Manage NetApp HCI

HCI

NetApp
November 17, 2020

Table of Contents

Manage NetApp HCI

Monitor your NetApp HCI system with NetApp Hybrid Cloud Control

Monitor storage and compute resources on the Hybrid Cloud Control Dashboard

With the NetApp Hybrid Cloud Control Dashboard, you can view all your storage and compute resources at a glance. Additionally, you can monitor storage capacity, storage performance, and compute utilization.

Only compute nodes that are managed and clusters with at least one managed node in H-series hardware appear on the Hybrid Cloud Control Dashboard.
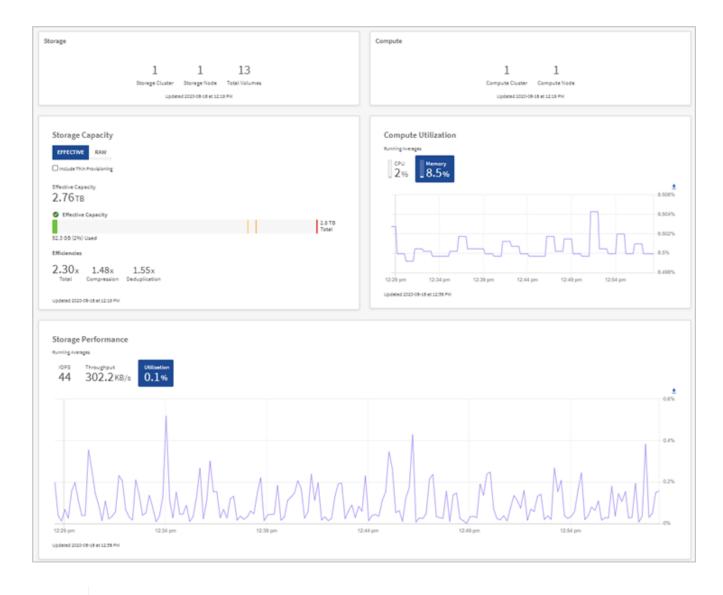
- Access the NetApp HCC Dashboard
- Monitor storage resources
- Monitor compute resources
- Monitor storage capacity
- Monitor storage performance
- Monitor compute utilization

Access the NetApp HCC Dashboard

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.

3. View the Hybrid Cloud Control Dashboard.

You might see some or all these panes, depending on your installation. For example, for storage-only installations, the Hybrid Cloud Control Dashboard shows only the Storage pane, the Storage Capacity pane, and the Storage Performance pane.

Monitor storage resources

Use the **Storage** pane to see your total storage environment. You can monitor the number of storage clusters, storage nodes, and total volumes.

Monitor compute resources

Use the **Compute** pane to see your total NetApp H-series compute environment. You can monitor the number of compute clusters and total compute nodes.

Monitor storage capacity

Monitoring the storage capacity of your environment is critical. Using the Storage Capacity pane, you can determine your storage capacity efficiency gains with or without compression, deduplication, and

thin provisioning features enabled.

You can see the total physical storage space available in your cluster on the **RAW** tab, and information about the provisioned storage on the **EFFECTIVE** tab.

> 💡 To view cluster health, also look at the SolidFire Active IQ Dashboard. See Monitor performance, capacity, and cluster health in NetApp SolidFire Active IQ.

Steps

1. Click the **RAW** tab, to see the total physical storage space used and available in your cluster.

   Look at the vertical lines to determine whether your used capacity is less than the total or less than Warning, Error, or Critical thresholds. Hover over the lines to see details.

   > ℹ️ You can set the threshold for Warning, which defaults to 3% below the Error threshold. The Error and Critical thresholds are preset and not configurable by design. The Error threshold indicates that less than one node of capacity remains in the cluster. For steps on setting the threshold, see Setting cluster full threshold.

   > 💡 For details about the related cluster thresholds Element API, see "getClusterFullThreshold" in the *Element API Guide*. To view details about block and metadata capacity, see Understanding cluster fullness levels in the *Element User Guide*.

2. Click the **EFFECTIVE** tab, to see information about total storage provisioned to connected hosts and to see efficiency ratings.

   a. Optionally, check **Include Thin Provisioning** to see thin provisioning efficiency rates in the Effective Capacity bar chart.

   b. **Effective Capacity bar chart**: Look at the vertical lines to determine whether your used capacity is less than the total or less than Warning, Error, or Critical thresholds. Similar to the

Raw tab, you can hover over the vertical lines to see details.

c. **Efficiencies**: Look at these ratings to determine your storage capacity efficiency gains with compression, deduplication, and thin provisioning features enabled. For example, if compression shows as "1.3x", this means that storage efficiency with compression enabled is 1.3 times more efficient than without it.

> **ⓘ** Total Efficiencies equals (maxUsedSpace * efficiency factor) / 2, where efficiencyFactor = (thinProvisioningFactor * deDuplicationFactor * compressionFactor). When Thin Provisioning is unchecked, it is not included in the Total Efficiency.

d. If the effective storage capacity nears an Error or Critical threshold, consider clearing the data on your system. Alternatively, consider expanding your system.

   See Expansion overview.

3. For further analysis and historical context, look at NetApp SolidFire Active IQ details.

Monitor storage performance

You can look at how much IOPS or throughput you can get out of a cluster without surpassing the useful performance of that resource by using the Storage Performance pane. Storage performance is the point at which you get the maximum utilization before latency becomes an issue.

The Storage Performance pane helps you identify whether the performance is reaching the point where the performance might degrade if the workloads increase.

The information on this pane refreshes every 10 seconds and shows an average of all the points on the graph.

For details about the associated Element API method, see the GetClusterStats method in the *Element API Reference Guide*.

Steps

1. View the Storage Performance pane. For details, hover over points in the graph.

a. **IOPS** tab: See the current operations per second. Look for trends in data or spikes. For example, if you see that the maximum IOPS is 160K and 100K of that is free or available IOPS, you might consider adding more workloads to this cluster. On the other hand, if you see that only 140K is available, you might consider offloading workloads or expanding your system.

b. **Throughput** tab: Monitor patterns or spikes in throughput. Also monitor for continuously high throughput values, which might indicate that you are nearing the maximum useful performance of the resource.

c. **Utilization** tab: Monitor the utilization of IOPS in relation to the total IOPS available summed up at the cluster level.

Storage Performance
Running Averages

IOPS **60** Throughput **439.9** KB/s Utilization **0.1**%

2. For further analysis, look at storage performance by using the NetApp Element Plug-in for vCenter Server.

   Performance shown in the NetApp Element Plug-in for vCenter Server.
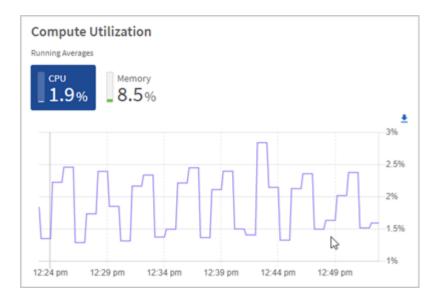
Monitor compute utilization

In addition to monitoring IOPS and throughput of your storage resources, you also might want to view the CPU and memory usage of your compute assets. The total IOPS that a node can provide is based on the physical characteristics of the node, for example, the number of CPUs, the CPU speed, and the amount of RAM.

Steps

1. View the **Compute Utilization** pane. Using both the CPU and Memory tabs, look for patterns or spikes in utilization. Also look for continuously high usage, indicating that you might be nearing the maximum utilization for the compute clusters.

   > **i** This pane shows data only for those compute clusters managed by this installation.

a. **CPU** tab: See the current average of CPU utilization on the compute cluster.

b. **Memory** tab: See the current average memory usage on the compute cluster.

2. For further analysis on compute information, look at these resources:

a. NetApp Element Plug-in for vCenter Server for cluster management details

b. NetApp SolidFire Active IQ for historical data

Find more information

- NetApp HCI Documentation Center
- NetApp HCI Resources Page

View your inventory on the Nodes page

You can view both your storage and compute assets in your system and determine their IP addresses, names, and software versions.

You can view storage information for your multiple node systems and any NetApp HCI Witness Nodes associated with two-node or three-node clusters.
Witness Nodes manage quorum within the cluster; they are not used for storage. Witness Nodes are applicable only to NetApp HCI and not to all-flash storage environments.

For more information about Witness Nodes, see Nodes definitions.

For SolidFire Enterprise SDS nodes, you can monitor inventory on the Storage tab.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.

   The NetApp Hybrid Cloud Control Dashboard appears.

3. In the left navigation, click **Nodes**.

   The Storage tab appears.

4. On the **Storage** tab of the Nodes page, review the following information:

   a. Two-node clusters: A "two-node" label appears on the Storage tab and the associated Witness Nodes are listed.

   b. Three-node clusters: The storage nodes and associated Witness Nodes are listed. Three-node clusters have a Witness Node deployed on standby to maintain high availability in the case of node failure.

   c. Clusters with four nodes or more: Information for clusters with four or more nodes appears. Witness Nodes do not apply. If you started with two or three storage nodes and added more nodes, the Witness Nodes still appear. Otherwise, the Witness Nodes table does not appear.

   d. The firmware bundle version: Starting with management services version 2.14, if you have clusters running Element 12.0 or later, you can see the firmware bundle version for these clusters. If the nodes in a cluster have different firmware versions on them, you can see **Multiple** in the **Firmware Bundle Version** column.

5. To view compute inventory information, click **Compute**.

6. You can manipulate the information on these pages in several ways:

   a. To filter the list of items in the results, click the **Filter** icon and select the filters. You can also enter text for the filter.

   b. To show or hide columns, click the **Show/Hide Columns** icon.

   c. To download the table, click the **Download** icon.

   d. To add or edit the stored BMC credentials for a compute node with BMC connection errors, click **Edit connection settings** in the error message text in the **BMC Connection Status** column. Only if the connection attempt fails for a compute node, an error message is displayed in this column for that node.

   > 💡 To view the number of storage and compute resources, look at the NetApp Hybrid Cloud Control (HCC) Dashboard. See Monitor storage and compute resources with the HCC Dashboard.

Find more information

- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Edit Baseboard Management Controller connection information

You can change Baseboard Management Controller (BMC) administrator credentials in NetApp Hybrid Cloud Control for each of your compute nodes. You might need to change credentials prior to upgrading BMC firmware or to resolve a `Hardware ID not available` or `Unable to Detect` error indicated in NetApp Hybrid Cloud Control.

What you'll need

Cluster administrator permissions to change BMC credentials.

> ℹ️ If you set BMC credentials during a health check, there can be a delay of up to 15 minutes before the change is reflected on the **Nodes** page.

Options

Choose one of the following options to change BMC credentials:

- Use NetApp Hybrid Cloud Control to edit BMC information
- Use the REST API to edit BMC information

Use NetApp Hybrid Cloud Control to edit BMC information

You can edit the stored BMC credentials using the NetApp Hybrid Cloud Control Dashboard.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.

3. In the left navigation blue box, select the NetApp HCI installation.

   The NetApp Hybrid Cloud Control Dashboard appears.

4. In the left navigation, click **Nodes**.

5. To view compute inventory information, click **Compute**.

   A list of your compute nodes appears. The **BMC Connection Status** column shows the result of BMC connection attempts for each compute node. If the connection attempt fails for a compute node, an error message is displayed in this column for that node.

6. To add or edit the stored BMC credentials for a compute node with BMC connection errors, click **Edit connection settings** in the error message text.

7. In the dialog that appears, add the correct administrator user name and password for the BMC of this compute node.

8. Click **Save**.

9. Repeat steps 6 through 8 for any compute node that has missing or incorrect stored BMC credentials.

   > ℹ️ Updating BMC information refreshes the inventory and ensures that management node services are aware of all hardware parameters needed to complete the upgrade.

Use the REST API to edit BMC information

You can edit the stored BMC credentials using the NetApp Hybrid Cloud Control REST API.

Steps

1. Locate the compute node hardware tag and BMC information:

   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`.

    iii. Click **Authorize** to begin a session.

    iv. 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 node asset id (`id`), BMC IP address (`bmcAddress`), and node serial number (`chassisSerialNumber`) for use in a later step.

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.117.1.111",
      "credentialsAvailable": false,
      "credentialsValidated": false
    },
    "chassisSerialNumber": "221111019323",
    "chassisSlot": "C",
    "hardwareId": null,
    "hardwareTag": "00000000-0000-0000-0000-ac1f6ab4ecf6",
    "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
```

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

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

3. 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.

    d. Close the window.

4. Click **PUT /nodes/{hardware_id}**.

5. Click **Try it out**.

6. Enter the node asset id that you saved earlier in the `hardware_id` parameter.

7. Enter the following information in the payload:

Parameter	Description
assetId	The installation asset id (`id`) that you saved in step 1(f).
bmcIp	The BMC IP address (`bmcAddress`) that you saved in step 1(k).
bmcPassword	An updated password to log into the BMC.
bmcUsername	An updated user name to log into the BMC.
serialNumber	The chassis serial number of the hardware.

Example payload:

```
{
    "assetId": "7bb41e3c-2e9c-2151-b00a-8a9b49c0b0fe",
    "bmcIp": "10.117.1.111",
    "bmcPassword": "mypassword1",
    "bmcUsername": "admin1",
    "serialNumber": "221111019323"
}
```

8. Click **Execute** to update BMC credentials.
   A successful result returns a response similar to the following:

```
{
    "credentialid": "33333333-cccc-3333-cccc-333333333333",
    "host_name": "hci-host",
    "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
    "ip": "1.1.1.1",
    "parent": "abcd01y3-ab30-1ccc-11ee-11f123zx7d1b",
    "type": "BMC"
}
```

Find more information

- Known issues and workarounds for compute node upgrades

- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Monitor volumes on your storage cluster

The SolidFire system provisions storage using volumes. Volumes are block devices accessed over the network by iSCSI or Fibre Channel clients. You can monitor details about access groups, accounts, initiators, used capacity, Snapshot data protection status, number of iSCSI sessions, and the Quality of Service (QoS) policy associated with the volume.

You can also see details on active and deleted volumes.

With this view, you might first want to monitor the Used capacity column.

You can access this information only if you have NetApp Hybrid Cloud Control administrative privileges.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.

3. In the left navigation blue box, select the NetApp HCI installation.

   The Hybrid Cloud Control Dashboard appears.

4. In the left navigation, select the cluster and select **Storage** > **Volumes**.

	ID ↑	Name	Account	Access Groups	Access	Used	Size	Snapshots	QoS Policy	Min IOPS	Max IOPS	Burst IOPS	iSCSI Sessions	Actions
☐	1	NetApp-H...	NetApp-HCI	NetApp-H...	Read/Write	2%	2.15 TB	0	None	50	15000	15000	3	⋮
☐	2	NetApp-H...	NetApp-HCI	NetApp-H...	Read/Write	0%	2.15 TB	0	None	50	15000	15000	3	⋮
☐	3	NetApp-H...	tenant_Emily mnode		Read/Write	0%	5.37 GB	0	None	1000	2000	4000	1	⋮
☐	4	NetApp-H...	tenant_Emily mnode		Read/Write	0%	53.69 GB	0	None	1000	2000	4000	1	⋮
☐	5	NetApp-H...	tenant_Emily mnode		Read/Write	0%	1.07 GB	0	None	1000	2000	4000	1	⋮
☐	6	NetApp-S...	tenant_Emily mnode		Read/Write	0%	1.07 GB	0	None	1000	2000	4000	1	⋮
☐	7	NetApp-H...	tenant_Emily mnode		Read/Write	0%	1.07 GB	0	None	1000	2000	4000	1	⋮
☐	8	NetApp-H...	tenant_Emily mnode		Read/Write	0%	42.95 GB	0	None	1000	20000	40000	1	⋮

1 - 12 of 12 results

5. On the Volumes page, use the following options:

  a. Filter the results by clicking the **Filter** icon.

  b. Hide or show columns by clicking the **Hide/Show** icon.

  c. Refresh data by clicking the **Refresh** icon.

  d. Download a CSV file by clicking on the **Download** icon.

6. Monitor the Used capacity column. If Warning, Error, or Critical thresholds are reached, the color represents the used capacity status:

  a. Warning - Yellow

  b. Error - Orange

  c. Critical - Red

7. From the Volumes view, click the tabs to see additional details about the volumes:

  a. **Access Groups**: You can see the volume access groups that are mapped from initiators to a collection of volumes for secured access.

    See information about volume access groups.

  b. **Accounts**: You can see the user accounts, which enable clients to connect to volumes on a node.

When you create a volume, it is assigned to a specific user account.

See information about NetApp HCI user accounts.

c. **Initiators**: You can see the iSCSI initiator IQN or Fibre Channel WWPNs for the volume. Each IQN added to an access group can access each volume in the group without requiring CHAP authentication. Each WWPN added to an access group enables Fibre Channel network access to the volumes in the access group.

See information about access groups, initiators, and CHAP authentication methods in the *NetApp Element User Guide.*

d. **QoS Policies**: You can see the QoS policy applied to the volume. A QoS policy applies standardized settings for minimum IOPS, maximum IOPS, and burst IOPS to multiple volumes.

See information about performance and QoS policies.

See information about Quality of Service policies in the *NetApp Element User Guide.*

Find more information

- NetApp SolidFire and Element Documentation Center
- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Monitor performance, capacity, and cluster health with SolidFire Active IQ

By using SolidFire Active IQ, you can monitor the events, performance, and capacity of your clusters. You can access SolidFire Active IQ from the NetApp Hybrid Cloud Control Dashboard.

Before you begin

- You must have a NetApp Support account to take advantage of this service.
- You must have authorization to use management node REST APIs.
- You have deployed a management node running version 12.0 or later.
- Your cluster version is running NetApp Element software 12.0 or later.
- You have Internet access. The Active IQ collector service cannot be used from dark sites.

About this task
You can obtain continually updated historical views of cluster-wide statistics. You can set up notifications to alert you about specified events, thresholds, or metrics on a cluster so that they can be addressed quickly.

As part of your normal support contract, NetApp Support monitors this data and alerts you to potential system issues.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.

3. From the Dashboard, click the menu on the upper right.

4. Select **View Active IQ**.

   The SolidFire Active IQ Dashboard appears.

5. To learn about SolidFire Active IQ, from the Dashboard, click the menu icon on the upper right and click **Documentation**.

6. From the SolidFire Active IQ interface, verify that the NetApp HCI compute and storage nodes are reporting telemetry correctly to Active IQ:

   a. If you have more than one NetApp HCI installation, click **Select a Cluster** and choose the cluster from the list.

   b. In the left navigation pane, click **Nodes**.

7. If a node or nodes are missing from the list, contact NetApp Support.

> To view the number of storage and compute resources, look at the Hybrid Cloud Control (HCC) Dashboard. See Monitor storage and compute resources with the HCC Dashboard.

Find more information

- NetApp SolidFire Active IQ Documentation
- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Collect logs for troubleshooting

If you have trouble with your NetApp HCI or SolidFire all-flash storage installation, you can collect logs to send to NetApp Support to help with diagnosis. You can either use NetApp Hybrid Cloud Control or the REST API to collect logs on NetApp HCI or Element systems.

What you'll need

- Ensure that your storage cluster version is running NetApp Element software 11.3 or later.
- Ensure that you have deployed a management node running version 11.3 or later.

Log collection options

Choose one of the following options:

- Use NetApp Hybrid Cloud Control to collect logs
- Use the REST API to collect logs

Use NetApp Hybrid Cloud Control to collect logs

You can access the log collection area from the NetApp Hybrid Cloud Control Dashboard.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

3. From the Dashboard, click the menu on the upper right.

4. Select **Collect Logs**.

   The **Collect Logs** page appears. If you have collected logs before, you can download the existing log package, or begin a new log collection.

5. Select a date range in the **Date Range** drop-down menu to specify what dates the logs should include.

   If you specify a custom start date, you can select the date to begin the date range. Logs will be collected from that date up to the present time.

6. In the **Log Collection** section, select the types of log files the log package should include.

   For storage and compute logs, you can expand the list of storage or compute nodes and select individual nodes to collect logs from (or all nodes in the list).

7. Click **Collect Logs** to start log collection.

   Log collection runs in the background, and the page shows the progress.

   > Depending on the logs you collect, the progress bar might remain at a certain percentage for several minutes, or progress very slowly at some points.

8. Click **Download Logs** to download the log package.

The log package is in a compressed UNIX .tgz file format.

Use the REST API to collect logs

You can use REST API to collect NetApp HCI or Element logs.

Steps

1. Locate the storage cluster ID:

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

   ```
   https://[management node IP]/logs/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.

2. Collect logs from NetApp HCI or Element:

   a. Click **POST /bundle**.

   b. Click **Try it out**.

   c. Change the values of the following parameters in the **Request body** field depending on which type of logs you need to collect and for what time range:

Parameter	Type	Description
`modifiedSince`	Date string	Only include logs modified after this date and time. For example, the value "2020-07-14T20:19:00.000Z" defines a start date of July 14, 2020 at 20:19 UTC.
`computeLogs`	Boolean	Set this parameter to `true` to include compute node logs.

Parameter	Type	Description
computeIds	UUID array	If computeLogs is set to true, populate this parameter with the management node asset IDs of compute nodes to limit log collection to those specific compute nodes. Use the GET https://[management node IP]/logs/1/bundle/options endpoint to see all possible node IDs you can use.
mnodeLogs	Boolean	Set this parameter to true to include management node logs.
storageCrashDumps	Boolean	Set this parameter to true to include storage node crash debug logs.
storageLogs	Boolean	Set this parameter to true to include storage node logs.
storageNodeIds	UUID array	If storageLogs is set to true, populate this parameter with the storage cluster node IDs to limit log collection to those specific storage nodes. Use the GET https://[management node IP]/logs/1/bundle/options endpoint to see all possible node IDs you can use.

d. Click **Execute** to begin log collection.

The response should return a response similar to the following:

```
{
  "_links": {
    "self": "https://10.1.1.5/logs/1/bundle"
  },
  "taskId": "4157881b-z889-45ce-adb4-92b1843c53ee",
  "taskLink": "https://10.1.1.5/logs/1/bundle"
}
```

3. Check on the status of the log collection task:

   a. Click **GET /bundle**.

b. Click **Try it out**.

c. Click **Execute** to return a status of the collection task.

d. Scroll to the bottom of the response body.

You should see a `percentComplete` attribute detailing the progress of the collection. If the collection is complete, the `downloadLink` attribute contains the full download link including the file name of the log package.

e. Copy the file name at the end of the `downloadLink` attribute.

4. Download the collected log package:

a. Click **GET /bundle/{filename}**.

b. Click **Try it out**.

c. Paste the file name you copied earlier into the `filename` parameter text field.

d. Click **Execute**.

After execution, a download link appears in the response body area.

e. Click **Download file** and save the resulting file to your computer.

The log package is in a compressed UNIX .tgz file format.

Find more information

- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Manage NetApp HCI storage with NetApp Hybrid Cloud Control

Create and manage user accounts by using NetApp Hybrid Cloud Control

In SolidFire storage systems, authoritative cluster users can be created to enable login access to NetApp Hybrid Cloud Control depending on the permissions you wish to grant "Administrator" or "Read-only" users. In addition to cluster users, there are also volume accounts, which enable clients to connect to volumes on a storage node.

When you create a volume, it is assigned to a specific volume account.

An account can have up to two-thousand volumes assigned to it, but a volume can belong to only one account.

Manage the following types of accounts:

- [Manage authoritative cluster accounts](#)
- [Manage volume accounts](#)

Manage authoritative cluster accounts

Authoritative user accounts are managed from the top right menu User Management option in NetApp Hybrid Cloud Control. These types of accounts enable you to authenticate against any storage asset associated with a NetApp Hybrid Cloud Control instance of nodes and clusters. With this account, you can manage volumes, accounts, access groups, and more across all clusters.

Create an authoritative cluster account

You can create an account by using NetApp Hybrid Cloud Control.

This account can be used to log in to the Hybrid Cloud Control, the per-node UI for the cluster, and the storage cluster in NetApp Element software.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, click on the top right Options icon and select **User Management**.

3. Select **Create User**.

4. Enter a name and password for the new account.

5. Select either Administrator or Read-only permissions.

   > To view the permissions from NetApp Element software, click **Show legacy permissions**. If you select a subset of these permissions, the account is assigned Read-only permissions. If you select all legacy permissions, the account is assigned Administrator permissions.

6. Check the box indicating that "I have read and accept the NetApp End User License Agreement."

7. Click **Create User**.

Edit an authoritative cluster account

You can change the permissions or password on a user account by using NetApp Hybrid Cloud Control.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, click on the icon in the top right and select **User Management**.

3. Optionally filter the list of user accounts by selecting **Cluster**, **LDAP**, or **Idp**.

   If you configured users on the storage cluster with LDAP, those accounts show a User Type of "LDAP." If you configured users on the storage cluster with Idp, those accounts show a User Type of "Idp."

4. In the **Actions** column in the table, expand the menu for the account and select **Edit**.

5. Make changes as needed.

6. Select **Save**.

Delete an authoritative user account

You can delete one or more accounts when it is no longer needed.

You cannot delete the primary administrator user account for the authoritative cluster.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, click on the icon in the top right and select **User Management**.

3. In the **Actions** column in the Users table, expand the menu for the account and select **Delete**.

4. Confirm the deletion by selecting **Yes**.

Manage volume accounts

Volume accounts are managed within the NetApp Hybrid Cloud Control Volumes table. These accounts are specific only to the storage cluster on which they were created. These types of accounts enable you to set permissions on volumes across the network, but have no effect outside of those volumes.

A volume account contains the CHAP authentication required to access the volumes assigned to it.

Create a volume account

Create an account specific to this volume.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, select **Storage** > **Volumes**.

3. Select the **Accounts** tab.

4. Select the **Create Account** button.

5. Enter a name for the new account.

6. In the CHAP Settings section, enter the following information:

- Initiator Secret for CHAP node session authentication

- Target Secret for CHAP node session authentication

> ℹ️ To auto-generate either password, leave the credential fields blank.

7. Select **Create Account**.

Edit a volume account

You can change the CHAP info and change whether an account is active or locked.

> ⛔ Deleting or locking an account associated with the management node results in an inaccessible management node.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, select **Storage** > **Volumes**.

3. Select the **Accounts** tab.

4. In the **Actions** column in the table, expand the menu for the account and select **Edit**.

5. Make changes as needed.

6. Confirm the changes by selecting **Yes**.

Delete a volume account

Delete an account that you no longer need.

Before you delete a volume account, delete and purge any volumes associated with the account first.

> ⛔ Deleting or locking an account associated with the management node results in an inaccessible management node.

> ℹ️ Persistent volumes that are associated with management services are assigned to a new account during installation or upgrade. If you are using persistent volumes, do not modify or delete the volumes or their associated account. If you do delete these accounts, you could render your management node unusable.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, select **Storage** > **Volumes**.

3. Select the **Accounts** tab.

4. In the **Actions** column in the table, expand the menu for the account and select **Delete**.

5. Confirm the deletion by selecting **Yes**.

Find more information

- Learn about accounts
- Work with user accounts
- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Create and manage volumes by using NetApp Hybrid Cloud Control

You can create a volume and associate the volume with a given account. Associating a volume with an account gives the account access to the volume through the iSCSI initiators and CHAP credentials.

You can specify QoS settings for a volume during creation.

You can manage volumes in NetApp Hybrid Cloud Control in the following ways:

- Create a volume
- Apply a QoS policy to a volume
- Edit a volume
- Clone volumes
- Delete a volume
- Restore a deleted volume
- Purge a deleted volume

Create a volume

You can create a storage volume using NetApp Hybrid Cloud Control.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select **Volumes** > **Overview** tab.

4. Select **Create Volume**.

5. Enter a name for the new volume.

6. Enter the total size of the volume.

> **i** The default volume size selection is in GB. You can create volumes using sizes measured in GB or GiB:
> 1GB = 1 000 000 000 bytes
> 1GiB = 1 073 741 824 bytes

7. Select a block size for the volume.

8. From the Account list, select the account that should have access to the volume.

> **i** If there are more than 50 accounts, the list does not appear. Begin typing and the auto-complete feature displays values for you to choose.

9. To set the Quality of Service, do one of the following:

   a. Select an existing QoS policy.

   b. Under QoS Settings, set customized minimum, maximum, and burst values for IOPS or use the default QoS values.

   Volumes that have a Max or Burst IOPS value greater than 20,000 IOPS might require high queue depth or multiple sessions to achieve this level of IOPS on a single volume.

10. Click **Create Volume**.

Apply a QoS policy to a volume

You can apply a QoS policy to an existing storage volume by using NetApp Hybrid Cloud Control.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select **Volumes** > **Overview**.

4. In the **Actions** column in the volumes table, expand the menu for the volume and select **Edit**.

5. Change the Quality of Service by doing one of the following:

   a. Select an existing policy.

   b. Under Custom Settings, set the minimum, maximum, and burst values for IOPS or use the default values.

> **i** If you are using QoS policies on a volume, you can set custom QoS to remove the QoS policy affiliation with the volume. Custom QoS override QoS policy values for volume QoS settings.

When you change IOPS values, increment in tens or hundreds. Input values require valid whole numbers. Configure volumes with an extremely high burst value. This enables the system to process occasional large block, sequential workloads more quickly, while still constraining the sustained IOPS for a volume.

6. Select **Save**.

Edit a volume

Using NetApp Hybrid Cloud Control, you can edit volume attributes such as QoS values, volume size, and the unit of measurement by which byte values are calculated. You can also modify account access for replication usage or to restrict access to the volume.

About this task

You can resize a volume when there is sufficient space on the cluster under the following conditions:

- Normal operating conditions.
- Volume errors or failures are being reported.
- The volume is being cloned.
- The volume is being resynced.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.
2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.
3. Select **Volumes** > **Overview**.
4. In the **Actions** column in the volumes table, expand the menu for the volume and select **Edit**.
5. Make changes as needed:

   a. Change the total size of the volume.

   > You can increase, but not decrease, the size of the volume. You can only resize one volume in a single resizing operation. Garbage collection operations and software upgrades do not interrupt the resizing operation.

   > If you are adjusting volume size for replication, first increase the size of the volume assigned as the replication target. Then you can resize the source volume. The target volume can be greater or equal in size to the source volume, but it cannot be smaller.

> **i** The default volume size selection is in GB. You can create volumes using sizes measured in GB or GiB:
> 1GB = 1 000 000 000 bytes
> 1GiB = 1 073 741 824 bytes

    b. Select a different account access level:

- Read Only

- Read/Write

- Locked

- Replication Target

    c. Select the account that should have access to the volume.

    Begin typing and the auto-complete function displays possible values for you to choose.

    d. Change the Quality of Service by doing one of the following:

      i. Select an existing policy.

      ii. Under Custom Settings, set the minimum, maximum, and burst values for IOPS or use the default values.

> **i** If you are using QoS policies on a volume, you can set custom QoS to remove the QoS policy affiliation with the volume. Custom QoS will override QoS policy values for volume QoS settings.

> **♀** When you change IOPS values, you should increment in tens or hundreds. Input values require valid whole numbers. Configure volumes with an extremely high burst value. This enables the system to process occasional large block, sequential workloads more quickly, while still constraining the sustained IOPS for a volume.

6. Select **Save**.

Clone volumes

You can create a clone of a single storage volume or clone a group of volumes to make a point-in-time copy of the data. When you clone a volume, the system creates a snapshot of the volume and then creates a copy of the data referenced by the snapshot.

Before you begin

- At least one cluster must be added and running.

- At least one volume has been created.

- A user account has been created.

- Available unprovisioned space must be equal to or more than the volume size.

About this task

The cluster supports up to two running clone requests per volume at a time and up to 8 active volume clone operations at a time. Requests beyond these limits are queued for later processing.

Volume cloning is an asynchronous process, and the amount of time the process requires depends on the size of the volume you are cloning and the current cluster load.

> ℹ️ Cloned volumes do not inherit volume access group membership from the source volume.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select the **Volumes** > **Overview** tab.

4. Select each volume you want to clone and click the **Clone** button that appears.

5. Do one of the following:

   ◦ To clone a single volume, perform the following steps:

     a. In the **Clone Volume** dialog box, enter a volume name for the volume clone.

        > 💡 Use descriptive naming best practices. This is especially important if multiple clusters or vCenter Servers are used in your environment.

     b. Select an account access level:

        ▪ Read Only

        ▪ Read/Write

        ▪ Locked

        ▪ Replication Target

     c. Select a size in GB or GIB for the volume clone.

        > ℹ️ Increasing the volume size of a clone results in a new volume with additional free space at the end of the volume. Depending on how you use the volume, you may need to extend partitions or create new partitions in the free space to make use of it.

     d. Select an account to associate with the volume clone.

     e. Click **Clone Volumes**.

- To clone multiple volumes, perform the following steps:

    a. In the **Clone Volumes** dialog box, enter an optional prefix for the volume clones in the **New Volume Name Prefix** field.

    b. Select a new type of access for the volume clones or copy the access type from the active volumes.

    c. Select a new account to associate with the volume clones or copy the account association from the active volumes.

    d. Click **Clone Volumes**.

> The time to complete a cloning operation is affected by volume size and current cluster load. Refresh the page if the cloned volume does not appear in the volume list.

Delete a volume

You can delete one or more volumes from an Element storage cluster.

About this task

The system does not immediately purge deleted volumes; they remain available for approximately eight hours. After eight hours, they are purged and no longer available. If you restore a volume before the system purges it, the volume comes back online and iSCSI connections are restored.

If a volume used to create a snapshot is deleted, its associated snapshots become inactive. When the deleted source volumes are purged, the associated inactive snapshots are also removed from the system.

> Persistent volumes that are associated with management services are created and assigned to a new account during installation or upgrade. If you are using persistent volumes, do not modify or delete the volumes or their associated account. If you do delete these volumes, you could render your management node unusable.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select **Volumes** > **Overview**.

4. Select one or more volumes to delete.

5. Do one of the following:

    - If you selected multiple volumes, click the **Delete** quick filter at the top of the table.

    - If you selected a single volume, in the **Actions** column of the Volumes table, expand the menu for the volume and select **Delete**.

6. Confirm the delete by selecting **Yes**.

Restore a deleted volume

After a storage volume is deleted, you can still restore it if you do so before eight hours after deletion.

The system does not immediately purge deleted volumes; they remain available for approximately eight hours. After eight hours, they are purged and no longer available. If you restore a volume before the system purges it, the volume comes back online and iSCSI connections are restored.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select **Volumes** > **Overview**.

4. Select **Deleted**.

5. In the **Actions** column of the Volumes table, expand the menu for the volume and select **Restore**.

6. Confirm the process by selecting **Yes**.

Purge a deleted volume

After storage volumes are deleted, they remain available for approximately eight hours. After eight hours, they are purged automatically and no longer available. If you do not want to wait for the eight hours, you can delete

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select **Volumes** > **Overview**.

4. Select **Deleted**.

5. Select one or more volumes to purge.

6. Do one of the following:

   ◦ If you selected multiple volumes, click the **Purge** quick filter at the top of the table.

   ◦ If you selected a single volume, in the **Actions** column of the Volumes table, expand the menu for the volume and select **Purge**.

7. In the **Actions** column of the Volumes table, expand the menu for the volume and select **Purge**.

8. Confirm the process by selecting **Yes**.

Find more information

- [Learn about volumes](#)

- [Work with volumes](#)

- [NetApp HCI Documentation Center](#)

- [NetApp HCI Resources Page](#)

Create and manage volume access groups

You can add new volume access groups, delete existing volume access groups, edit the details of a volume access group, and view the details of a volume access group by using NetApp Hybrid Cloud Control.

What you'll need

- You have administrator credentials for this NetApp HCI system.

- You are running management node 12.2 or later.

- You have upgraded your management services to at least version 2.15.28. NetApp Hybrid Cloud Control storage management is not available in earlier service bundle versions.

- Ensure you have a logical naming scheme for volume access groups.

Add a volume access group

You can add a volume access group to a storage cluster by using NetApp Hybrid Cloud Control.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select **Volumes**.

4. Select the **Access Groups** tab.

5. Select the **Create Access Group** button.

6. In the resulting dialog, enter a name for the new volume access group.

7. (Optional) In the **Initiators** section, select one or more initiators to associate with the new volume access group.

   If you associate an initiator with the volume access group, that initiator can access each volume in the group without the need for authentication.

8. (Optional) In the **Volumes** section, select one or more volumes to include in this volume access group.

9. Select **Create Access Group**.

Edit a volume access group

You can edit the properties of an existing volume access group by using NetApp Hybrid Cloud Control.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select **Volumes**.

4. Select the **Access Groups** tab.

5. In the **Actions** column of the table of access groups, expand the options menu for the access group you need to edit.

6. In the options menu, select **Edit**.

   The **Edit Access Group** dialog appears.

7. Make any needed changes to the name, associated initiators, or associated volumes.

8. Confirm your changes by selecting **Save**.

9. In the **Access Groups** table, verify that the access group reflects your changes.

Delete a volume access group

You can remove a volume access group by using NetApp Hybrid Cloud Control, and at the same time remove the initiators associated with this access group from the system.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.

3. Select **Volumes**.

4. Select the **Access Groups** tab.

5. In the **Actions** column of the table of access groups, expand the options menu for the access group you need to delete.

6. In the options menu, select **Delete**.

   The **Delete Access Group** dialog appears.

7. If you do not wish to delete the initiators that are associated with the access group, deselect the **Delete initiators in this access group** checkbox.

8. Confirm the delete operation by selecting **Yes**.

Find more information

- Learn about volume access groups
- Work with volume access groups and initiators
- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Create and manage volume QoS policies

A QoS (Quality of Service) policy enables you to create and save a standardized quality of service setting that can be applied to many volumes. The selected cluster must be Element 10.0 or later to use QoS policies; otherwise, QoS policy functions are not available.

> ℹ️ See NetApp HCI Concepts content for more information about using QoS policies instead of individual volume QoS.

Using NetApp Hybrid Cloud Control, you can create and manage QoS policies by completing the following tasks:

- Create a QoS policy
- Apply a QoS policy to a volume
- Change the QoS policy assignment of a volume
- Edit a QoS policy
- Delete a QoS policy

Create a QoS policy

You can create QoS policies and apply them to volumes that should have equivalent performance.

> ℹ️ If you are using QoS policies, do not use custom QoS on a volume. Custom QoS will override and adjust QoS policy values for volume QoS settings.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.
2. From the Dashboard, expand the menu for your storage cluster.
3. Select **Storage** > **Volumes**.
4. Click the **QoS Policies** tab.
5. Click **Create Policy**.

6. Enter the **Policy Name**.

> 💡 Use descriptive naming best practices. This is especially important if multiple clusters or vCenter Servers are used in your environment.

7. Enter the minimum IOPS, maximum IOPS, and burst IOPS values.

8. Click **Create QoS Policy**.

   A system ID is generated for the policy and the policy appears on the QoS Policies page with its assigned QoS values.

Apply a QoS policy to a volume

You can assign an existing QoS policy to a volume using NetApp Hybrid Cloud Control.

What you'll need

The QoS policy you want to assign has been created.

About this task

This task describes how to assign a QoS policy to an individual volume by changing its settings. The latest version of NetApp Hybrid Cloud Control does not have a bulk assign option for more than one volume. Until the functionality to bulk assign is provided in a future release, you can use the Element web UI or vCenter Plug-in UI to bulk assign QoS policies.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the menu for your storage cluster.

3. Select **Storage** > **Volumes**.

4. Click the **Actions** menu next to the volume you intend to modify.

5. In the resulting menu, select **Edit**.

6. In the dialog box, enable **Assign QoS Policy** and select the QoS policy from the drop-down list to apply to the selected volume.

> ℹ️ Assigning QoS will override any individual volume QoS values that have been previously applied.

7. Click **Save**.

   The updated volume with the assigned QoS policy appears on the Overview page.

Change the QoS policy assignment of a volume

You can remove the assignment of a QoS policy from a volume or select a different QoS policy or custom QoS.

What you'll need

The volume you want to modify is assigned a QoS policy.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the menu for your storage cluster.

3. Select **Storage** > **Volumes**.

4. Click the **Actions** menu next to the volume you intend to modify.

5. In the resulting menu, select **Edit**.

6. In the dialog box, do one of the following:

   ◦ Disable **Assign QoS Policy** and modify the **Min IOPS**, **Max IOPS**, and **Burst IOPS** values for individual volume QoS.

   > 🛈 When QoS policies are disabled, the volume uses default QoS IOPS values unless otherwise modified.

   ◦ Select a different QoS policy from the drop-down list to apply to the selected volume.

7. Click **Save**.

   The updated volume appears on the Overview page.

Edit a QoS policy

You can change the name of an existing QoS policy or edit the values associated with the policy. Changing QoS policy performance values affects QoS for all volumes associated with the policy.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the menu for your storage cluster.

3. Select **Storage** > **Volumes**.

4. Click the **QoS Policies** tab.

5. Click the **Actions** menu next to the QoS policy you intend to modify.

6. Click **Edit**.

7. In the **Edit QoS Policy** dialog box, change one or more of the following:

   ◦ **Name**: The user-defined name for the QoS policy.

   ◦ **Min IOPS**: The minimum number of IOPS guaranteed for the volume. Default = 50.

   ◦ **Max IOPS**: The maximum number of IOPS allowed for the volume. Default = 15,000.

   ◦ **Burst IOPS**: The maximum number of IOPS allowed over a short period of time for the volume. Default = 15,000.

8. Click **Save**.

   The updated QoS policy appears on the QoS Policies page.

   > 💡 You can click on the link in the **Active Volumes** column for a policy to show a filtered list of the volumes assigned to that policy.

Delete a QoS policy

You can delete a QoS policy if it is no longer needed. When you delete a QoS policy, all volumes assigned with the policy maintain the QoS values previously defined by the policy but as individual volume QoS. Any association with the deleted QoS policy is removed.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

2. From the Dashboard, expand the menu for your storage cluster.

3. Select **Storage** > **Volumes**.

4. Click the **QoS Policies** tab.

5. Click the **Actions** menu next to the QoS policy you intend to modify.

6. Click **Delete**.

7. Confirm the action.

Find more information

- NetApp HCI Documentation Center
- NetApp SolidFire and Element Documentation Center (Documentation Center Versions)

Work with the management node

Management node overview

You can use the management node (mNode) to upgrade system services, manage

cluster assets and settings, run system tests and utilities, configure Active IQ for system monitoring, and enable NetApp Support access for troubleshooting.

For clusters running Element software version 11.3 or later, you can work with the management node by using one of two interfaces:

- With the management node UI (`https:// [mNode IP}:442`), you can make changes to network and cluster settings, run system tests, or use system utilities.

- With the built-in REST API UI (`https://[mNode IP}/mnode`), you can run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or asset management.

Install or recover a management node:

- Install a management node

- Configure a storage Network Interface Controller (NIC)

- Recover a management node

Access the management node:

- Access the management node (UI or REST API)

Tasks you can perform with the management node UI:

- Configure alert monitoring on NetApp HCI

- Modify and test the management node network, cluster, and system settings

- Run system utilities from the management node

Tasks you can perform with the management node REST APIs:

- Get authorization to use REST APIs

- Enable Active IQ and NetApp HCI monitoring

- Add compute and controller assets to the management node

- Create and manage storage cluster assets

- View or edit existing controller assets

- Configure a proxy server for the management node

- Use the REST API to collect NetApp HCI logs

Enable remote NetApp Support connections to help you troubleshoot:

- Enable remote NetApp Support connections

Find more information

- NetApp HCI Documentation Center

- NetApp HCI Resources Page

Install or recover a management node

Install a management node

You can manually install the management node for your cluster running NetApp Element software using the appropriate image for your configuration.

This manual process is intended for SolidFire all-flash storage administrators and NetApp HCI administrators who are not using the NetApp Deployment Engine for management node installation.

What you'll need

- Your cluster version is running NetApp Element software 11.3 or later.

- Your installation uses IPv4. The management node 11.3 does not support IPv6.

    > If you need to IPv6 support, you can use the management node 11.1.

- You have permission to download software from the NetApp Support Site.

- You have identified the management node image type that is correct for your platform:

Platform	Installation image type
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

- (Management node 12.0 and 12.2 with proxy server) You have updated NetApp Hybrid Cloud Control to management services version 2.16 before configuring a proxy server.

About this task

The Element 12.2 management node is an optional upgrade. It is not required for existing deployments.

Prior to following this procedure, you should have an understanding of persistent volumes and whether or not you want to use them. Persistent volumes are optional but recommended for management node configuration data recovery in the event of a VM loss.

Steps

1. Download ISO or OVA and deploy the VM

2. [Create the management node admin and configure the network](#)

3. [Configure the management node](#)

4. [Configure controller assets](#)

5. [(NetApp HCI only) Configure compute node assets](#)

Download ISO or OVA and deploy the VM

1. Download the OVA or ISO for your installation from the NetApp Support Site:

   Element software: https://mysupport.netapp.com/site/products/all/details/element-software/downloads-tab
   NetApp HCI: https://mysupport.netapp.com/site/products/all/details/netapp-hci/downloads-tab

   a. Click **Download Latest Release** and accept the EULA.

   b. Select the management node image you want to download.

2. If you downloaded the OVA, follow these steps:

   a. Deploy the OVA.

   b. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (for example, eth1) or ensure that the management network can route to the storage network.

3. If you downloaded the ISO, follow these steps:

   a. Create a new 64-bit virtual machine from your hypervisor with the following configuration:

      - Six virtual CPUs

      - 24GB RAM

      - 400GB virtual disk, thin provisioned

      - One virtual network interface with internet access and access to the storage MVIP.

      - (Optional for SolidFire all-flash storage) One virtual network interface with management network access to the storage cluster. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (eth1) or ensure that the management network can route to the storage network.

      > **!** Do not power on the virtual machine prior to the step indicating to do so later in this procedure.

   b. Attach the ISO to the virtual machine and boot to the .iso install image.

      > **i** Installing a management node using the image might result in 30-second delay before the splash screen appears.

4. Power on the virtual machine for the management node after the installation completes.

Create the management node admin and configure the network

1. Using the terminal user interface (TUI), create a management node admin user.

> 💡 To move through the menu options, press the Up or Down arrow keys. To move through the buttons, press Tab. To move from the buttons to the fields, press Tab. To navigate between fields, press the Up or Down arrow keys.

2. Configure the management node network (eth0).

> ℹ️ If you need an additional NIC to isolate storage traffic, see instructions on configuring another NIC: Configure a storage Network Interface Controller (NIC).

Configure the management node

1. SSH into the management node.

2. Using SSH, run the following command to gain root privileges. Enter your password when prompted:

```
sudo su
```

3. Ensure time is synced between the management node and the storage cluster using NTP:

    a. Edit the `/etc/ntp.conf` file.

    b. Change the default time server(s) to the same NTP server used on the storage cluster.

    c. In vSphere, verify that the **Synchronize guest time with host** box is un-checked in the VM options.

    > ℹ️ Do not enable this option if you make future changes to the VM.

4. Configure and run the management node setup command:

    > ℹ️ You will be prompted to enter passwords in a secure prompt. If your cluster is behind a proxy server, you must configure the proxy settings so you can reach a public network.

```
/sf/packages/mnode/setup-mnode --mnode_admin_user [username] --storage_mvip [mvip]
--storage_username [username] --telemetry_active [true]
```

    a. Replace the value in [ ] brackets (including the brackets) for each of the following required

parameters:

> **i** The abbreviated form of the command name is in parentheses ( ) and can be substituted for the full name.

- **--mnode_admin_user (-mu) [username]**: The username for the management node administrator account. This is likely to be the username for the user account you used to log into the management node.

- **--storage_mvip (-sm) [MVIP address]**: The management virtual IP address (MVIP) of the storage cluster running Element software.

- **--storage_username (-su) [username]**: The storage cluster administrator username for the cluster specified by the `--storage_mvip` parameter.

- **--telemetry_active (-t) [true]**: Retain the value true that enables data collection for analytics by Active IQ.

b. (Optional): Add Active IQ endpoint parameters to the command:

- **--remote_host (-rh) [AIQ_endpoint]**: The endpoint where Active IQ telemetry data is sent to be processed. If the parameter is not included, the default endpoint is used.

c. (Recommended): Add the following persistent volume parameters. Do not modify or delete the account and volumes created for persistent volumes functionality or a loss in management capability will result.

- **--use_persistent_volumes (-pv) [true/false, default: false]**: Enable or disable persistent volumes. Enter the value true to enable persistent volumes functionality.

- **--persistent_volumes_account (-pva) [account_name]**: If `--use_persistent_volumes` is set to true, use this parameter and enter the storage account name that will be used for persistent volumes.

> **i** Use a unique account name for persistent volumes that is different from any existing account name on the cluster. It is critically important to keep the account for persistent volumes separate from the rest of your environment.

- **--persistent_volumes_mvip (-pvm) [mvip]**: Enter the management virtual IP address (MVIP) of the storage cluster running Element software that will be used with persistent volumes. This is only required if multiple storage clusters are managed by the management node. If multiple clusters are not managed, the default cluster MVIP will be used.

d. Configure a proxy server:

- **--use_proxy (-up) [true/false, default: false]**: Enable or disable the use of the proxy. This parameter is required to configure a proxy server.

- **--proxy_hostname_or_ip (-pi) [host]**: The proxy hostname or IP. This is required if you want to use a proxy. If you specify this, you will be prompted to input `--proxy_port`.

- **--proxy_username (-pu) [username]**: The proxy username. This parameter is optional.

- **--proxy_password (-pp) [password]**: The proxy password. This parameter is optional.

- **--proxy_port (-pq) [port, default: 0]**: The proxy port. If you specify this, you will be prompted to input the proxy host name or IP (`--proxy_hostname_or_ip`).

- **--proxy_ssh_port (-ps) [port, default: 443]**: The SSH proxy port. This defaults to port 443.

e. (Optional) Use parameter help if you need additional information about each parameter:

- **--help (-h)**: Returns information about each parameter. Parameters are defined as required or optional based on initial deployment. Upgrade and redeployment parameter requirements might vary.

f. Run the `setup-mnode` command.

Configure controller assets

1. Locate the installation ID:

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

   b. Go to the storage MVIP and log in. This action causes the certificate to be accepted for the next step.

   c. Open the inventory service REST API UI on the management node:

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

   d. 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.

   e. From the REST API UI, click **GET /installations**.

   f. Click **Try it out**.

   g. Click **Execute**.

   h. From the code 200 response body, copy and save the `id` for the installation for use in a later step.

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

2. (NetApp HCI only) Locate the hardware tag for your compute node in vSphere:

   a. Select the host in the vSphere Web Client navigator.

   b. Click the **Monitor** tab, and click **Hardware Health**.

   c. The node BIOS manufacturer and model number are listed. Copy and save the value for `tag` for

use in a later step.

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

   a. Access the mnode service API UI on the management node by entering the management node IP address followed by `/mnode`:

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

   b. 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`.

      iii. Click **Authorize** to begin a session.

      iv. Close the window.

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

   d. Click **Try it out**.

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

   f. Enter the required payload values with type `vCenter` and vCenter credentials.

   g. Click **Execute**.

(NetApp HCI only) Configure compute node assets

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

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

   b. Click **Try it out**.

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

   d. In the payload, enter the required payload values as defined in the Model tab. Enter `ESXi Host` as `type` and enter the hardware tag you saved during a previous step for `hardware_tag`.

   e. Click **Execute**.

Find more Information

- Persistent volumes
- Add an asset to the management node
- Configure a storage NIC
- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Configure a storage Network Interface Controller (NIC)

If you are using an additional NIC for storage, you can SSH in to the management node or use the vCenter console and run a curl command to set up that network interface.

Before you begin

- You know your eth0 IP address.

- Your cluster version is running NetApp Element software 11.3 or later.

- You have deployed a management node 11.3 or later.

Steps

1. Open an SSH or vCenter console.

2. Replace the values in the following command template and run the command:

   > Values are represented by `$` for each of the required parameters for your new storage network interface. The `cluster` object in the following template is required and can be used for management node host name renaming. The `--insecure` or `-k` options should not be used in production environments.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
    "params": {
            "network": {
                    "$eth1": {
                            "#default" : false,
                            "address" : "$storage_IP",
                            "auto" : true,
                            "family" : "inet",
                            "method" : "static",
                            "mtu" : "9000",
                            "netmask" : "$subnet_mask",
                            "status" : "Up"
                            }
                    },
            "cluster": {
                    "name": "$mnode_host_name"
                    }
        },
    "method": "SetConfig"
}
'
```

Find more Information

- [Add an asset to the management node](#)
- [NetApp HCI Documentation Center](#)
- [NetApp HCI Resources Page](#)

Recover a management node

You can manually recover and redeploy the management node for your cluster running NetApp Element software if your previous management node used persistent volumes.

You can deploy a new OVA and run a redeploy script to pull configuration data from a previously installed management node running version 11.3 and later.

What you'll need

- Your previous management node was running NetApp Element software version 11.3 or later with [persistent volumes](#) functionality engaged.

- You know the MVIP and SVIP of the cluster containing the persistent volumes.

- Your cluster version is running NetApp Element software 11.3 or later.

- Your installation uses IPv4. The management node 11.3 does not support IPv6.

- You have permission to download software from the NetApp Support Site.

- You have identified the management node image type that is correct for your platform:

Platform	Installation image type
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

Steps

1. Download ISO or OVA and deploy the VM

2. Configure the network

3. Configure the management node

Download ISO or OVA and deploy the VM

1. Download the OVA or ISO for your installation from the NetApp Support Site:

   Element software: https://mysupport.netapp.com/site/products/all/details/element-software/downloads-tab
   NetApp HCI: https://mysupport.netapp.com/site/products/all/details/netapp-hci/downloads-tab

   a. Click **Download Latest Release** and accept the EULA.

   b. Select the management node image you want to download.

2. If you downloaded the OVA, follow these steps:

   a. Deploy the OVA.

   b. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (for example, eth1) or ensure that the management network can route to the storage network.

3. If you downloaded the ISO, follow these steps:

   a. Create a new 64-bit virtual machine from your hypervisor with the following configuration:

      - Six virtual CPUs

      - 24GB RAM

- 400GB virtual disk, thin provisioned

- One virtual network interface with internet access and access to the storage MVIP.

- (Optional for SolidFire all-flash storage) One virtual network interface with management network access to the storage cluster. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (eth1) or ensure that the management network can route to the storage network.

> **!** Do not power on the virtual machine prior to the step indicating to do so later in this procedure.

b. Attach the ISO to the virtual machine and boot to the .iso install image.

> **i** Installing a management node using the image might result in 30-second delay before the splash screen appears.

4. Power on the virtual machine for the management node after the installation completes.

Configure the network

1. Using the terminal user interface (TUI), create a management node admin user.

> **♡** To move through the menu options, press the Up or Down arrow keys. To move through the buttons, press Tab. To move from the buttons to the fields, press Tab. To navigate between fields, press the Up or Down arrow keys.

2. Configure the management node network (eth0).

> **i** If you need an additional NIC to isolate storage traffic, see instructions on configuring another NIC: Configure a storage Network Interface Controller (NIC).

Configure the management node

1. Log in to the management node using SSH or the console provided by your hypervisor.

2. Run the following command to gain root privileges. Enter your password when prompted:

```
sudo su
```

3. Ensure time is synced between the management node and the storage cluster using NTP:

   a. Edit the `/etc/ntp.conf` file.

   b. Change the default time server(s) to the same NTP server used on the storage cluster.

c. In vSphere, verify that the **Synchronize guest time with host** box is un-checked in the VM options.

> 🛈 Do not enable this option if you make future changes to the VM.

4. Create a temporary destination directory for the management services bundle contents:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

5. Download the management services bundle (version 2.15.28 or later) that was previously installed on the existing management node and save it in the /sf/etc/mnode/ directory.

6. Extract the downloaded bundle using the following command, replacing the value in [ ] brackets (including the brackets) with the name of the bundle file:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle file]
```

7. Extract the resulting file to the /sf/etc/mnode-archive directory:

```
tar -C /sf/etc/mnode/mnode-archive -xvf /sf/etc/mnode/services_deploy_bundle.tar.gz
```

8. Create a configuration file for accounts and volumes:

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name": "[persistent
volume account name]"}' | sudo tee /sf/etc/mnode/mnode-archive/management-services-
metadata.json
```

a. Replace the value in [ ] brackets (including the brackets) for each of the following required parameters:

- **[mvip IP address]**: The management virtual IP address of the storage cluster.

- **[persistent volume account name]**: The name of the account associated with all persistent volumes in this storage cluster.

9. Configure and run the management node redeploy command to connect to persistent volumes hosted on the cluster and start services with previous management node configuration data:

> 🛈 You will be prompted to enter passwords in a secure prompt. If your cluster is behind a proxy server, you must configure the proxy settings so you can reach a public network.

```
/sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

a. Replace the value in [ ] brackets (including the brackets) with the user name for the management node administrator account. This is likely to be the username for the user account you used to log into the management node.

> **ℹ** You can add the user name or allow the script to prompt you for the information.

b. Run the `redeploy-mnode` command. The script displays a success message when the redeployment is complete.

c. If you access Element or NetApp HCI web interfaces (such as the management node or NetApp Hybrid Cloud Control) using the Fully Qualified Domain Name (FQDN) of the system, reconfigure authentication for the management node.

Find more Information

- Persistent volumes
- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Access the management node

Beginning with NetApp Element software version 11.3, the management node contains two UIs: a UI for managing REST-based services and a per-node UI for managing network and cluster settings and operating system tests and utilities.

For clusters running Element software version 11.3 or later, you can make use one of two interfaces:
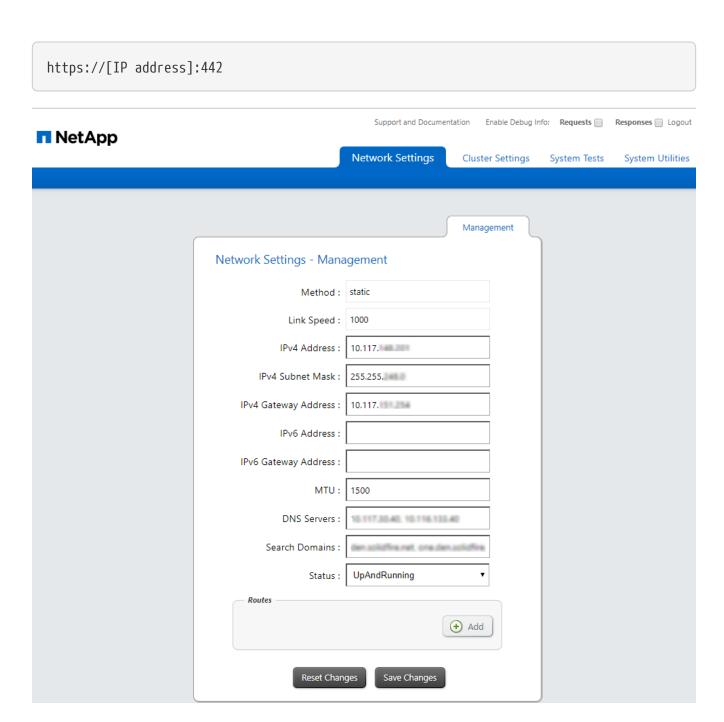
- By using the management node UI (`https:// [mNode IP}:442`), you can make changes to network and cluster settings, run system tests, or use system utilities.

- By using the built-in REST API UI (`https://[mNode IP}/mnode`), you can run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or asset management.

Access the management node per-node UI

From the per-node UI, you can access network and cluster settings and utilize system tests and utilities.

Steps

1. Access the per-node UI for the management node by entering the management node IP address followed by :442
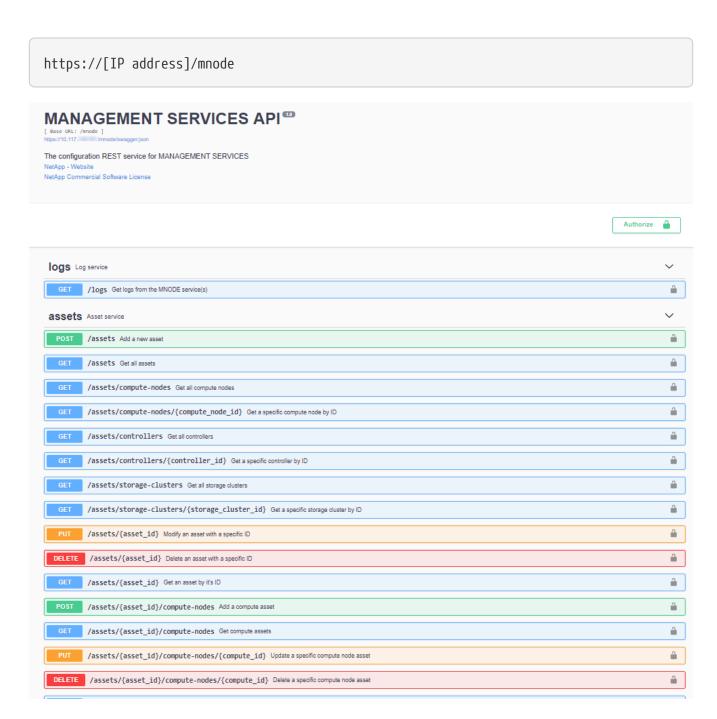
```
https://[IP address]:442
```


2. Enter the management node user name and password when prompted.

Access the management node REST API UI

From the REST API UI, you can access a menu of service-related APIs that control management services on the management node.

Steps

1. To access the REST API UI for management services, enter the management node IP address followed by /mnode:

```
https://[IP address]/mnode
```


MANAGEMENT SERVICES API 1.0

[Base URL: /mnode]
https://10.117.____/mnode/swagger.json

The configuration REST service for MANAGEMENT SERVICES

NetApp - Website
NetApp Commercial Software License

Authorize 🔒

logs Log service ⌄

| GET | /logs | Get logs from the MNODE service(s) | 🔒 |

assets Asset service ⌄

POST	/assets	Add a new asset	🔒
GET	/assets	Get all assets	🔒
GET	/assets/compute-nodes	Get all compute nodes	🔒
GET	/assets/compute-nodes/{compute_node_id}	Get a specific compute node by ID	🔒
GET	/assets/controllers	Get all controllers	🔒
GET	/assets/controllers/{controller_id}	Get a specific controller by ID	🔒
GET	/assets/storage-clusters	Get all storage clusters	🔒
GET	/assets/storage-clusters/{storage_cluster_id}	Get a specific storage cluster by ID	🔒
PUT	/assets/{asset_id}	Modify an asset with a specific ID	🔒
DELETE	/assets/{asset_id}	Delete an asset with a specific ID	🔒
GET	/assets/{asset_id}	Get an asset by it's ID	🔒
POST	/assets/{asset_id}/compute-nodes	Add a compute asset	🔒
GET	/assets/{asset_id}/compute-nodes	Get compute assets	🔒
PUT	/assets/{asset_id}/compute-nodes/{compute_id}	Update a specific compute node asset	🔒
DELETE	/assets/{asset_id}/compute-nodes/{compute_id}	Delete a specific compute node asset	🔒

2. Click **Authorize** or any lock icon and enter cluster admin credentials for permissions to use APIs.

Find more Information

- Enable the Active IQ collector service for SolidFire all-flash storage
- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Work with the management node UI

Management node UI overview

With the management node UI (`https://[management node IP]:442`), you can make changes to network and cluster settings, run system tests, or use system utilities.

Tasks you can perform with the management node UI:

- Configure alert monitoring on NetApp HCI
- Modify and test the management node network, cluster, and system settings
- Run system utilities from the management node

Find more information

- Access the management node
- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Configure alert monitoring on NetApp HCI

You can configure settings to monitor alerts on your NetApp HCI system.

NetApp HCI alert monitoring forwards NetApp HCI storage cluster system alerts to vCenter Server, enabling you to view all alerts for NetApp HCI from the vSphere Web Client interface.

> ℹ️ These tools are not configured or used for storage-only clusters, such as SolidFire all-flash storage. Running the tools for these clusters results in the following 405 error, which is expected given the configuration: `webUIParseError : Invalid response from server. 405`

1. Open the per-node management node UI (`https://[IP address]:442`).
2. Click the **Alert Monitor** tab.
3. Configure the alert monitoring options.

Alert monitoring options

options	Description
Run Alert Monitor Tests	Runs the monitor system tests to check for the following: • NetApp HCI and VMware vCenter connectivity • Pairing of NetApp HCI and VMware vCenter through datastore information supplied by the QoSSIOC service • Current NetApp HCI alarm and vCenter alarm lists
Collect Alerts	Enables or disables the forwarding of NetApp HCI storage alarms to vCenter. You can select the target storage cluster from the drop-down list. The default setting for this option is `Enabled`.
Collect Best Practice Alerts	Enables or disables the forwarding of NetApp HCI storage Best Practice alerts to vCenter. Best Practice alerts are faults that are triggered by a sub-optimal system configuration. The default setting for this option is `Disabled`. When disabled, NetApp HCI storage Best Practice alerts do not appear in vCenter.

options	Description
Send Support Data To AIQ	Controls the flow of support and monitoring data from VMware vCenter to NetApp SolidFire Active IQ. Options are the following: • Enabled: All vCenter alarms, NetApp HCI storage alarms, and support data are sent to NetApp SolidFire Active IQ. This enables NetApp to proactively support and monitor the NetApp HCI installation, so that possible problems can be detected and resolved before affecting the system. • Disabled: No vCenter alarms, NetApp HCI storage alarms, or support data are sent to NetApp SolidFire Active IQ. ⓘ If you turned off the **Send data to AIQ** option using NetApp Deployment Engine, you need to enable telemetry again using the management node REST API to configure the service from this page.

options	Description
Send Compute Node Data To AIQ	Controls the flow of support and monitoring data from the compute nodes to NetApp SolidFire Active IQ. Options are the following: • Enabled: Support and monitoring data about the compute nodes is transmitted to NetApp SolidFire Active IQ to enable proactive support for the compute node hardware. • Disabled: Support and monitoring data about the compute nodes is not transmitted to NetApp SolidFire Active IQ. ℹ️ If you turned off the **Send data to AIQ** option using NetApp Deployment Engine, you need to enable telemetry again using the management node REST API to configure the service from this page.

Find more Information

- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Work with the management node REST API

Management node REST API UI overview

By using the built-in REST API UI (`https://[mNode IP}/mnode`), you can run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or asset management.

Tasks you can perform with REST APIs:

- Get authorization to use REST APIs
- Enable Active IQ and NetApp HCI monitoring
- Add compute and controller assets to the management node
- Create and manage storage cluster assets

- View or edit existing controller assets

- Configure a proxy server for the management node

- Use the REST API to collect NetApp HCI logs

Find more information

- Access the management node

- NetApp HCI Documentation Center

- NetApp HCI Resources Page

Get authorization to use REST APIs

You must authorize before you can use APIs for management services in the REST API UI. You do this by obtaining an access token.

To obtain a token, you provide cluster admin credentials and a client ID. Each token lasts approximately ten minutes. After a token expires, you can authorize again for a new access token.

Authorization functionality is set up for you during management node installation and deployment. The token service is based on the storage cluster you defined during setup.

Before you begin
- Your cluster version should be running NetApp Element software 11.3 or later.

- You should have deployed a management node running version 11.3 or later.

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

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

2. Click **Authorize**.

   > Alternately, you can click on a lock icon next to any service API.

3. Complete the following:

   a. Enter the cluster user name and password.

   b. Select **Request body** from the Type drop-down list.

   c. Enter the client ID as `mnode-client`.

   d. Do not enter a value for the client secret.

   e. Click **Authorize** to begin a session.

> **ℹ** If the error message `Auth Error TypeError: Failed to fetch` is returned after you attempt to authorize, you might need to accept the SSL certificate for the MVIP of your cluster. Copy the IP in the Token URL, paste the IP into another browser tab, and authorize again.

The Available authorizations screen indicates **Authorized**.

4. Close the Available authorizations dialog box.

> **ℹ** If you try to run a command after the token expires, a `401 Error: UNAUTHORIZED` message appears. If you see this, authorize again.

Find more information

- NetApp HCI Documentation Center
- NetApp HCI Resources Page

Configure a proxy server

If your cluster is behind a proxy server, you must configure the proxy settings so that you can reach a public network.

A proxy server is used for telemetry collectors and reverse tunnel connections. You can enable and configure a proxy server using the REST API UI if you did not already configure a proxy server during installation or upgrade. You can also modify existing proxy server settings or disable a proxy server.

The command to configure a proxy server updates and then returns the current proxy settings for the management node. The proxy settings are used by Active IQ, the NetApp HCI monitoring service that is deployed by the NetApp Deployment Engine, and other Element software utilities that are installed on the management node, including the reverse support tunnel for NetApp Support.

Before you begin

- You should know host and credential information for the proxy server you are configuring.
- Ensure that your cluster version is running NetApp Element software 11.3 or later.
- Ensure that you have deployed a management node running version 11.3 or later.
- (Management node 12.0 and 12.2) You have updated NetApp Hybrid Cloud Control to management services version 2.16 before configuring a proxy server.

Steps

1. Access the REST API UI on the management node by entering the management node IP address followed by `/mnode`:

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

2. Click **Authorize** or any lock icon and complete the following:

   a. Enter the cluster user name and password.

   b. Enter the client ID as `mnode-client`.

   c. Click **Authorize** to begin a session.

   d. Close the window.

3. Click **PUT /settings**.

4. Click **Try it out**.

5. To enable a proxy server, you must set `use_proxy` to true. Enter the IP or host name and proxy port destinations.

   The proxy user name, proxy password, and SSH port are optional and should be omitted if not used.

```
{
"proxy_ip_or_hostname": "[IP or name]",
"use_proxy": [true/false],
"proxy_username": "[username]",
"proxy_password": "[password]",
"proxy_port": [port value],
"proxy_ssh_port": [port value: default is 443]
}
```

6. Click **Execute**.

Find more information

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

Create and manage storage cluster assets

You can add new storage cluster assets to the management node, edit the stored credentials for known storage cluster assets, and delete storage cluster assets from the management node using the REST API.

What you'll need

- Ensure that your storage cluster version is running NetApp Element software 11.3 or later.
- Ensure that you have deployed a management node running version 11.3 or later.

Storage cluster asset management options

Choose one of the following options:

- Retrieve the installation ID and cluster ID of a storage cluster asset
- Add a new storage cluster asset
- Edit the stored credentials for a storage cluster asset
- Delete a storage cluster asset

Retrieve the installation ID and cluster ID of a storage cluster asset

You can use the REST API get the installation ID and the ID of the storage cluster. You need the installation ID to add a new storage cluster asset, and the cluster ID to modify or delete a specific storage cluster asset.

Steps

1. Access the REST API UI for the inventory service by entering the management node IP address followed by `/inventory/1/`:

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

2. Click **Authorize** or any lock icon and complete the following:

   a. Enter the cluster user name and password.

   b. Enter the client ID as `mnode-client`.

   c. Click **Authorize** to begin a session.

   d. Close the window.

3. Click **GET /installations**.

4. Click **Try it out**.

5. Click **Execute**.

   The API returns a list of all known installations.

6. From the code 200 response body, save the value in the `id` field, which you can find in the list of installations. This is the installation ID. For example:

```
"installations": [
    {
      "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",
      "name": "my-hci-installation",
      "_links": {
        "collection": "https://localhost/inventory/1/installations",
        "self": "https://localhost/inventory/1/installations/1234a678-12ab-35dc-7b4a-
1234a5b6a7ba"
      }
    }
  ]
```

7. Access the REST API UI for the storage service by entering the management node IP address followed by `/storage/1/`:

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

8. Click **Authorize** or any lock icon and complete the following:

   a. Enter the cluster user name and password.

   b. Enter the client ID as `mnode-client`.

   c. Click **Authorize** to begin a session.

   d. Close the window.

9. Click **GET /clusters**.

10. Click **Try it out**.

11. Enter the installation ID you saved earlier into the `installationId` parameter.

12. Click **Execute**.

    The API returns a list of all known storage clusters in this installation.

13. From the code 200 response body, find the correct storage cluster and save the value in the cluster's `storageId` field. This is the storage cluster ID.

Add a new storage cluster asset

You can use the REST API to add one or more new storage cluster assets to the management node inventory. When you add a new storage cluster asset, it is automatically registered with the management node.

What you'll need

- You have copied the storage cluster ID and installation ID for any storage clusters you want to add.

- If you are adding more than one storage node, you have read and understood the limitations of the

[authorative cluster](#) and multiple storage cluster support.

> ℹ️ All users defined on the authoritative cluster are defined as users on all other clusters tied to the Hybrid Cloud Control instance.

Steps

1. Access the REST API UI for the storage service by entering the management node IP address followed by `/storage/1/`:

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

2. Click **Authorize** or any lock icon and complete the following:

   a. Enter the cluster user name and password.

   b. Enter the client ID as `mnode-client`.

   c. Click **Authorize** to begin a session.

   d. Close the window.

3. Click **POST /clusters**.

4. Click **Try it out**.

5. Enter the new storage cluster's information in the following parameters in the **Request body** field:

   ```
   {
      "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
      "mvip": "10.0.0.1",
      "password": "admin",
      "userId": "admin"
   }
   ```

Parameter	Type	Description
`installationId`	string	The installation in which to add the new storage cluster. Enter the installation ID you saved earlier into this parameter.
`mvip`	string	The IPv4 management virtual IP address (MVIP) of the storage cluster.
`password`	string	The password used to communicate with the storage cluster.

Parameter	Type	Description
userId	string	The user ID used to communicate with the storage cluster (the user must have administrator privileges).

6. Click **Execute**.

   The API returns an object containing information about the newly added storage cluster asset, such as the name, version, and IP address information.

Edit the stored credentials for a storage cluster asset

You can edit the stored credentials that the management node uses to log in to a storage cluster. The user you choose must have cluster admin access.

> **i** Ensure you have followed the steps in Retrieve the installation ID and cluster ID of a storage cluster asset before continuing.

Steps

1. Access the REST API UI for the storage service by entering the management node IP address followed by `/storage/1/`:

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

2. Click **Authorize** or any lock icon and complete the following:

   a. Enter the cluster user name and password.

   b. Enter the client ID as `mnode-client`.

   c. Click **Authorize** to begin a session.

   d. Close the window.

3. Click **PUT /clusters/{storageId}**.

4. Click **Try it out**.

5. Paste the storage cluster ID you copied earlier into the `storageId` parameter.

6. Change one or both of the following parameters in the **Request body** field:

   ```
   {
      "password": "adminadmin",
      "userId": "admin"
   }
   ```

Parameter	Type	Description
password	string	The password used to communicate with the storage cluster.
userId	string	The user ID used to communicate with the storage cluster (the user must have administrator privileges).

7. Click **Execute**.

Delete a storage cluster asset

You can delete a storage cluster asset if the storage cluster is no longer in service. When you remove a storage cluster asset, it is automatically unregistered from the management node.

> ℹ️ Ensure you have followed the steps in Retrieve the installation ID and cluster ID of a storage cluster asset before continuing.

Steps

1. Access the REST API UI for the storage service by entering the management node IP address followed by `/storage/1/`:

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

2. Click **Authorize** or any lock icon and complete the following:

   a. Enter the cluster user name and password.

   b. Enter the client ID as `mnode-client`.

   c. Click **Authorize** to begin a session.

   d. Close the window.

3. Click **DELETE /clusters/{storageId}**.

4. Click **Try it out**.

5. Enter the storage cluster ID you copied earlier in the `storageId` parameter.

6. Click **Execute**.

   Upon success, the API returns an empty response.

Find more information

- Authoritative cluster

-

-

Enable remote NetApp Support connections

If you require technical support for your NetApp Element software-based storage system, NetApp Support can connect remotely with your system if you enable remote access. To gain remote access, NetApp Support can open a reverse Secure Shell (SSH) connection to your environment.

About this task

You can open a TCP port for an SSH reverse tunnel connection with NetApp Support. This connection enables NetApp Support to log in to your management node. If your management node is behind a proxy server, the following TCP ports are required in the sshd.config file:

TCP port	Description	Connection direction
443	API calls/HTTPS for reverse port forwarding via open support tunnel to the web UI	Management node to storage nodes
22	SSH login access	Management node to storage nodes or from storage nodes to management node

Steps

- Log in to your management node and open a terminal session.

- At a prompt, enter the following:

  ```
  rst -r sfsupport.solidfire.com -u element -p <port_number>
  ```

- To close the remote support tunnel, enter the following:

  ```
  rst --killall
  ```

Find more information

-

-

Power your NetApp HCI system off or on

Powering your NetApp HCI system off or on

You can power off or power on your NetApp HCI system if you have a scheduled outage, need to perform hardware maintenance, or need to expand the system. Use the following tasks to power off or power on your NetApp HCI system as required.

You might need to power off your NetApp HCI system under a number of different circumstances, such as:

- Scheduled outages
- Chassis fan replacements
- Firmware upgrades
- Storage or compute resource expansion

The following is an overview of the tasks you need to complete to power off a NetApp HCI system:

- Power off all virtual machines except the VMware vCenter server (vCSA).
- Power off all ESXi servers except the one hosting the vCSA.
- Power off the vCSA.
- Power off the NetApp HCI storage system.

The following is an overview of the tasks you need to complete to power on a NetApp HCI system:

- Power on all physical storage nodes.
- Power on all physical compute nodes.
- Power on the vCSA.
- Verify the system and power on additional virtual machines.

Find more information

- [Firmware and driver versions in NetApp HCI and NetApp Element software](#)

Power off compute resources for a NetApp HCI system

To power off NetApp HCI compute resources, you need to power off individual VMware ESXi hosts as well as the VMware vCenter Server Appliance in a certain order.

Steps

1. Log in to the vCenter instance controlling the NetApp HCI system and determine the ESXi machine hosting the vCenter Server Virtual Appliance (vCSA).

2. After you have determined the ESXi host running the vCSA, power down all other virtual machines other than the vCSA as follows:

   a. Select a virtual machine.

   b. Right-click and select **Power** > **Shut Down Guest OS**.

3. Power off all ESXi hosts that are not the ESXi host running the vCSA.

4. Power off the vCSA.

   This will cause the vCenter session to end because the vCSA disconnects during the power-off process. All virtual machines should now be shut down with only one ESXi host powered on.

5. Log in to the running ESXi host.

6. Verify that all virtual machines on the host are powered off.

7. Shut down the ESXi host.

   This disconnects any iSCSI sessions open to the NetApp HCI storage cluster.

Find more information

- [Firmware and driver versions in NetApp HCI and NetApp Element software](#)

Power off storage resources for a NetApp HCI system

When you power off storage resources for NetApp HCI, you need to use the `Shutdown` Element API method to properly halt the storage nodes.

Steps

After you power off the compute resources, you use a web browser to shut down all the nodes of the NetApp HCI storage cluster.

1. Log in to the storage cluster and verify that you are connected to the correct MVIP.

2. Verify that the iSCSI session count is zero.

3. Navigate to **Cluster** > **Nodes** > **Active**, and record the node IDs for all of the active nodes in the cluster.

4. To power off the NetApp HCI storage cluster, open a web browser and use the following URL to invoke the power off and halt procedure, where `{MVIP}` is the management IP address of the NetApp HCI storage system and the `nodes=[]` array includes the node IDs that you recorded in step 2. For example:

   ```
   https://{MVIP}/json-rpc/1.0?method=Shutdown&nodes=[1,2,3,4]&option=halt
   ```

5. Enter the cluster administrator user name and password.

6. Validate that the API call returned successfully by verifying that all storage cluster nodes are included in the `successful` section of the API result.

You have successfully powered off all the NetApp HCI storage nodes.

Find more information

- [Firmware and driver versions in NetApp HCI and NetApp Element software](#)

Power on storage resources for a NetApp HCI system

You can power on NetApp HCI after the scheduled outage is complete.

Steps

1. Power on all the storage nodes using either the physical power button or the BMC.

2. If using the BMC, log in to each node and navigate to **Remote Control** > **Power Control** > **Power On Server**.

3. When all the storage nodes are online, log in to the NetApp HCI storage system and verify that all nodes are operational.

Find more information

- [Firmware and driver versions in NetApp HCI and NetApp Element software](#)

Power on compute resources for a NetApp HCI system

You can power on compute resources for a NetApp HCI system after the scheduled outage is complete.

Steps

1. Power on compute nodes using the same steps you performed for powering on the storage nodes.

2. When all the compute nodes are operational, log in to the ESXi host that was running the vCSA.

3. Log in to the compute host and verify that it sees all the NetApp HCI datastores. For a typical NetApp HCI system, you should see all the ESXi local datastores and at least the following shared datastores:

```
NetApp-HCI-Datastore-[01,02]
```

1. Assuming all storage is accessible, power on the vCSA and any other required virtual machines as follows:

   a. Select the virtual machines in the navigator, select all the virtual machines that you want to power on, and click the **Power on** button.

2. After you power on the virtual machines, wait for approximately 5 minutes and then use a web browser to navigate to the IP address or FQDN of the vCSA applicance.

   If you do not wait long enough, a message appears stating that the vSphere Client web server is initializing.

3. After the vSphere Client initializes, log in and verify that all ESXi hosts and virtual machines are online.

Find more information

- Firmware and driver versions in NetApp HCI and NetApp Element software