H610S upgrade process and have upgraded your storage nodes using one the standard Element storage upgrade procedures:
 1. [Upgrade Element software at connected sites](#)
 2. [Upgrade Element software at dark sites](#)



Phase 2 requires on-site personnel.

Steps

1. (Phase 2) Complete the power reset process required for each H610S node in the cluster:



If the cluster also has non-H610S nodes, these non-H610S nodes are exempt from phase 2 and do not need to be shut down or have their power disconnected.

- a. Contact NetApp Support for assistance and to schedule this upgrade.
- b. Follow the phase 2 upgrade procedure in this [KB](#) that is required to complete an upgrade for each H610S node.

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Upgrade a management node

You can upgrade your management node to management node version 12.0 from version 11.0 or later.

Choose one of the following management node upgrade options:

- If you are upgrading from management node 11.3 or later:
[Upgrade a management node to version 12.0 from 11.3 or later](#)
- If you are upgrading from management node 11.0 or 11.1:
[Upgrade a management node to version 12.0 from 11.1 or 11.0](#)
- If you are upgrading from a management node version 10.x:
[Migrating from management node version 10.x to 11.x](#)

Choose this option if you have **sequentially** updated (1) your management services version and (2) your Element storage version and you want to **keep** your existing management node:

- If you are keeping existing management node:
[Reconfigure authentication using the management node REST API](#)



If you do not sequentially update your management services followed by Element storage, you cannot reconfigure reauthentication using this procedure. Follow the appropriate upgrade procedure instead.

Before you begin

- The vCenter Plug-in 4.4 or later requires a management node 11.3 or later that is created with modular architecture and provides individual services.

Upgrade a management node to version 12.0 from 11.3 or later

You can perform an in-place upgrade of the management node from 11.3 or later to version 12.0 without needing to provision a new management node virtual machine. You can use this procedure if you are upgrading from any of the following management node versions: 11.3, 11.5, 11.7, or 11.8.

Before you begin

- The management node you are intending to upgrade is version 11.3 or later and uses IPv4 networking. The management node version 12.0 does not support IPv6.



To check the version of your management node, log in to your management node and view the Element version number in the login banner.

- You have updated your management services bundle to the latest version using Hybrid Cloud Control (HCC). You can access HCC from the following IP: `<a href="https://<ManagementNodeIP>" class="bare">https://<ManagementNodeIP>`
- You have configured an additional network adapter (if required) using the instructions for configuring a storage NIC (eth1) in the management node user guide your product.



Persistent volumes might require an additional network adapter if eth0 is not able to be routed to the SVIP. Configure a new network adapter on the iSCSI storage network to allow the configuration of persistent volumes.

- Storage nodes are running Element 11.3 or later. Use the latest HealthTools to upgrade Element software.

Steps

1. Log in to the management node virtual machine using SSH or console access.
2. Download the management node ISO for [NetApp HCI](#) or [Element](#) software from the NetApp Support Site to the management node virtual machine.



The name of the ISO is similar to `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Check the integrity of the download by running md5sum on the downloaded file and compare the output to what is available on NetApp Support Site for NetApp HCI or Element software, as in the following example:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

4. Mount the management node ISO image and copy the contents to the file system using the following commands:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. Change to the home directory, and unmount the ISO file from `/mnt`:

```
sudo umount /mnt
```

6. Delete the ISO to conserve space on the management node:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

7. On an 11.3 or later management node, run the following command to upgrade your management node OS version. The script retains all necessary configuration files after the upgrade, such as Active IQ collector and proxy settings.

```
sudo /sf/rftfi/bin/sfrtfti_inplace file:///upgrade/casper/filesystem.squashfs  
sf_upgrade=1
```

The management node reboots with a new OS after the upgrade process completes.

8. On the 11.3 or later management node, run the `redeploy-mnode` script to retain previous management services configuration settings:



The script retains previous management services configuration, including configuration from the Active IQ collector service, controllers (vCenters), or proxy, depending on your settings.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

Upgrade a management node to version 12.0 from 11.1 or 11.0

You can perform an in-place upgrade of the management node from 11.0 or 11.1 to version 12.0 without needing to provision a new management node virtual machine.

Before you begin

- Storage nodes are running Element 11.3 or later.



Use the latest HealthTools to upgrade Element software.

- The management node you are intending to upgrade is version 11.0 or 11.1 and uses IPv4 networking. The management node version 12.0 does not support IPv6.



To check the version of your management node, log in to your management node and view the Element version number in the login banner. For management node 11.0, the VM memory needs to be manually increased to 12GB.

- You have configured an additional network adapter (if required) using the instructions for configuring a storage NIC (eth1) in the management node user guide your product.



Persistent volumes might require an additional network adapter if eth0 is not able to be routed to the SVIP. Configure a new network adapter on the iSCSI storage network to allow the configuration of persistent volumes.

Steps

1. Log in to the management node virtual machine using SSH or console access.
2. Download the management node ISO for [NetApp HCI](#) or [Element](#) software from the NetApp Support Site to the management node virtual machine.



The name of the ISO is similar to `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Check the integrity of the download by running md5sum on the downloaded file and compare the output to what is available on NetApp Support Site for NetApp HCI or Element software, as in the following example:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

4. Mount the management node ISO image and copy the contents to the file system using the following commands:

```
sudo mkdir -p /upgrade
```

```
sudo mount solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. Change to the home directory, and unmount the ISO file from /mnt:

```
sudo umount /mnt
```

6. Delete the ISO to conserve space on the management node:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

7. Run one of the following scripts with options to upgrade your management node OS version. Only run the script that is appropriate for your version. Each script retains all necessary configuration files after the upgrade, such as Active IQ collector and proxy settings.

- a. On an 11.1 (11.1.0.73) management node, run the following command:

```
sudo /sf/rftfi/bin/sftrtfi_inplace file:///upgrade/casper/filesystem.squashfs  
sf_upgrade=1 sf_keep_paths="/sf/packages/solidfire-sioc-4.2.3.2288  
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc /sf/packages/nma"
```

- b. On an 11.1 (11.1.0.72) management node, run the following command:

```
sudo /sf/rftfi/bin/sftrtfi_inplace file:///upgrade/casper/filesystem.squashfs  
sf_upgrade=1 sf_keep_paths="/sf/packages/solidfire-sioc-4.2.1.2281  
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc /sf/packages/nma"
```

- c. On an 11.0 (11.0.0.781) management node, run the following command:

```
sudo /sf/rftfi/bin/sftrtfi_inplace file:///upgrade/casper/filesystem.squashfs  
sf_upgrade=1 sf_keep_paths="/sf/packages/solidfire-sioc-4.2.0.2253  
/sf/packages/solidfire-nma-1.4.8/conf /sf/packages/sioc /sf/packages/nma"
```

The management node reboots with a new OS after the upgrade process completes.

8. On the 12.0 management node, run the **upgrade-mnode** script to retain previous configuration settings.



If you are migrating from an 11.0 or 11.1 management node, the script copies the Active IQ collector to the new configuration format.

- a. For a single storage cluster managed by an existing management node 11.0 or 11.1 with persistent volumes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true - persistent  
volume> -pva <persistent volume account name - storage volume account>
```

- b. For a single storage cluster managed by an existing management node 11.0 or 11.1 with no persistent volumes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
```

- c. For multiple storage clusters managed by an existing management node 11.0 or 11.1 with persistent volumes:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true - persistent volume> -pva <persistent volume account name - storage volume account> -pvm <persistent volumes mvip>
```

- d. For multiple storage clusters managed by an existing management node 11.0 or 11.1 with no persistent volumes (the **-pvm** flag is just to provide one of the cluster's MVIP addresses):

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for persistent volumes>
```

9. (For all NetApp HCI installations and SolidFire stand-alone storage installations with NetApp Element Plug-in for vCenter Server) Update the vCenter Plug-in on the 12.0 management node by following the steps in the [Upgrade the Element Plug-in for vCenter Server to version 4.4](#) topic.

10. Use the management node API to add assets:

- a. From a browser, log into the management node REST API UI:

- i. Go to the storage MVIP and log in.

This action causes certificate to be accepted for the next step.

- ii. Open the REST API UI on the management node:

```
https://[management node IP]/mnode
```

- b. From the management node REST API UI, click **Authorize** or any lock icon and complete the following:

- i. Enter the cluster user name and password.

- ii. Enter the client ID as **mnode-client** if the value is not already populated.

- iii. Copy the token URL string and paste it into another browser tab to initiate a token request.

- iv. Click **Authorize** to begin a session.

- v. Close the window.

- c. Run **GET /assets** to find the base asset ID that you will need for the next steps:

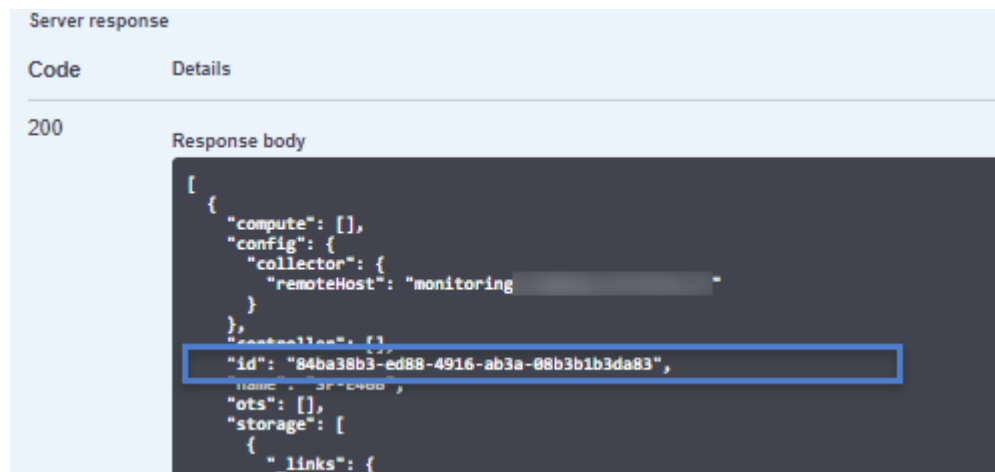
- i. Click **GET /assets**.

- ii. Click **Try it out**.

iii. Click **Execute**.

iv. Copy the value for "**id**" for the base asset to your clipboard:

NOTE: Your installation has a base asset configuration that was created during installation or upgrade.



d. Add a vCenter controller asset for HCI monitoring (NetApp HCI installations only) and Hybrid Cloud Control (for all installations) to the management node known assets:

i. Click **POST /assets/{asset_id}/controllers** to add a controller sub-asset.

ii. Click **Try it out**.

iii. Enter the required payload values as defined in the **Model** tab with type **vCenter** and vCenter credentials.

iv. Enter the parent base asset ID you copied to your clipboard in the **asset_id** field.

v. Click **Execute**.

e. (For NetApp HCI only) Add a compute node asset to the management node known assets:

i. Click **POST/assets/{asset_id}/compute-nodes** to add a compute node sub-asset with credentials for the compute node asset.

ii. Click **Try it out**.

iii. In the payload, enter the required payload values as defined in the **Model** tab. Use type **ESXi Host** and remove the **hardware_tag** parameter.

iv. Enter the parent base asset ID you copied to your clipboard in the **asset_id** field.

v. Click **Execute**.

Migrating from management node version 10.x to 11.x

If you have a management node at version 10.x, you cannot upgrade from 10.x to 11.x. You can instead use this migration procedure to copy over the configuration from 10.x to a newly deployed 11.1 management node. If your management node is currently at 11.0 or higher, you should skip this procedure. You need management node 11.0 or 11.1 and the latest HealthTools to upgrade Element software from 10.3 + through 11.x.

Steps

1. From the VMware vSphere interface, deploy the management node 11.1 OVA and power it on.
2. Open the management node VM console, which brings up the terminal user interface (TUI).
3. Use the TUI to create a new administrator ID and assign a password.
4. In the management node TUI, log in to the management node with the new ID and password and validate that it works.
5. From the vCenter or management node TUI, get the management node 11.1 IP address and browse to the IP address on port 9443 to open the management node UI.

```
https://<mNode 11.1 IP address>:9443
```

6. In vSphere, select **NetApp Element Configuration > mNode Settings**. (In older versions, the top-level menu is **NetApp SolidFire Configuration**.)
7. Click **Actions > Clear**.
8. To confirm, click **Yes**. The mNode Status field should report Not Configured.



When you go to the **mNode Settings** tab for the first time, the mNode Status field might display as **Not Configured** instead of the expected **UP**; you might not be able to choose **Actions > Clear**. Refresh the browser. The mNode Status field will eventually display **UP**.

9. Log out of vSphere.
10. In a web browser, open the management node registration utility and select **QoSSIOC Service Management**:

```
https://<mNode 11.1 IP address>:9443
```

11. Set the new QoSSIOC password.



The default password is **solidfire**. This password is required to set the new password.

12. Click the **vCenter Plug-in Registration** tab.
13. Select **Update Plug-in**.
14. Enter required values. When you are finished, click **UPDATE**.
15. Log in to vSphere and select **NetApp Element Configuration > mNode Settings**.
16. Click **Actions > Configure**.
17. Provide the management node IP address, management node user ID (the user name is **admin**),

password that you set on the **QoSSIIOC Service Management** tab of the registration utility, and vCenter user ID and password.

In vSphere, the **mNode Settings** tab should display the mNode status as **UP**, which indicates management node 11.1 is registered to vCenter.

18. From the management node registration utility (<https://<mNode 11.1 IP address>:9443>), restart the SIOC service from **QoSSIIOC Service Management**.
19. Wait for one minute and check the **NetApp Element Configuration > mNode Settings** tab. This should display the mNode status as **UP**.

If the status is **DOWN**, check the permissions for `/sf/packages/sioc/app.properties`. The file should have read, write, and execute permissions for the file owner. The correct permissions should appear as follows:

```
-rwx-----
```

20. After the SIOC process starts and vCenter displays mNode status as **UP**, check the logs for the `sf-hci-nma` service on the management node. There should be no error messages.
21. (For management node 11.1 only) SSH into the management node version 11.1 with root privileges and start the NMA service with the following commands:

```
# systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
```

```
# systemctl start sf-hci-nma21
```

22. Perform actions from vCenter to remove a drive, add a drive or reboot nodes. This triggers storage alerts, which should be reported in vCenter. If this is working, NMA system alerts are functioning as expected.
23. If ONTAP Select is configured in vCenter, configure ONTAP Select alerts in NMA by copying the `.ots.properties` file from the previous management node to the management node version 11.1 `/sf/packages/nma/conf/.ots.properties` file, and restart the NMA service using the following command:

```
systemctl restart sf-hci-nma
```

24. Verify that ONTAP Select is working by viewing the logs with the following command:

```
journalctl -f | grep -i ots
```

25. Configure Active IQ by doing the following:

- a. SSH in to the management node version 11.1 and go to the `/sf/packages/collector` directory.
- b. Run the following command:

```
sudo ./manage-collector.py --set-username netapp --set-password --set-mvip <MVIP>
```

- c. Enter the management node UI password when prompted.
- d. Run the following commands:

```
./manage-collector.py --get-all
```

```
sudo systemctl restart sfcollector
```

- e. Verify `sfcollector` logs to confirm it is working.

26. In vSphere, the **NetApp Element Configuration** > **mNode Settings** tab should display the mNode status as **UP**.
27. Verify NMA is reporting system alerts and ONTAP Select alerts.
28. If everything is working as expected, shut down and delete management node 10.x VM.

Reconfigure authentication using the management node REST API

You can keep your existing management node if you have sequentially upgraded (1) management services and (2) Element storage. If you have followed a different upgrade order, see the procedures for in-place management node upgrades.

Before you begin

- You have updated your management services to 2.10.29 or later.
- Your storage cluster is running Element 12.0 or later.
- Your management node is 11.3 or later.
- You have sequentially updated your management services followed by upgrading your Element storage. You cannot reconfigure authentication using this procedure unless you have completed upgrades in the sequence described.

Steps

1. Open the management node REST API UI on the management node:

```
https://[management node IP]/mnode
```

2. Click **Authorize** and complete the following:
 - a. Enter the cluster user name and password.
 - b. Enter the client ID as `mnode-client` if the value is not already populated.
 - c. Click **Authorize** to begin a session.
3. From the REST API UI, click **POST /services/reconfigure-auth**.
4. Click **Try it out**.
5. For the `load_images` parameter, select `true`.
6. Click **Execute**.

The response body indicates that reconfiguration was successful.

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Upgrade the Element Plug-in for vCenter Server to version 4.4

For existing vSphere environments with a registered NetApp Element Plug-in for vCenter Server (VCP), you can update your plug-in registration after you first update the management services package that contains the plug-in service.

You can update the plug-in registration on vCenter Server Virtual Appliance (vCSA) or Windows using the registration utility. You must change your registration for the vCenter Plug-in on every vCenter Server where you need to use the plug-in.

This upgrade procedure covers the following upgrade scenarios:

- You are upgrading to a 6.5 or 6.7 HTML5 vSphere Web Client.
- You are upgrading to a 6.5 or 6.7 Flash vSphere Web Client.



The plug-in is not compatible with version 6.7 U2 of the HTML5 vSphere Web Client. It is compatible with the version 6.7 U2 vSphere Web Client for Flash. The plug-in has not yet been tested for use with vSphere 7.0.

Before you begin

- **Admin privileges:** You have vCenter Administrator role privileges to install a plug-in.
- **vSphere upgrades:** You have performed any required vCenter upgrades before upgrading the NetApp Element Plug-in for vCenter Server. This procedure assumes that vCenter upgrades have already been completed.


- **vCenter Server:** Your vCenter Plug-in version 4.x is registered with a vCenter Server. From the registration utility ([https://\[management node IP\]:9443](https://[management node IP]:9443)), click **Registration Status**, complete the necessary fields, and click **Check Status** to verify that the vCenter Plug-in is already registered and the version number of the current installation.
- **Management services updates:** You have updated your [management services bundle](#) to the latest version. Updates to the vCenter plug-in are distributed using management services updates that are released outside of major product releases for NetApp HCI and SolidFire all-flash storage.
- **Management node upgrades:** You are running a management node that has been [upgraded](#) to version 11.3 or later. vCenter Plug-in 4.4 or later requires a an 11.3 or later management node with a modular architecture that provides individual services. Your management node must be powered on with its IP address or DHCP address configured.
- **Element storage upgrades:** You have a cluster running NetApp Element software 11.3 or later.
- **vSphere Web Client:** You have logged out of the vSphere Web Client before beginning any plug-in upgrade. The web client will not recognize updates made during this process to your plug-in if you do not log out.

Steps

1. Enter the IP address for your management node in a browser, including the TCP port for registration:

[https://\[management node IP\]:9443](https://[management node IP]:9443)

The registration utility UI opens to the **Manage QoSSIOC Service Credentials** page for the plug-in.



NetApp Element Plug-in for vCenter Server Management Node


[QoSSIOC Service Management](#)
[vCenter Plug-in Registration](#)

GoSSIOC Management

Manage Credentials


Restart QoSSIOC Service


Manage QoSSIOC Service Credentials



The current QoSSIOC password is set to the default value of 'solidfire'. You should customize credentials to better ensure QoSSIOC service security.

Old Password

New Password 

Confirm Password 

SUBMIT CHANGES

Contact NetApp Support at <http://mysupport.netapp.com>

2. Click **vCenter Plug-in Registration**.

The screenshot shows the 'vCenter Plug-in - Registration' page. On the left, under 'Manage vCenter Plug-in', the 'Register Plug-in' option is selected. The main area contains registration details: 'vCenter Address' (vCenter Server Address), 'vCenter User' (vCenter Admin User Name), 'vCenter Password' (vCenter Admin Password), and 'Plug-in Zip URL' (with a 'Customize URL' checkbox). A 'REGISTER' button is at the bottom. A footer link points to 'http://mysupport.netapp.com'.

3. Within **Manage vCenter Plug-in**, select **Update Plug-in**.

4. Confirm or update the following information:

- The IPv4 address or the FQDN of the vCenter service on which you will register your plug-in.
- The vCenter Administrator user name.



The user name and password credentials you enter must be for a user with vCenter Administrator role privileges.

- The vCenter Administrator password.
- (For in-house servers/dark sites) A custom URL for the plug-in ZIP.



You can click **Custom URL** to customize the URL if you are using an HTTP or HTTPS server (dark site) or have modified the ZIP file name or network settings. For additional configuration steps if you intend to customize a URL, see Element Plug-in for vCenter Server documentation about modifying vCenter properties for an in-house (dark site) HTTP server.

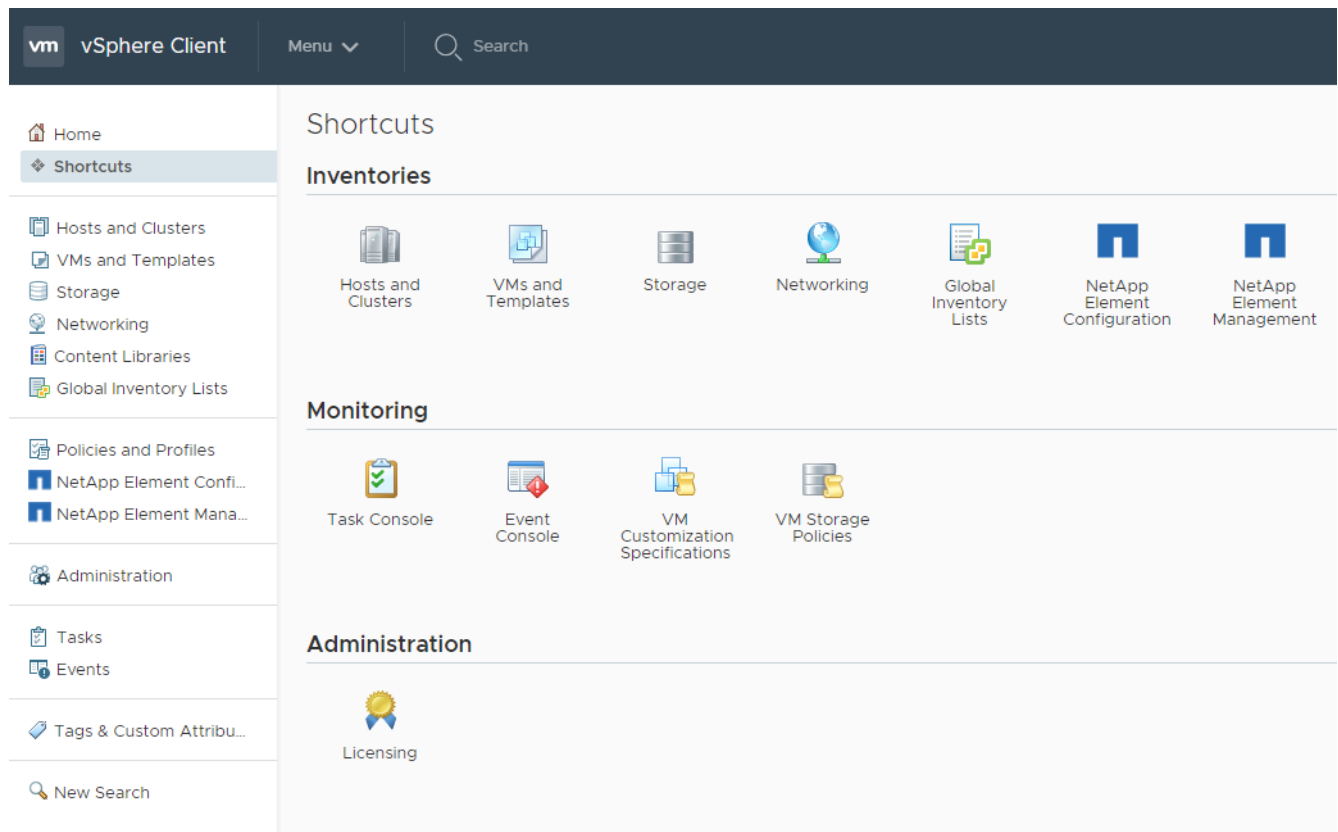
5. Click **Update**.

- Log in to the vSphere Web Client as a vCenter Administrator.



This action creates a new database and completes the installation in the vSphere Web Client. If the vCenter Plug-in icons are not visible from the vSphere main page, see [Element Plug-in for vCenter Server documentation](#) about troubleshooting the plug-in.

- Verify that the NetApp Element Configuration and Management extension points appear in the Shortcuts tab of the vSphere Web Client and in the side panel.



If the vCenter Plug-in icons are not visible, see [Element Plug-in for vCenter Server documentation](#) about troubleshooting the plug-in.

- Verify the version change in the **About** tab in the **NetApp Element Configuration** extension point of the plug-in.

You should see the following version details or details of a more recent version:

NetApp Element Plug-in Version: 4.4.0
NetApp Element Plug-in Build Number: 72



The vCenter Plug-in contains online Help content. To ensure that your Help contains the latest content, clear your browser cache after upgrading your plug-in.

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Run compute node health checks prior to upgrading compute firmware

You must run health checks prior to upgrading compute firmware to ensure all compute nodes in your cluster are ready to be upgraded. Compute node health checks can only be run against compute clusters of one or more managed NetApp HCI compute nodes.

You can run health checks using NetApp Hybrid Cloud Control (HCC) UI or HCC API:

- [Use NetApp Hybrid Cloud Control to run compute node health checks prior to upgrading firmware](#) (Preferred method)
- [Use API to run compute node health checks prior to upgrading firmware](#)

You can also find out more about compute node health checks that are run by the service:

- [Compute node health checks made by the service](#)

What you'll need

- You have updated to the latest management services bundle (2.11 or later).
- You are running management node 11.3 or later.
- Your storage cluster is running NetApp Element software 11.3 or later.

Use NetApp Hybrid Cloud Control to run compute node health checks prior to upgrading firmware


Using NetApp Hybrid Cloud Control (HCC), you can verify that a compute node is ready for a firmware upgrade.

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 the **Compute firmware** tab.
5. Click the health check  for the cluster you want to check for upgrade readiness.
6. On the **Compute Health Check** page, click **Run Health Check**.
7. If there are issues, do the following:
 - a. Go to the specific KB article listed for each issue or perform the specified remedy.
 - b. If a KB is specified, complete the process described in the relevant KB article.
 - c. After you have resolved cluster issues, click **Re-Run Health Check**.

After the health check completes without errors, the compute nodes in the cluster are ready to upgrade. See [Update compute node firmware](#) to proceed.

Use API to run compute node health checks prior to upgrading firmware

You can use REST API to verify that compute nodes in a cluster are ready to be upgraded. The health check verifies that there are no obstacles to upgrading, such as ESXi host issues or other vSphere issues. You will need to run compute node health checks for each compute cluster in your environment.

Steps

1. Locate the controller ID and cluster ID:
 - a. Open the inventory service REST API UI on the management node:

```
https://[management node IP]/inventory/1
```
 - b. Click **Authorize** and complete the following:
 - i. Enter the cluster user name and password.
 - ii. Enter the client ID as `mnode-client` if the value is not already populated.
 - iii. Click **Authorize** to begin a session.
 - c. From the REST API UI, click **GET /installations**.
 - d. Click **Try it out**.
 - e. Click **Execute**.
 - f. From the code 200 response body, copy the `"id"` for the installation you plan to use for health checks.
 - g. From the REST API UI, click **GET /installations/{id}**.
 - h. Click **Try it out**.
 - i. Enter the installation ID.

- j. Click **Execute**.
- k. From the code 200 response body, copy the IDs for each of the following:
 - i. The cluster ID ("**clusterID**")
 - ii. A controller ID ("**controllerId**")

```
{
  "_links": {
    "collection": "https://10.117.187.199/inventory/1/installations",
    "self": "https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ]
    }
  },
}
```

2. Run health checks on the compute nodes in the cluster:

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

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

- b. Click **Authorize** and complete the following:
 - i. Enter the cluster user name and password.
 - ii. Enter the client ID as **mnode-client** if the value is not already populated.
 - iii. Click **Authorize** to begin a session.
- c. Click **POST /compute/{CONTROLLER_ID}/health-checks**.
- d. Click **Try it out**.

- e. Enter the **"controllerId"** you copied from the previous step in the **Controller_ID** parameter field.
- f. In the payload, enter the **"clusterId"** that you copied from the previous step as the **"cluster"** value and remove the **"nodes"** parameter.

```
{
  "cluster": "domain-1"
}
```

- g. Click **Execute** to run a health check on the cluster.

The code 200 response gives a **"resourceLink"** URL with the task ID appended that is needed to confirm the health check results.

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

- h. Copy the task ID portion of the **"resourceLink"** URL to verify the task result.
3. Verify the result of the health checks:
- a. Return to the compute service REST API UI on the management node:

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

- b. Click **GET /compute/tasks/{task_id}**.
- c. Click **Try it out**.
- d. Enter the task ID portion of the **"resourceLink"** URL from the **POST /compute/{CONTROLLER_ID}/health-checks** code 200 response in the **task_id** parameter field.
- e. Click **Execute**.
- f. If the **status** returned indicates that there were problems regarding compute node health, do the following:
 - i. Go to the specific KB article (**KbLink**) listed for each issue or perform the specified remedy.
 - ii. If a KB is specified, complete the process described in the relevant KB article.
 - iii. After you have resolved cluster issues, run **POST /compute/{CONTROLLER_ID}/health-checks** again (see step 2).

If health checks complete without issues, the response code 200 indicates a successful result.

Compute node health checks made by the service

Compute health checks, whether performed by HCC or API methods, make the following checks per node.

| Check description | Node/cluster | Action needed to resolve | Knowledgebase article with procedure |
|--|--------------|---|--------------------------------------|
| Is DRS enabled and fully automated? | Cluster | Turn on DRS and make sure it is fully automated. | See this KB. |
| Is DPM disabled in vSphere? | Cluster | Turn off Distributed Power Management. | See this KB. |
| Is HA admission control enabled in vSphere? | Cluster | Turn off HA admission control. | See this KB. |
| Is FT enabled for a VM on a host in the cluster? | Node | Suspend Fault Tolerance on any affected virtual machines. | See this KB. |
| Are there critical alarms in vCenter for the cluster? | Cluster | Launch vSphere and resolve and/or acknowledge any alerts before proceeding. | No KB needed to resolve issue. |
| Are there generic/global informational alerts in vCenter? | Cluster | Launch vSphere and resolve and/or acknowledge any alerts before proceeding. | No KB needed to resolve issue. |
| Are management services up to date? | HCI system | You must update management services before you perform an upgrade or run pre-upgrade health checks. | No KB needed to resolve issue. |
| Are there errors on the current ESXi node in vSphere? | Node | Launch vSphere and resolve and/or acknowledge any alerts before proceeding. | No KB needed to resolve issue. |
| Is virtual media mounted to a VM on a host in the cluster? | Node | Unmount all virtual media disks (CD/DVD/floppy) from the VMs. | No KB needed to resolve issue. |

| Check description | Node/cluster | Action needed to resolve | Knowledgebase article with procedure |
|---|--------------|---|--------------------------------------|
| Is BMC version the minimum required version that has RedFish support? | Node | Manually update your BMC firmware. | No KB needed to resolve issue. |
| Is ESXi host up and running? | Node | Start your ESXi host. | No KB needed to resolve issue. |
| Is ESXi host in maintenance mode? | Node | Your ESXi host should be placed in maintenance mode prior to updating firmware. | No KB needed to resolve issue. |
| Is BMC up and running? | Node | Power on your BMC and ensure it is connected to a network this management node can reach. | No KB needed to resolve issue. |
| Are there partner ESXi host(s) available? | Node | Make one or more ESXi host(s) in cluster available (not in maintenance mode) to migrate virtual machines. | No KB needed to resolve issue. |
| Are you able to connect with BMC via IPMI protocol? | Node | Enable IPMI protocol on BMC. | No KB needed to resolve issue. |

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Update compute node firmware

For any H-Series compute node, you can update the firmware for hardware components such as the BMC, BIOS, and NIC using the RTFI image while leaving the ESXi installation and other configuration data in place.

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

Before you begin

See the firmware and driver matrix for your hardware in [NetApp KB article 1088658](#) (login required).

About this task

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

As an alternative to using the USB thumb drive method described in this procedure, you can mount the compute node RTFI image 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 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 HCI software downloads](#) page 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** heading, download the NetApp HCI compute node image.
4. Write the raw contents of the compute node RTFI image to a USB thumb drive with at least 32GB capacity (using dd or Etcher).
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 updated compute node using vCenter.
11. Remove the USB flash drive from the updated compute node.
12. Repeat this task for other compute nodes in your ESXi cluster until all compute nodes are updated.

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Update compute node drivers

For any H-Series compute node, you can update the drivers used on the nodes using VMware Update Manager.

Before you begin

See the firmware and driver matrix for your hardware in [NetApp KB article 1088658](#) (login required).

About this task

Perform only one of these update operations at a time.

Steps

1. Browse to the [NetApp HCI software downloads](#) page and click the download link for correct version of NetApp HCI.
2. Accept the End User License Agreement.
3. Under the **Driver Packages for VMWare ESXi** heading, download the driver package for your node type and ESXi version.
4. Extract the downloaded driver bundle on your local computer.



The NetApp driver bundle includes one or more VMware Offline Bundle ZIP files; do not extract these ZIP files.

5. After upgrading the firmware on the compute nodes, go to **VMware Update Manager** in vCenter.
6. Import the driver offline bundle file for the compute nodes into the **Patch Repository**.
7. Create a new host baseline for the compute node.
8. Choose **Host Extension** for Name and Type and select all imported driver packages to be included in the new baseline.
9. In the **Host and Clusters** menu in vCenter, select the cluster with the compute nodes you would like to update and navigate to the **Update Manager** tab.
10. Click **Remediate** and then select the newly created host baseline. Ensure that drivers included in the baseline are selected.
11. Proceed through the wizard to the **Host Remediation Options** and ensure that the **Do Not Change VM Power State** option is selected to keep virtual machines online during the driver update.



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.

12. Proceed to the **Ready to Complete** page in the wizard and click **Finish**.

The drivers for all compute nodes in the cluster are updated one node at a time while virtual machines stay online.

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

vSphere upgrade sequences with vCenter Plug-in

Upgrade your vSphere components for a NetApp HCI system with the Element Plug-in for vCenter Server

When you upgrade the VMware vSphere components of your NetApp HCI installation, there are some additional steps you will need to take for the Element Plug-in for vCenter Server.

Steps

1. For vCSA upgrades, [clear](#) mNode settings in the plug-in (**NetApp Element Configuration > mNode Settings**). The **mNode Status** field displays **Not Configured** after the process is complete.
2. For vCSA and Windows upgrades, [unregister](#) the plug-in from the vCenter Server with which it is associated using the registration utility.
3. [Upgrade vSphere, including vCenter Server, ESXi, VMs, and other VMware components.](#)



When upgrading ESXi for compute nodes for a [two-node cluster](#), upgrade only one compute node at a time so that only one witness node is temporarily unavailable and cluster quorum can be maintained.

4. [Register](#) the Element Plug-in for vCenter Server again with vCenter.
5. [Add clusters](#) using the plug-in.
6. [Configure QoSSIOC settings](#) using the plug-in.
7. [Enable QoSSIOC](#) for all datastores controlled by the plug-in.

Find more information

- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)
- [NetApp HCI Two-Node Storage Cluster Technical Report](#)

Upgrade your vSphere components for a NetApp SolidFire storage system with the Element Plug-in for vCenter Server

When you upgrade the VMware vSphere components of your SolidFire Element storage installation, there are some additional steps you will need to take for systems with Element Plug-in for vCenter Server.

Steps

1. For vCSA upgrades, [clear](#) mNode settings in the plug-in (**NetApp Element Configuration > mNode Settings**). The **mNode Status** field displays **Not Configured** after the process is complete.
2. For vCSA and Windows upgrades, [unregister](#) the plug-in from the vCenter Server with which it is associated using the registration utility.
3. [Upgrade vSphere, including vCenter Server, ESXi, VMs, and other VMware components.](#)
4. [Register](#) the Element Plug-in for vCenter Server again with vCenter.
5. [Add clusters](#) using the plug-in.
6. [Configure QoSSIOC settings](#) using the plug-in.
7. [Enable QoSSIOC](#) for all datastores controlled by the plug-in.

Find more information

- [NetApp HCI Documentation Center](#)
- [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.