Manage NetApp HCI

HCI

NetApp
February 24, 2021

Table of Contents

Manage NetApp HCI

NetApp HCI management overview

You can manage credentials for NetApp HCI, user accounts, storage clusters, volumes, volume access groups, initiators, volume QoS policies and the management node.

Here are the items you can work with:

- Update vCenter and ESXi credentials
- Manage NetApp HCI storage assets
- Work with the management node
- Power your NetApp HCI system off or on

Find more information

- NetApp HCI Resources page

Update vCenter and ESXi credentials

To maintain full functionality of NetApp Hybrid Cloud Control for your NetApp HCI installation, when you change your credentials in vCenter and ESXi hosts, you also need to update those credentials in the asset service on the management node.

About this task

NetApp Hybrid Cloud Control communicates with vCenter and the individual compute nodes running VMware vSphere ESXi to retrieve information for the dashboard and to facilitate rolling upgrades of firmware, software and drivers. NetApp Hybrid Cloud Control and its related services on the management node use credentials (username/password) to authenticate against VMware vCenter and ESXi.

If communication between these components fails, NetApp Hybrid Cloud Control and vCenter display error messages when authentication problems occur. NetApp Hybrid Cloud Control will display a red error banner if it cannot communicate with the associated VMware vCenter instance in the NetApp HCI installation. VMware vCenter will display ESXi account lockout messages for individual ESXi hosts as a result of NetApp Hybrid Cloud Control using outdated credentials.

The management node in NetApp HCI refers to these components using the following names:

- "Controller assets" are vCenter instances associated with your NetApp HCI installation.
- "Compute node assets" are the ESXi hosts in your NetApp HCI installation.

During the initial installation of NetApp HCI using the NetApp Deployment Engine, the management node stored the credentials for the administrative user you specified for vCenter and the “root” account password on ESXi servers.

Update vCenter password by using the management node REST API

Follow the steps to update the controller assets. See View or edit existing controller assets.

Update the ESXi password by using the management node REST API

Steps

1. To gain an overview of the Management node REST API user interface, see the Management node REST API user interface overview.
2. Access the REST API UI for management services on the management node:

   ```
   https://<management node IP>/mnode
   ```

   Replace <management node IP> with the IPv4 address of your management node on the management network used for NetApp HCI.

3. Click **Authorize** or any lock icon and complete the following:
   a. Enter the NetApp SolidFire cluster administrative user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Click **Authorize** to begin a session.
   d. Close the window.
4. From the REST API UI, click **GET /assets/compute_nodes**.

   This retrieves the records of compute node assets that are stored in the management node.

   Here is the direct link to this API in the UI:

   ```
   https://<management node
   IP>/mnode/#/assets/routes.v1.assets_api.get_compute_nodes
   ```

5. Click **Try it out**.
6. Click **Execute**.
7. From the response body, identify the compute node asset records that need updated credentials. You can use the "ip" and "host_name" properties to find the correct ESXi host records.

   ```
   "config": { },
   "credentialid": <credential_id>,
   "hardware_tag": <tag>,
   "host_name": <host_name>,
   "id": <id>,
   "ip": <ip>,
   "parent": <parent>,
   "type": ESXi Host
   ```

   The next step uses the "parent" and "id" fields in the compute asset record to reference the record to be updated.

8. Configure the specific compute node asset:
    a. Click **PUT /assets/{asset_id}/compute-nodes/{compute_id}**.

       Here is the direct link to the API in the UI:

       ```
       https://<management node
       IP>/mnode/#/assets/routes.v1.assets_api.put_assets_compute_id
       ```

    b. Click **Try it out**.
    c. Enter the “asset_id” with the “parent” information.
    d. Enter the “compute_id” with the “id” information.
    e. Modify the request body in the user interface to update only the password and user name parameters in the compute asset record:

       ```
       {
       "password": "string",
       "username": "root"
       }
       ```

    f. Click **Execute**.
    g. Validate that the response is HTTP 200, which indicates that the new credentials have been stored in the referenced compute asset record
9. Repeat the previous two steps for additional compute node assets that need to be updated with a new password.
10. Wait for about 15 minutes for the account lockout message in vCenter to disappear.

Find more information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Manage NetApp HCI storage

Manage NetApp HCI storage overview

With NetApp HCI, you can manage these storage assets by using the NetApp Hybrid Cloud Control.

- Create and manage user accounts
- Add and manage storage clusters
- Create and manage volumes
- Create and manage volume access groups
- Create and manage initiators

- Create and manage volume QoS policies

Find more information

- SolidFire and Element 12.2 Documentation Center
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Create and manage user accounts by using NetApp Hybrid Cloud Control

In Element-based storage systems, authoritative cluster users can be created to enable login access to NetApp Hybrid Cloud Control depending on the permissions you want 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.

Manage the following types of accounts:

- Manage authoritative cluster accounts
- Manage volume accounts

Enable LDAP

To use LDAP for any user account, you must first enable LDAP.

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. From the Users page, click **Configure LDAP**.
4. Define your LDAP configuration.
5. Select the authentication type of Search and Bind or Direct Bind.
6. Before you save the changes, click **Test LDAP Log In** at the top of the page, enter the user name and password of a user you know exists, and click **Test**.
7. Click **Save**.

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. Select the authentication type of cluster or LDAP.
5. Complete one of the following:
   - If you selected LDAP, enter the DN.

     > To use LDAP, you must first enable LDAP or LDAPS. See Enable LDAP.

   - If you selected Cluster as the Auth Type, enter a name and password for the new account.
6. 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.

   > To ensure that all children of a group inherit permissions, create a DN organization admin group in the LDAP server. All the children accounts of that group will inherit those permissions.

7. Check the box indicating that "I have read and accept the NetApp End User License Agreement."
8. 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**.
7. Log out of NetApp Hybrid Cloud Control.
8. Update the credentials for the authoritative cluster asset using the NetApp Hybrid Cloud Control API.

> It might take the NetApp Hybrid Cloud Control UI up to 15 minutes to refresh the inventory. To manually refresh inventory, access the REST API UI inventory service `https://[management node IP]/inventory/1/` and run `GET /installations/{id}` for the cluster.

9. Log into NetApp Hybrid Cloud Control.

Delete an authoritative user account

You can delete one or more accounts when it is no longer needed. You can delete an LDAP user account.

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

   > 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.

> ℹ 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 Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Add and manage storage clusters using NetApp Hybrid Cloud Control

You can add storage clusters to the management node assets inventory so that they can be managed using NetApp Hybrid Cloud Control (HCC). The first storage cluster added during system setup is the default authoritative storage cluster, but additional clusters can be added using HCC UI.

After a storage cluster is added, you can monitor cluster performance, change storage cluster credentials for the managed asset, or remove a storage cluster from the management node asset inventory if it no longer needs to be managed using HCC.

What you'll need

- **Cluster administrator permissions**: You have permissions as administrator on the authoritative storage cluster. The authoritative cluster is the first cluster added to the management node inventory during system setup.
- **Element software**: Your storage cluster version is running NetApp Element software 11.3 or later.
- **Management node**: You have deployed a management node running version 11.3 or later.
- **Management services**: You have updated your management services bundle to version 2.17 or later.

Options

- Add a storage cluster
- Confirm storage cluster status
- Edit storage cluster credentials
- Remove a storage cluster

Add a storage cluster

You can add a storage cluster to the management node assets inventory using NetApp Hybrid Cloud Control. This allows you to manage and monitor the cluster using the HCC UI.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the authoritative storage cluster administrator credentials.
2. From the Dashboard, select the options menu on the top right and select **Configure**.
3. In the **Storage Clusters** pane, select **Storage Cluster Details**.
4. Select **Add Storage Cluster**.
5. Enter the following information:
   - Storage cluster management virtual IP address

     > Only remote storage clusters that are not currently managed by a management node can be added.

   - Storage cluster user name and password
6. Select **Add**.

After you add the storage cluster, the cluster inventory can take up to 15 minutes to refresh and display the new addition. You might need to refresh the page in your browser to see the changes.

7. If you are adding Element eSDS clusters, enter or upload your SSH private key and SSH user account.

Confirm storage cluster status

You can monitor the connection status of storage clusters assets using the NetApp Hybrid Cloud Control UI.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the authoritative storage cluster administrator credentials.
2. From the Dashboard, select the options menu on the top right and select **Configure**.
3. Review the status of storage clusters in the inventory.
4. From the **Storage Clusters** pane, select **Storage Cluster Details** for additional detail.

Edit storage cluster credentials

You can edit the storage cluster's administrator user name and password using the NetApp Hybrid Cloud Control UI.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the authoritative storage cluster administrator credentials.
2. From the Dashboard, select the options menu on the top right and select **Configure**.
3. In the **Storage Clusters** pane, select **Storage Cluster Details**.
4. Select the **Actions** menu for the cluster and select **Edit Cluster Credentials**.
5. Update the storage cluster user name and password.
6. Select **Save**.

Remove a storage cluster

Removing a storage cluster from NetApp Hybrid Cloud Control removes the cluster from the management node inventory. After you remove a storage cluster, the cluster can no longer be managed by HCC and you can access it only by navigating directly to its management IP address.

You cannot remove the authoritative cluster from the inventory. To determine the authoritative cluster, go to **User Management > Users**. The authoritative cluster is listed next to the heading **Users**.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the authoritative storage cluster administrator credentials.
2. From the Dashboard, select the options menu on the top right and select **Configure**.
3. In the **Storage Clusters** pane, select **Storage Cluster Details**.
4. Select the **Actions** menu for the cluster and select **Remove Storage Cluster**.

Clicking **Yes** next removes the cluster from the installation.

5. Select **Yes**.

Find more information

- Create and manage storage cluster assets
- 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:

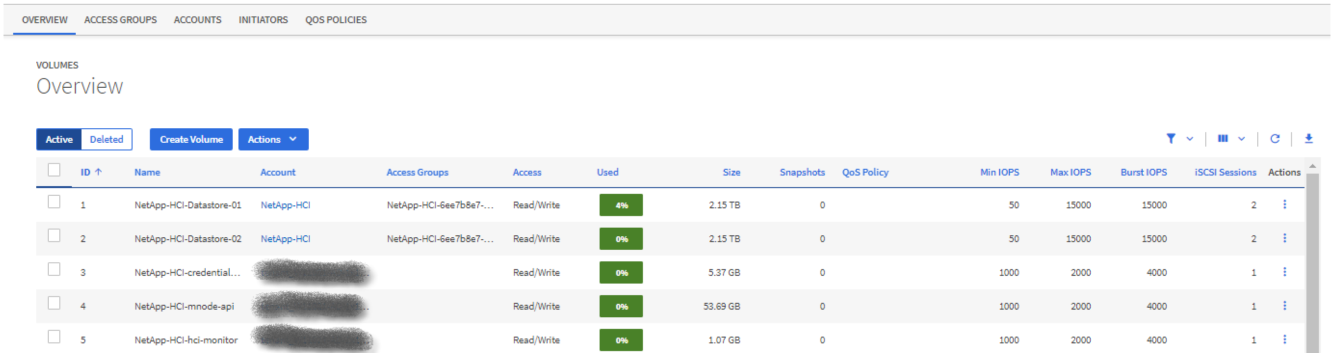
- Create a volume
- Apply a QoS policy to a volume
- Edit a volume
- Clone volumes
- Delete a volume
- Restore a deleted volume
- Purge a deleted volume

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.



VOLUMES

Overview

□	ID ↑	Name	Account	Access Groups	Access	Used	Size	Snapshots	QoS Policy	Min IOPS	Max IOPS	Burst IOPS	iSCSI Sessions	Actions
□	1	NetApp-HCI-Datastore-01	NetApp-HCI	NetApp-HCI-6ee7b8e7-…	Read/Write	4%	2.15 TB	0		50	15000	15000	2	⋮
□	2	NetApp-HCI-Datastore-02	NetApp-HCI	NetApp-HCI-6ee7b8e7-…	Read/Write	0%	2.15 TB	0		50	15000	15000	2	⋮
□	3	NetApp-HCI-credential…	[redacted]		Read/Write	0%	5.37 GB	0		1000	2000	4000	1	⋮
□	4	NetApp-HCI-mnode-api	[redacted]		Read/Write	0%	53.69 GB	0		1000	2000	4000	1	⋮
□	5	NetApp-HCI-hci-monitor	[redacted]		Read/Write	0%	1.07 GB	0		1000	2000	4000	1	⋮

4. Select **Create Volume**.
5. Enter a name for the new volume.
6. Enter the total size of the volume.

   > 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.

   If an account does not exist, click **Create New Account**, enter a new account name, and click **Create**. The account is created and associated with the new volume.

   > 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.

      > 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.

      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.

   If an account does not exist, click **Create New Account**, enter a new account name, and click **Create**. The account is created and associated with the existing volume.

    a. 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.

> 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.

> 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.

        > 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.

        If an account does not exist, click **Create New Account**, enter a new account name, and click **Create**. The account is created and associated with the volume.

     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 Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Create and manage volume access groups

You can create new volume access groups, make changes to the name, associated initiators, or associated volumes of access groups, or delete existing volume access groups using NetApp Hybrid Cloud Control.

What you'll need

- You have administrator credentials for this NetApp HCI system.
- 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. You can make changes to the name, associated initiators, or associated volumes of an access group.

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**.
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**.
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
- Add initiator to a volume access group
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Create and manage initiators

You can use initiators for CHAP-based rather than account-based access to volumes. You can create and delete initiators, and give them friendly aliases to simplify administration and volume access. When you add an initiator to a volume access group, that initiator enables access to all volumes in the group.

What you'll need

- You have cluster administrator credentials.
- You have upgraded your management services to at least version 2.17. NetApp Hybrid Cloud Control initiator management is not available in earlier service bundle versions.

Options

- Create an initiator
- Add initiators to a volume access group
- Change an initiator alias
- Delete initiators

Create an initiator

You can create iSCSI or Fibre Channel initiators and optionally assign them aliases.

About this task

The accepted format of an initiator IQN is `iqn.yyyy-mm` where y and m are digits followed by text which must only contain digits, lower-case alphabetic characters, a period (`.`), colon (`:`) or dash (`-`).
A sample of the format is as follows:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

The accepted format of a Fibre Channel initiator WWPN is `:Aa:bB:CC:dd:11:22:33:44` or `AabBCCdd11223344`.
A sample of the format is as follows:

```
5f:47:ac:c0:5c:74:d4:02
```

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the 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 **Initiators** tab.
5. Select the **Create Initiators** button.

Option	Steps
Create one or more initiators	a. Enter the IQN or WWPN for the initiator in the **IQN/WWPN** field. b. Enter a friendly name for the initiator in the **Alias** field. c. (Optional) Select **Add Initiator** to open new initiator fields or use the bulk create option instead. d. Select **Create Initiators**.
Bulk create initiators	a. Select **Bulk Add IQNs/WWPNs**. b. Enter a list of IQNs or WWPNs in the text box. Each IQN or WWPN must be comma or space separated or on its own line. c. Select **Add IQNs/WWPNs**. d. (Optional) Add unique aliases to each initiator. e. Remove any initiator from the list that might already exist in the installation. f. Select **Create Initiators**.

Add initiators to a volume access group

You can add initiators to an volume access group. When you add an initiator to a volume access group, the initiator enables access to all volumes in that volume access group.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the 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 **Initiators** tab.
5. Select one or more initiators you want to add.
6. Select **Actions > Add to Access Group**.
7. Select the access group.
8. Confirm your changes by selecting **Add Initiator**.

Change an initiator alias

You can change the alias of an existing initiator or add an alias if one does not already exist.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the 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 **Initiators** tab.
5. In the **Actions** column, expand the options menu for the initiator.
6. Select **Edit**.
7. Make any needed changes to the alias or add a new alias.
8. Select **Save**.

Delete initiators

You can delete one or more initiators. When you delete an initiator, the system removes it from any associated volume access group. Any connections using the initiator remain valid until the connection is reset.

Steps

1. Log in to NetApp Hybrid Cloud Control by providing the 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 **Initiators** tab.
5. Delete one or more initiators:
   a. Select one or more initiators you want to delete.
   b. Select **Actions > Delete**.
   c. Confirm the delete operation and select **Yes**.

Find more information

- Learn about initiators
- Learn about volume access groups
- NetApp Element Plug-in for vCenter Server
- 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.

> 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.

> 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.

   > 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 Element Plug-in for vCenter Server
- 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 use 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)

Perform tasks with the management node UI:

- Management node UI overview

Perform tasks with the management node REST APIs:

- Management node REST API UI overview

Disable or enable remote SSH functionality or start a remote support tunnel session with NetApp Support to help you troubleshoot:

- Enable remote NetApp Support connections
- Manage SSH functionality on the management node

Find more information

- NetApp Element Plug-in for vCenter Server
- 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 time sync
4. Set up the management node
5. Configure controller assets
6. (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).

   > 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 time sync

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

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

   b. Stop NTPD:

```
sudo service ntpd stop
```

c. Edit the NTP configuration file `/etc/ntp.conf`:

   i. Comment out the default servers (`server 0.gentoo.pool.ntp.org`) by adding a `#` in front of each.

   ii. Add a new line for each default time server you want to add. The default time servers must be the same NTP servers used on the storage cluster that you will use in a later step.

   ```
   vi /etc/ntp.conf

   #server 0.gentoo.pool.ntp.org
   #server 1.gentoo.pool.ntp.org
   #server 2.gentoo.pool.ntp.org
   #server 3.gentoo.pool.ntp.org
   server <insert the hostname or IP address of the default time
   server>
   ```

   iii. Save the configuration file when complete.

d. Force an NTP sync with the newly added server.

```
sudo ntpd -gq
```

e. Restart NTPD.

```
sudo service ntpd start
```

f. Disable time synchronization with host via the hypervisor (the following is a VMware example):

> If you deploy the mNode in a hypervisor environment other than VMware, for example, from the .iso image in an Openstack environment, refer to the hypervisor documentation for the equivalent commands.

   i. Disable periodic time synchronization:

   ```
   vmware-toolbox-cmd timesync disable
   ```

   ii. Display and confirm the current status of the service:

   ```
   vmware-toolbox-cmd timesync status
   ```

iii. 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.

Set up the management node

1. Configure and run the management node setup command:

> 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:

> 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. Configure the management node with the same storage cluster that you used during NTP servers configuration.
- **--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.

> 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 Element Plug-in for vCenter Server
- 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 a tagged or untagged 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.

Configuration options

Choose the option that is relevant for your environment:

- Configure a storage Network Interface Controller (NIC) for an untagged network interface
- Configure a storage Network Interface Controller (NIC) for a tagged network interface

Configure a storage Network Interface Controller (NIC) for an untagged network interface

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. `--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"
}
'
```

Configure a storage Network Interface Controller (NIC) for a tagged network interface

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. `--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",
                                   "virtualNetworkTag" : "$vlan_id"
                                   }
                          },
               "cluster": {
                         "name": "$mnode_host_name",
                         "cipi": "$eth1.$vlan_id",
                         "sipi": "$eth1.$vlan_id"
                         }
             },
    "method": "SetConfig"
}
'
```

Find more Information

- Add an asset to the management node
- NetApp Element Plug-in for vCenter Server
- 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 time sync
4. 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.

> 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).

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

Configure time sync

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

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

   b. Stop NTPD:

   ```
   sudo service ntpd stop
   ```

   c. Edit the NTP configuration file `/etc/ntp.conf`:

      i. Comment out the default servers (`server 0.gentoo.pool.ntp.org`) by adding a `#` in front of each.

      ii. Add a new line for each default time server you want to add. The default time servers must be the same NTP servers used on the storage cluster that you will use in a later step.

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time
server>
```

iii. Save the configuration file when complete.

d. Force an NTP sync with the newly added server.

```
sudo ntpd -gq
```

e. Restart NTPD.

```
sudo service ntpd start
```

f. Disable time synchronization with host via the hypervisor (the following is a VMware example):

> If you deploy the mNode in a hypervisor environment other than VMware, for example, from the .iso image in an Openstack environment, refer to the hypervisor documentation for the equivalent commands.

i. Disable periodic time synchronization:

```
vmware-toolbox-cmd timesync disable
```

ii. Display and confirm the current status of the service:

```
vmware-toolbox-cmd timesync status
```

iii. 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.

Configure the management node

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

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

2. 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.
3. 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]
   ```

4. 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
   ```

5. 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. Configure the management node with the same storage cluster that you used during NTP servers configuration.
      - **[persistent volume account name]**: The name of the account associated with all persistent volumes in this storage cluster.
6. 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:

   > ℹ 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.

> If you had previously disabled SSH functionality on the management node, you need to disable SSH again on the recovered management node. SSH capability that provides NetApp Support remote support tunnel (RST) session access is enabled on the management node by default.

Find more Information

- Persistent volumes
- NetApp Element Plug-in for vCenter Server
- 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.

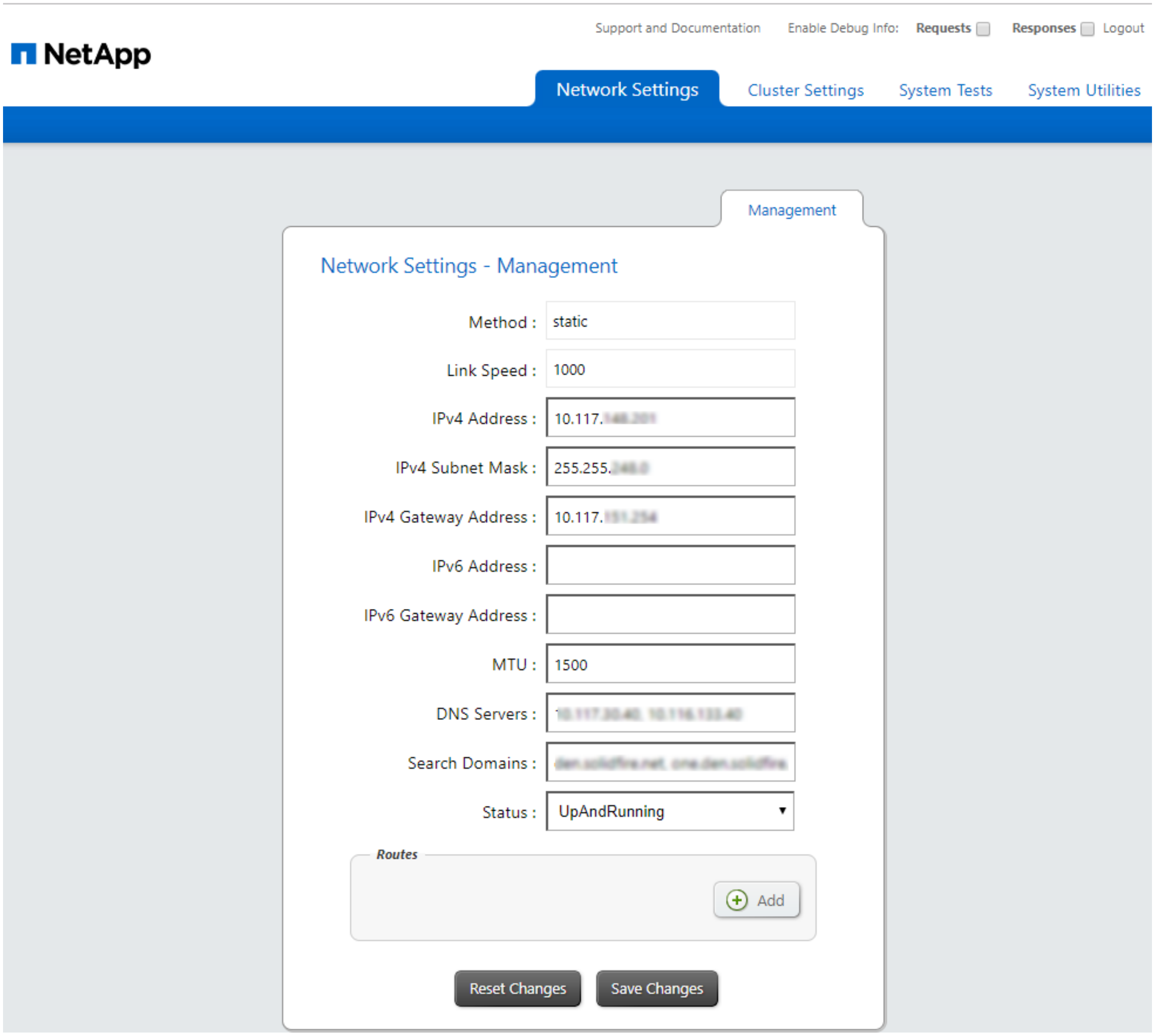
Access the management node per-node UI

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
```



Network Settings - Management

Method :	static
Link Speed :	1000
IPv4 Address :	10.117.[redacted]
IPv4 Subnet Mask :	255.255.[redacted]
IPv4 Gateway Address :	10.117.[redacted]
IPv6 Address :	
IPv6 Gateway Address :	
MTU :	1500
DNS Servers :	[redacted]
Search Domains :	[redacted]
Status :	UpAndRunning ▾

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

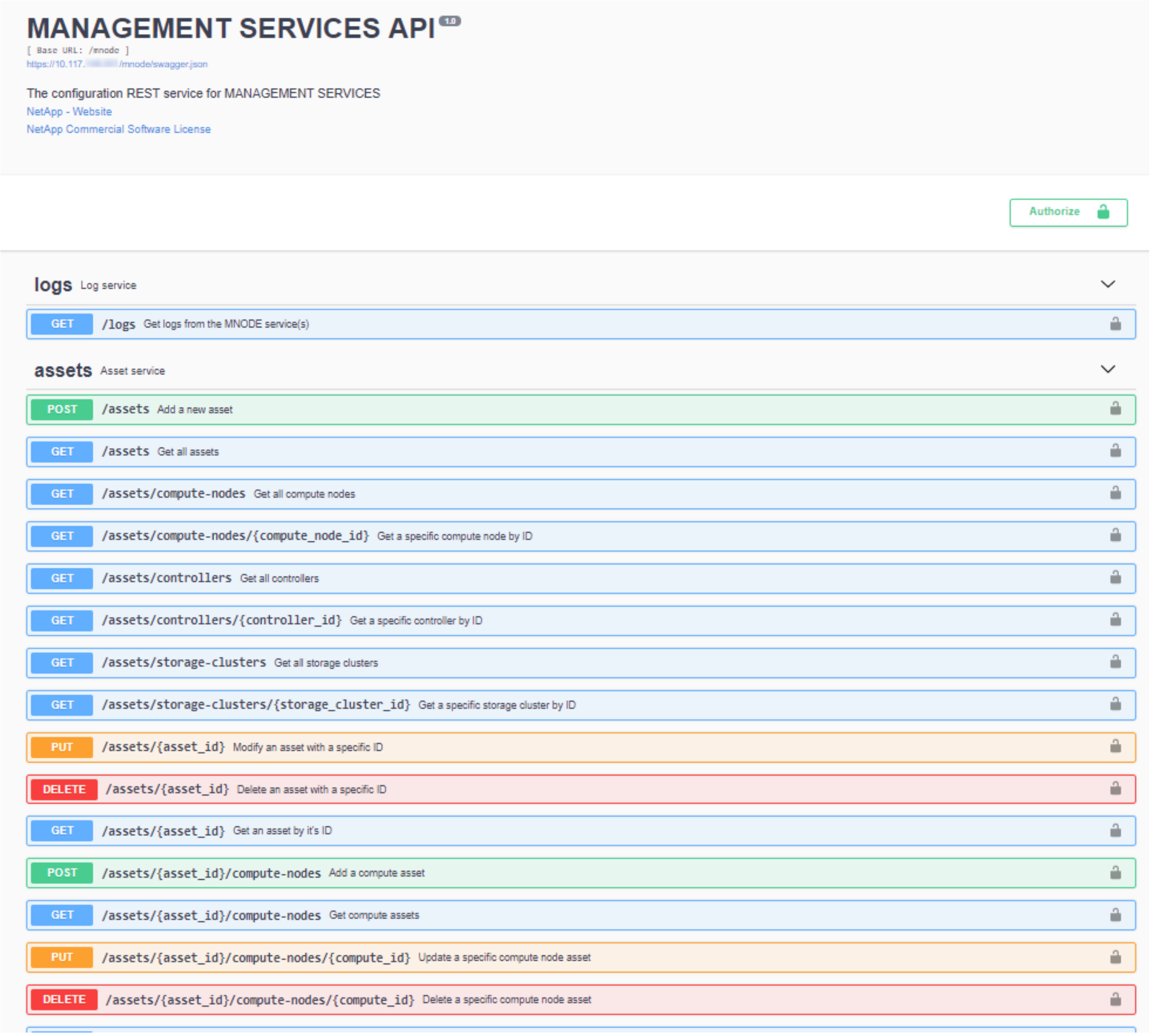
Access the management node REST API UI

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.[redacted]/mnode/swagger.json

The configuration REST service for MANAGEMENT SERVICES
NetApp - Website
NetApp Commercial Software License

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 Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Work with the management node UI

Management node UI overview

With the management node UI (`https://<managementNodeIP>: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 Element Plug-in for vCenter Server
- 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.

> 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. ℹ 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.
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. ℹ 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 Element Plug-in for vCenter Server

- 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://<managementNodeIP>/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:

Authorization

- Get authorization to use REST APIs

Asset configuration

- Enable Active IQ and NetApp HCI monitoring
- Configure a proxy server for the management node
- Configure NetApp Hybrid Cloud Control for multiple vCenters
- Add compute and controller assets to the management node
- Create and manage storage cluster assets

Asset management

- View or edit existing controller assets
- Create and manage storage cluster assets
- Remove an asset from the management node
- Use the REST API to collect NetApp HCI logs
- Verify management node OS and services versions
- Getting logs from management services

Find more information

- Access the management node
- NetApp Element Plug-in for vCenter Server
- 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. Access the REST API UI for the service by entering the management node IP address followed by the service name, for example `/mnode/`:

   ```
   https://<managementNodeIP>/mnode/
   ```

2. Click **Authorize**.

   > ℹ 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. Enter the client ID as `mnode-client`.

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

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

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 Element Plug-in for vCenter Server
- 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 authoritative cluster and multiple storage cluster support.

> 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.
`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.

> 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
- NetApp Element Plug-in for vCenter Server
- 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 Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Verify management node OS and services versions

You can verify the version numbers of the management node OS, management services bundle, and individual services running on the management node using the REST API in the management node.

What you’ll need

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

Options

- API commands
- REST API UI steps

API commands

- Get version information about the management node OS, the management services bundle, and the management node API (mnode-api) service that are running on the management node:

```
curl -X GET "https://<managementNodeIP>/mnode/about" -H  "accept:
application/json"
```

- Get version information about individual services running on the management node:

```
curl -X GET "https://<managementNodeIP>/mnode/services?status=running"
-H  "accept: */*" -H  "Authorization: Bearer <ID>"
```

> You can find the bearer ID used by the API by running a GET command and retrieving it from the curl response.

REST API UI steps

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

```
https://<managementNodeIP>/mnode/
```

2. Do one of the following:
   - Get version information about the management node OS, the management services bundle, and the management node API (mnode-api) service that are running on the management node:
     a. Select **GET /about**.

     b. Select **Try it out**.

     c. Select **Execute**.

     The management services bundle version (`"mnode_bundle_version"`), management node OS version (`"os_version"`), and management node API version (`"version"`) are indicated in the response body.
   - Get version information about individual services running on the management node:
     a. Select **GET /services**.

     b. Select **Try it out**.

     c. Select the status as **Running**.

     d. Select **Execute**.

     The services that are running on the management node are indicated in the response body.

Find more information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Getting logs from management services

You can retrieve logs from the services running on the management node using the REST API. You can pull logs from all public services or specify specific services and use query parameters to better define the return results.

What you’ll need

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

Steps

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

   ```
   https://[managementNodeIP]/mnode
   ```

2. Select **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 if the value is not already populated.
   c. Select **Authorize** to begin a session.
   d. Close the window.
3. Select **GET /logs**.
4. Select **Try it out**.
5. Specify the following parameters:
   - `Lines`: Enter the number of lines you want the log to return. This parameter is an integer that defaults to 1000.

     > Avoid requesting the entire history of log content by setting Lines to 0.

   - `since`: Adds a ISO-8601 timestamp for the service logs starting point.

     > Use a reasonable `since` parameter when gathering logs of wider timespans.

   - `service-name`: Enter a service name.

     > Use the `GET /services` command to list services on the management node.

   - `stopped`: Set to `true` to retrieve logs from stopped services.
6. Select **Execute**.

Find more Information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Manage support connections

Start a remote NetApp Support session

If you require technical support for your NetApp HCI or SolidFire all-flash storage system, NetApp Support can connect remotely with your system. To start a session and 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

By default, the capability for remote access is enabled on the management node. To disable remote access functionality, see Manage SSH functionality on the management node. You can enable remote access functionality again, if needed.

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

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Manage SSH functionality on the management node

You can disable, re-enable, or determine the status of the SSH capability on the management node (mNode) using the REST API. SSH capability that provides NetApp Support remote support tunnel (RST) session access is enabled on the management node by default.

What you'll need

- **Cluster administrator permissions**: You have permissions as administrator on the storage cluster.
- **Element software**: Your cluster is running NetApp Element software 11.3 or later.
- **Management node**: You have deployed a management node running version 11.3 or later.
- **Management services updates**: You have updated your management services bundle to version 2.17.

Options

You can do any of the following tasks after you authenticate:

- Disable or enable the SSH capability on the management node
- Determine status of the SSH capability on the management node

Disable or enable the SSH capability on the management node

You can disable or re-enable SSH capability on the management node. SSH capability that provides NetApp Support remote support tunnel (RST) session access is enabled on the management node by default. Disabling SSH does not terminate or disconnect existing SSH client sessions to the management node. If you disable SSH and elect to re-enable it at a later time, you can do so using the same API.

API command

```
curl -X PUT
"https://<managementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer <ID>"
```

> ℹ You can find the bearer ID used by the API by running a GET command and retrieving it from the curl response.

REST API UI steps

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

   ```
   https://<managementNodeIP>/mnode/
   ```

2. Select **Authorize** and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Select **Authorize** to begin a session.
   d. Close the window.
3. From the REST API UI, select **PUT /settings/ssh**.
   a. Click **Try it out**.
   b. Set the **enabled** parameter to `false` to disable SSH or `true` to re-enable SSH capability that you previously disabled.
   c. Click **Execute**.

Determine status of the SSH capability on the management node

You can determine whether or not SSH capability is enabled on the management node using a management node service API. SSH is enabled by default on the management node.

API command

```
curl -X GET "https://<managementNodeIP>/mnode/settings/ssh" -H  "accept:
application/json" -H  "Authorization: Bearer <ID>"
```

> You can find the bearer ID used by the API by running a GET command and retrieving it from the curl response.

REST API UI steps

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

   ```
   https://<managementNodeIP>/mnode/
   ```

2. Select **Authorize** and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Select **Authorize** to begin a session.
   d. Close the window.
3. From the REST API UI, select **GET /settings/ssh**.
   a. Click **Try it out**.
   b. Click **Execute**.

Find more information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

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

Copyright Information

Trademark Information