Manage and monitor storage with NetApp Hybrid Cloud Control

Element Software

NetApp
November 18, 2021

Table of Contents

Manage and monitor storage with NetApp Hybrid Cloud Control

With NetApp SolidFire all-flash storage, you can manage and monitor storage assets and configure components in your storage system using the NetApp Hybrid Cloud Control.

- Add and manage storage clusters
- Configure Fully Qualified Domain Name web UI access
- Create and manage user accounts
- Create and manage volumes
- Create and manage volume access groups
- Create and manage initiators
- Create and manage volume QoS policies
- Monitor your SolidFire system with NetApp Hybrid Cloud Control

Find more information

- NetApp Element Plug-in for vCenter Server
- SolidFire and Element 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.

Starting with Element 12.2, you can use the maintenance mode feature options to enable and disable maintenance mode for your storage cluster nodes.

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
- Enable and disable maintenance mode

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 2 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**.

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

5. Select **Yes**.

Enable and disable maintenance mode

If you need to take a storage node offline for maintenance such as software upgrades or host repairs, you can minimize the I/O impact to the rest of the storage cluster by enabling maintenance mode for that node. When you disable maintenance mode, the node is monitored to ensure certain criteria are met before the node can transition out of maintenance mode.

Information is available on the maintenance mode enable and disable feature options and the possible scenarios while using maintenance mode.

What you'll need

- **Element software**: Your storage cluster version is running NetApp Element software 12.2 or later.
- **Management node**: You have deployed a management node running version 12.2 or later.
- **Management services**: You have updated your management services bundle to version 2.19 or later.
- You have access to log in at the administrator level.

Enable maintenance mode

You can use the following procedure to enable maintenance mode for a storage cluster node.

Only one node can be in maintenance mode at a time.

Steps

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

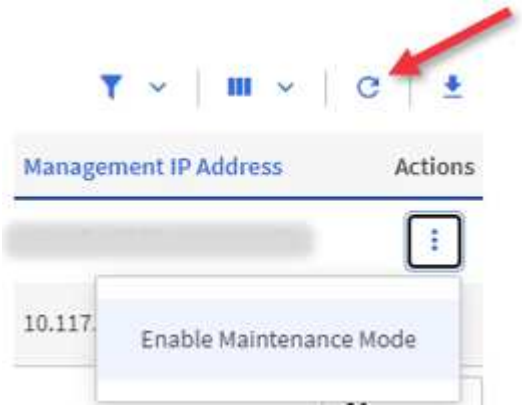
   ```
   https://[management node IP address]
   ```

2. Log in to NetApp Hybrid Cloud Control by providing the SolidFire all-flash storage cluster administrator credentials.

   The maintenance mode feature options are disabled at the read-only level.

3. In the left navigation blue box, select the SolidFire all-flash installation.
4. In the left navigation pane, select **Nodes**.
5. To view storage inventory information, select **Storage**.
6. Enable maintenance mode on a storage node:

   The storage nodes table is updated automatically every two minutes for non-user initiated actions. Before an action, to ensure that you have the most up-to-date status, you can refresh the nodes table by using the refresh icon located on the upper-right side of the nodes table.

   a. Under **Actions**, select **Enable Maintenance Mode**.

      While **Maintenance Mode** is being enabled, maintenance mode actions are unavailable for the selected node and all other nodes on the same cluster.

      After **Enabling Maintenance Mode** completes, the **Node Status** column displays a wrench icon and the text "**Maintenance Mode**" for the node that is in maintenance mode.

Disable maintenance mode

After a node is successfully placed in maintenance mode, the **Disable Maintenance Mode** action is available for this node. Actions on the other nodes are unavailable until maintenance mode is disabled successfully on the node undergoing maintenance.

Steps

1. For the node under maintenance mode, under **Actions**, select **Disable Maintenance Mode**.

   While **Maintenance Mode** is being disabled, maintenance mode actions are unavailable for the selected node and all other nodes on the same cluster.

   After **Disabling Maintenance Mode** completes, the **Node Status** column displays **Active**.

   When a node is in maintenance mode, it does not accept new data. As a result, it can take longer to disable maintenance mode because the node must sync its data back up before it can exit maintenance mode. The longer you spend in maintenance mode, the longer it can take to disable maintenance mode.

Troubleshoot

If you encounter errors when you are either enabling or disabling maintenance mode, a banner error displays at the top of the nodes table. For more information on the error, you can select the **Show Details** link that is provided on the banner to show what the API returns are.

Find more information

- Create and manage storage cluster assets
- SolidFire and Element Resources page

Configure Fully Qualified Domain Name web UI access

SolidFire all-flash storage with NetApp Element software 12.2 or later enables you to access storage cluster web interfaces using the Fully Qualified Domain Name (FQDN). If you want to use the FQDN to access web user interfaces such as the Element web UI, per-node UI, or management node UI, you must first add a storage cluster setting to identify the FQDN used by the cluster.

This process enables the cluster to properly redirect a login session and improves integration with external services such as key managers and identity providers for multi-factor authentication.

What you'll need

- This feature requires Element 12.2 or later.
- Configuring this feature using NetApp Hybrid Cloud Control REST APIs requires management services 2.15 or later.
- Configuring this feature using the NetApp Hybrid Cloud Control UI requires management services 2.19 or later.
- To use REST APIs, you must have deployed a management node running version 11.5 or later.
- You need fully qualified domain names for the management node and each storage cluster that resolve correctly to the management node IP address and each storage cluster IP address.

You can configure or remove FQDN web UI access using NetApp Hybrid Cloud Control and the REST API. You can also troubleshoot incorrectly configured FQDNs.

- Configure FQDN web UI access using NetApp Hybrid Cloud Control

- Configure FQDN web UI access using the REST API
- Remove FQDN web UI access using NetApp Hybrid Cloud Control
- Remove FQDN web UI access using the REST API
- Troubleshooting

Configure FQDN web UI access using NetApp Hybrid Cloud Control

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the storage cluster administrator credentials.
3. Select the menu icon at the top right of the page.
4. Select **Configure**.
5. In the **Fully Qualified Domain Names** pane, select **Set Up**.
6. In the resulting window, enter the FQDNs for the management node and each storage cluster.
7. Select **Save**.

   The **Fully Qualified Domain Names** pane lists each storage cluster with its associated MVIP and FQDN.

   > Only connected storage clusters with the FQDN set are listed in the **Fully Qualified Domain Names** pane.

Configure FQDN web UI access using the REST API

Steps

1. Ensure that the Element storage nodes and the mNode have DNS configured correctly for the network environment so that FQDNs in the environment can be resolved. To set DNS, go to the per-node UI for storage nodes and to the management node, then select **Network Settings** > **Management Network**.
   a. Per-node UI for storage nodes: `https://<storage_node_management_IP>:442`
   b. Per-node UI for the management node: `https://<management_node_IP>:442`
2. Change the storage cluster settings using the Element API.
   a. Access the Element API and create the following cluster interface preference using the CreateClusterInterfacePreference API method, inserting the cluster MVIP FQDN for the preference value:
      - Name: `mvip_fqdn`
      - Value: `Fully Qualified Domain Name for the Cluster MVIP`

        In this example, FQDN=storagecluster.my.org:

```
https://<Cluster_MVIP>/json-rpc/12.2?
method=CreateClusterInterfacePreference&name=mvip_fqdn&value=stora
gecluster.my.org
```

3. Change the management node settings using the REST API on the management node:
   a. Access the REST API UI for the management node by entering the management node IP address followed by `/mnode/2/`

      For example:

      `https://<management_node_IP>/mnode/2/`

   b. Click **Authorize** or any lock icon and enter the cluster user name and password.
   c. Enter the client ID as `mnode-client`.
   d. Click **Authorize** to begin the session and then close the window.
   e. From the server list, select `mnode2`.
   f. Click **GET /settings**.
   g. Click **Try it out**.
   h. Click **Execute**.
   i. Record any proxy settings reported in the response body.
   j. Click **PUT/setttings**.
   k. Click **Try it out**.
   l. In the request body area, enter the management node FQDN as the value for the `mnode_fqdn` parameter.
   m. Enter any proxy setting values you recorded earlier in the remaining parameters in the request body. If you leave the proxy parameters empty or do not include them in the request body, existing proxy settings will be removed.
   n. Click **Execute**.

Remove FQDN web UI access using NetApp Hybrid Cloud Control

You can use this procedure to remove FQDN web access for the management node and the storage clusters.

Steps

1. In the **Fully Qualified Domain Names** pane, select **Edit**.
2. In the resulting window, delete the contents in the **FQDN** text field.
3. Select **Save**.

   The window closes and the FQDN is no longer listed in the **Fully Qualified Domain Names** pane.

Remove FQDN web UI access using the REST API

Steps

1. Change the storage cluster settings using the Element API.
   a. Access the Element API and delete the following cluster interface preference using the `DeleteClusterInterfacePreference` API method:
      - Name: `mvip_fqdn`

      For example:

      ```
      https://<Cluster_MVIP>/json-
      rpc/12.2?method=DeleteClusterInterfacePreference&name=mvip_fqdn
      ```

2. Change the management node settings using the REST API on the management node:
   a. Access the REST API UI for the management node by entering the management node IP address followed by `/mnode/2/`. For example:

      ```
      https://<management_node_IP>/mnode/2/
      ```

   b. Select **Authorize** or any lock icon and enter the Element cluster user name and password.
   c. Enter the client ID as `mnode-client`.
   d. Select **Authorize** to begin a session.
   e. Close the window.
   f. Select **PUT /settings**.
   g. Select **Try it out**.
   h. In the request body area, do not enter a value for the `mnode_fqdn` parameter. Also specify whether the proxy should be used (`true` or `false`) for the `use_proxy` parameter.

      ```
      {
       "mnode_fqdn": "",
       "use_proxy": false
      }
      ```

   i. Select **Execute**.

Troubleshooting

If FQDNs are configured incorrectly, you might have problems accessing either the management node, a storage cluster, or both. Use the following information to help troubleshoot the issue.

Issue	Cause	Resolution
• You get a browser error when attempting to access either the management node or the storage cluster using the FQDN. • You cannot log in to either the management node or the storage cluster using an IP address.	The management node FQDN and storage cluster FQDN are both incorrectly configured.	Use the REST API instructions on this page to remove the management node and storage cluster FQDN settings and configure them again.
• You get a browser error when attempting to access the storage cluster FQDN. • You cannot log in to either the management node or the storage cluster using an IP address.	The management node FQDN is correctly configured, but the storage cluster FQDN is incorrectly configured.	Use the REST API instructions on this page to remove the storage cluster FQDN settings and configure them again
• You get a browser error when attempting to access the management node FQDN. • You can log in to the management node and storage cluster using an IP address.	The management node FQDN is incorrectly configured, but the storage cluster FQDN is correctly configured.	Log in to NetApp Hybrid Cloud Control to correct the management node FQDN settings in the UI, or use the REST API instructions on this page to correct the settings.

Find more information

- SolidFire and Element Resources page
- NetApp Element Plug-in for vCenter Server

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 Element storage cluster administrator credentials.
2. From the Dashboard, select on the top right Options icon and select **User Management**.
3. From the Users page, select **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, select **Test LDAP Log In** at the top of the page, enter the user name and password of a user you know exists, and select **Test**.
7. Select **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 Element storage cluster administrator credentials.
2. From the Dashboard, select 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, select **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. Select **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 Element storage cluster administrator credentials.
2. From the Dashboard, select 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.

It might take the NetApp Hybrid Cloud Control UI up to 2 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.

8. 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 Element storage cluster administrator credentials.
2. From the Dashboard, select 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 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 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.

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 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
- SolidFire and Element 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:

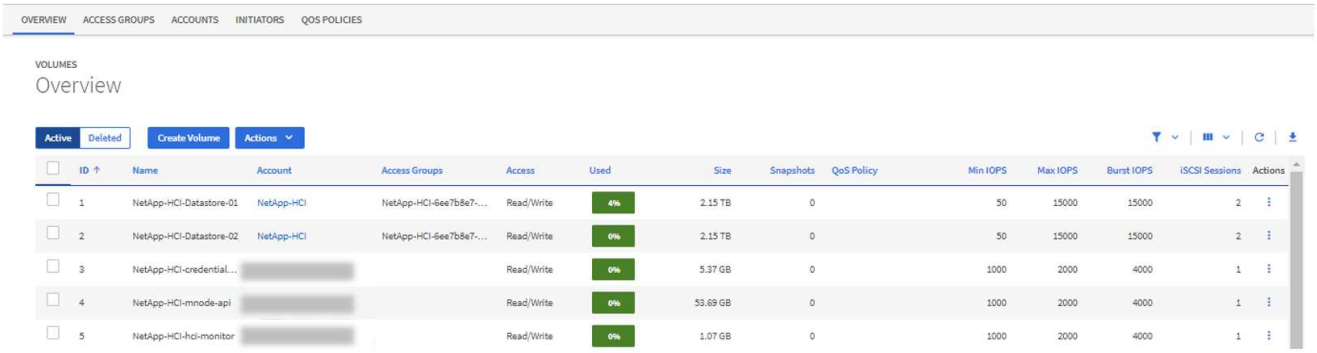
- Create a volume
- Apply a QoS policy to a volume
- Edit a volume
- Clone volumes
- Add volumes to a volume access group
- Delete a volume
- Restore a deleted volume
- Purge a deleted volume

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 Element storage cluster administrator credentials.
2. From the Dashboard, expand the name of your storage cluster on the left navigation menu.
3. Select **Volumes** > **Overview** tab.



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

> 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, select **Create New Account**, enter a new account name, and select **Create Account**. The account is created and associated with the new volume in the **Account** list.

> 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 configure the Quality of Service for the volume, do one of the following:
   - Under **Quality of Service Settings**, set customized minimum, maximum, and burst values for IOPS or use the default QoS values.
   - Select an existing QoS policy by enabling the **Assign Quality of Service Policy** toggle and choosing an existing QoS policy from the resulting list.
   - Create and assign a new QoS policy by enabling the **Assign Quality of Service Policy** toggle and selecting **Create New QoS Policy**. In the resulting window, enter a name for the QoS policy and then enter QoS values. When finished, select **Create Quality of Service Policy**.

   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. Select **Create Volume**.

Apply a QoS policy to a volume

You can apply a QoS policy to existing storage volumes by using NetApp Hybrid Cloud Control. If instead you need to set custom QoS values for a volume, you can Edit a volume. To create a new QoS policy, see Create and manage volume QoS policies.

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** > **Overview**.
4. Select one or more volumes to associate with a QoS policy.
5. Select the **Actions** drop-down list at the top of the volumes table, and select **Apply QoS Policy**.
6. In the resulting window, select a QoS policy from the list and select **Apply QoS Policy**.

> 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 values override QoS policy values for volume QoS settings.

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 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, select **Create New Account**, enter a new account name, and select **Create**. The account is created and associated with the existing volume.

d. Change the Quality of Service by doing one of the following:
   i. Select an existing policy.
   ii. Under Custom Settings, set the minimum, maximum, and burst values for IOPS or use the default values.

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 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.
5. Select the **Actions** drop-down list at the top of the volumes table, and select **Clone**.
6. In the resulting window, do the following:
   a. Enter a volume name prefix (this is optional).
   b. Choose the access type from the **Access** list.
   c. Choose an account to associate with the new volume clone (by default, **Copy from Volume** is selected, which will use the same account that the original volume uses).
   d. If an account does not exist, select **Create New Account**, enter a new account name, and select **Create Account**. The account is created and associated with the volume.

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

      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.

   e. Select **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.

Add volumes to a volume access group

You can add a single volume or a group of volumes to a 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** > **Overview**.

4. Select one or more volumes to associate with a volume access group.
5. Select the **Actions** drop-down list at the top of the volumes table, and select **Add to Access Group**.
6. In the resulting window, select a volume access group from the **Volume Access Group** list.
7. Select **Add Volume**.

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 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. Select the **Actions** drop-down list at the top of the volumes table, and select **Delete**.
6. In the resulting window, confirm the action 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 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 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, select 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
- SolidFire and Element Software Documentation
- NetApp Element Plug-in for vCenter Server
- SolidFire and Element 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 SolidFire all-flash storage 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 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 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 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
- SolidFire and Element 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
- SolidFire and Element 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 SolidFire all-flash storage 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 Element storage cluster administrator credentials.
2. From the Dashboard, expand the menu for your storage cluster.
3. Select **Storage > Volumes**.
4. Select the **QoS Policies** tab.
5. Select **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. Select **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 Element storage cluster administrator credentials.
2. From the Dashboard, expand the menu for your storage cluster.
3. Select **Storage > Volumes**.
4. Select 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. Select **Save**.

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 Element storage cluster administrator credentials.
2. From the Dashboard, expand the menu for your storage cluster.
3. Select **Storage > Volumes**.
4. Select 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. Select **Save**.

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 Element storage cluster administrator credentials.

2. From the Dashboard, expand the menu for your storage cluster.
3. Select **Storage > Volumes**.
4. Select the **QoS Policies** tab.
5. Select the **Actions** menu next to the QoS policy you intend to modify.
6. Select **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. Select **Save**.

You can select 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 Element storage cluster administrator credentials.
2. From the Dashboard, expand the menu for your storage cluster.
3. Select **Storage > Volumes**.
4. Select the **QoS Policies** tab.
5. Select the **Actions** menu next to the QoS policy you intend to modify.
6. Select **Delete**.
7. Confirm the action.

Find more information

- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Software Documentation

Monitor your SolidFire system with NetApp Hybrid Cloud Control

Monitor storage resources on the Hybrid Cloud Control Dashboard

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

performance.

When you launch a new NetApp Hybrid Cloud Control session for the first time, there might be a delay with loading the NetApp Hybrid Cloud Control Dashboard view when the management node is managing many clusters. The loading time varies depending on the number of clusters being actively managed by the management node. For subsequent launches, you will experience faster loading times.

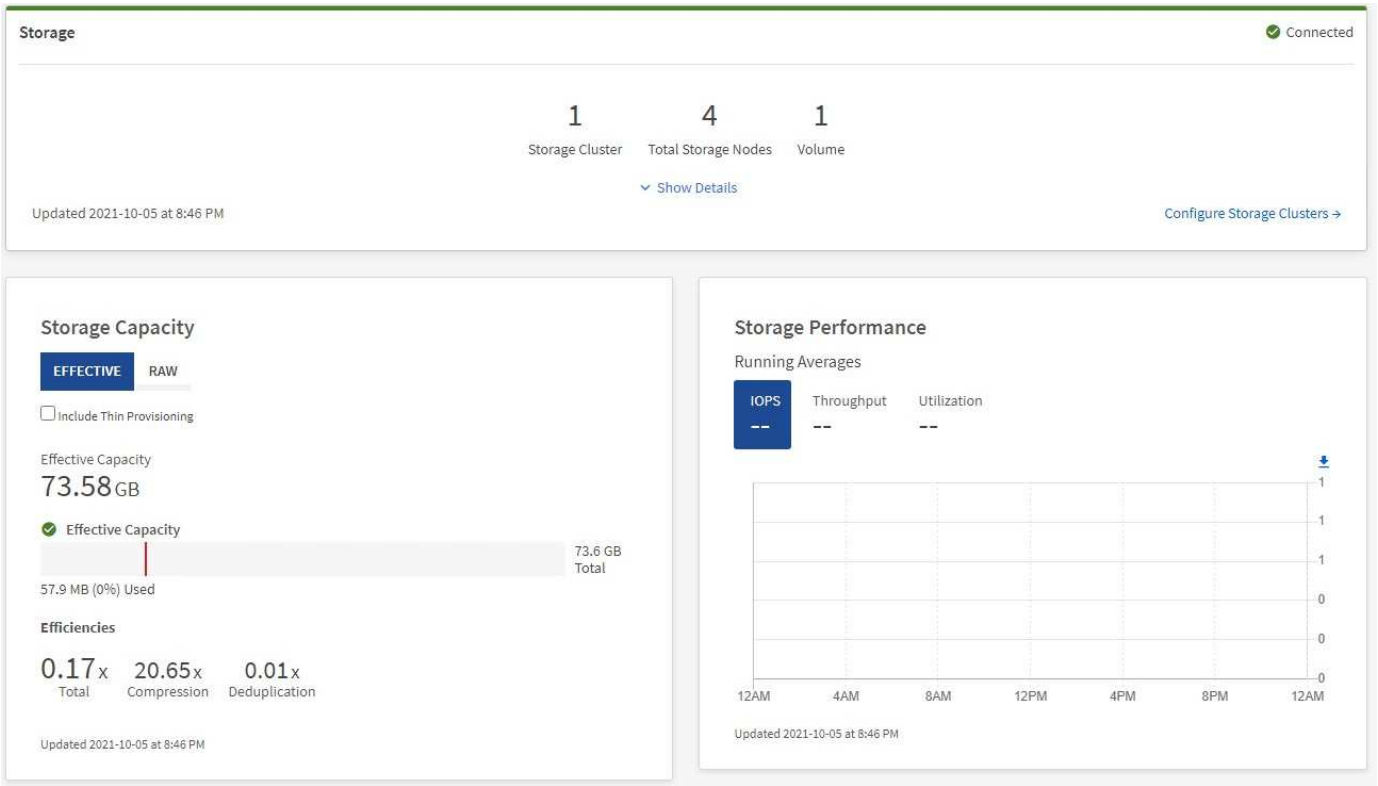
- Access the NetApp HCC Dashboard
- Monitor storage resources
- Monitor storage capacity
- Monitor storage performance

Access the NetApp HCC Dashboard

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

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

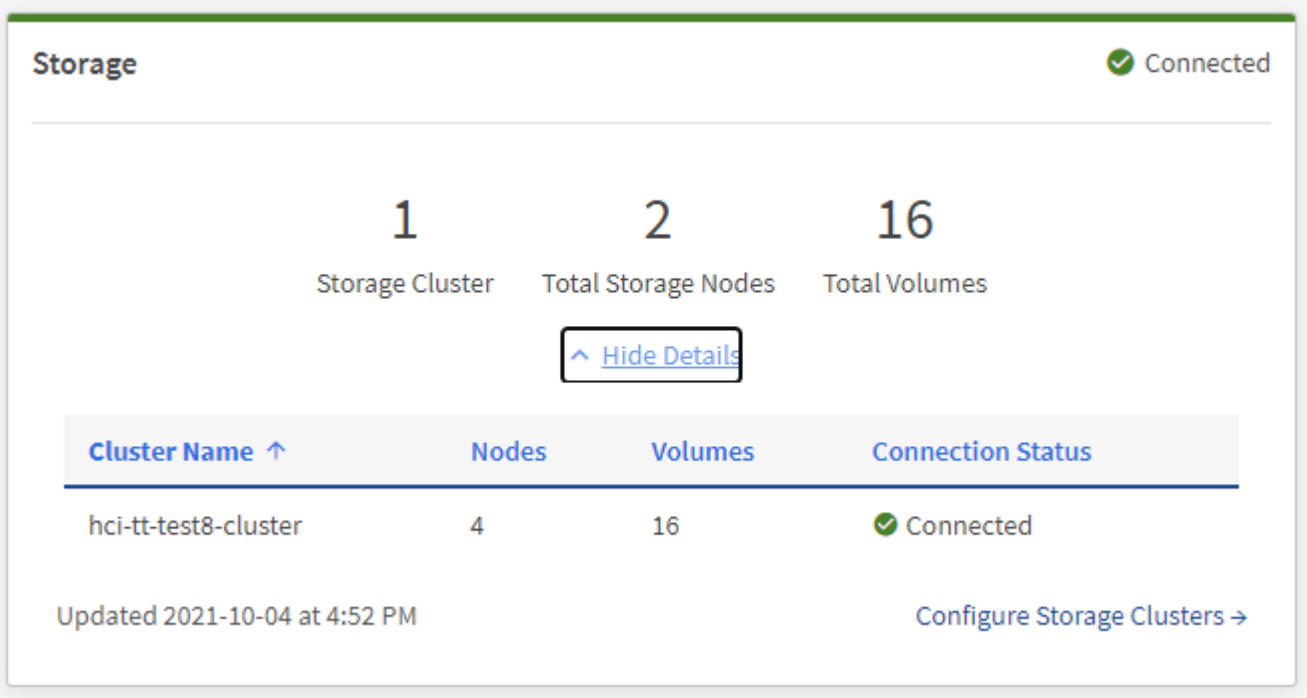
2. Log in to NetApp Hybrid Cloud Control by providing the SolidFire all-flash storage cluster administrator credentials.
3. View the Hybrid Cloud Control Dashboard.



Monitor storage resources

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

To see details, in the Storage pane, select **Show Details**.



The Total Storage Nodes number does not include Witness Nodes from two-node storage clusters. The Witness Nodes are included in the Nodes number in the details section for that cluster.

To see the most recent storage cluster data, use the Storage Clusters page, where polling occurs more frequently than on the Dashboard.

Monitor storage capacity

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

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

Steps

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

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

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

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

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

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

   b. **Effective Capacity bar chart**: Look at the vertical lines to determine whether your used capacity is less than the total or less than Warning, Error, or Critical thresholds. Similar to the Raw tab, you can hover over the vertical lines to see details.

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

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

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

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

Monitor storage performance

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

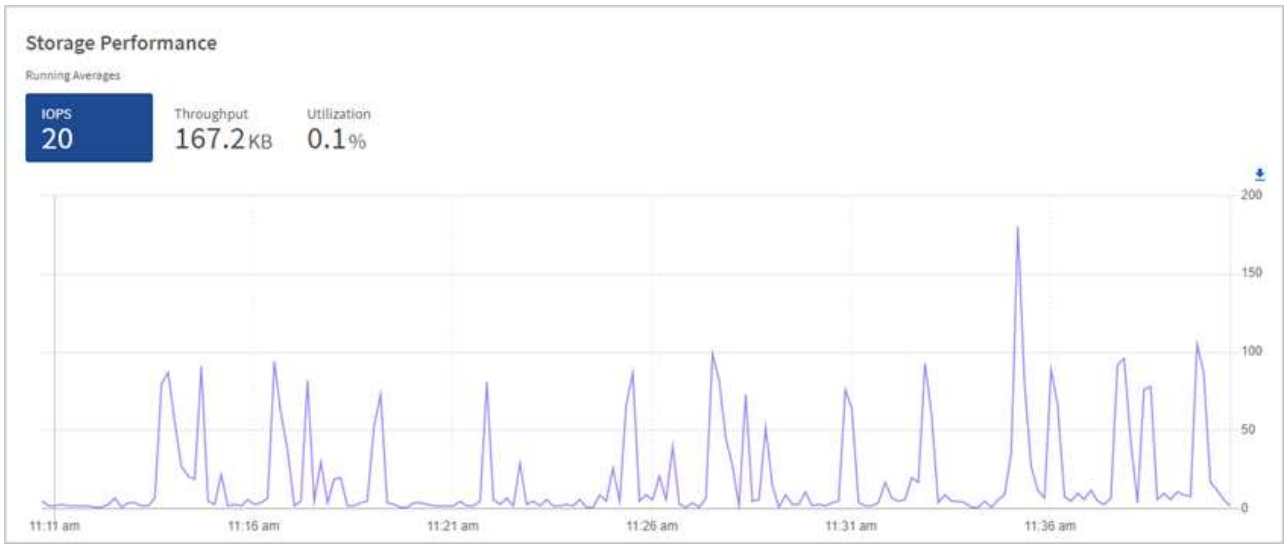
The Storage Performance pane helps you identify whether the performance is reaching the point where the performance might degrade if the workloads increase.

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

For details about the associated Element API method, see the GetClusterStats method in the *Element software API documentation*.

Steps

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



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

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

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

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

Find more information

- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Resources page

View your inventory on the Nodes page

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

You can view storage information for your multiple node systems. If custom protection domains are assigned, you can see which protection domains are assigned to specific nodes.

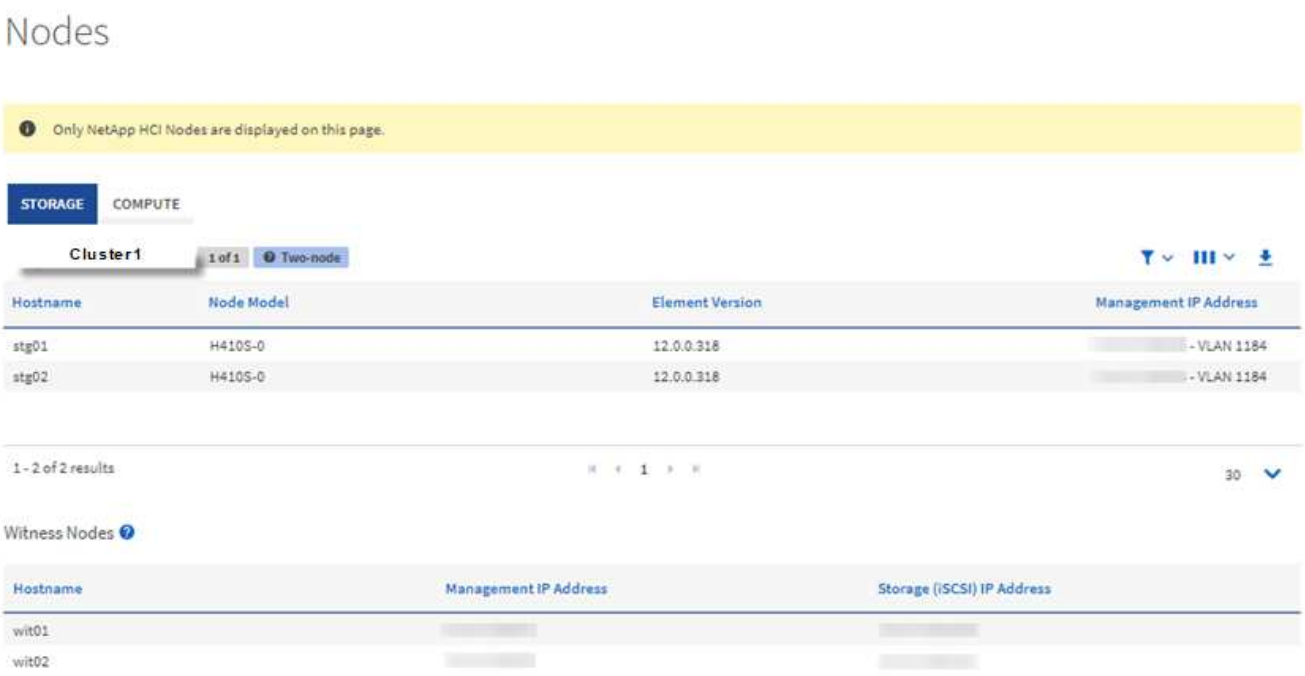
For SolidFire Enterprise SDS nodes, you can monitor inventory on the Storage tab.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the SolidFire all-flash storage cluster administrator credentials.
3. In the left navigation, select **Nodes**.



> When you launch a new NetApp Hybrid Cloud Control session for the first time, there might be a delay with loading the NetApp Hybrid Cloud Control Nodes page when the management node is managing many clusters. The loading time varies depending on the number of clusters being actively managed by the management node. For subsequent launches, you will experience faster loading times.

4. On the **Storage** tab of the Nodes page, review the following information:
   a. Two-node clusters: A “two-node” label appears on the Storage tab and the associated Witness Nodes are listed.
   b. Three-node clusters: The storage nodes and associated Witness Nodes are listed. Three-node clusters have a Witness Node deployed on standby to maintain high availability in the case of node failure.
   c. Clusters with four nodes or more: Information for clusters with four or more nodes appears. Witness Nodes do not apply. If you started with two or three storage nodes and added more nodes, the Witness Nodes still appear. Otherwise, the Witness Nodes table does not appear.
   d. The firmware bundle version: Starting with management services version 2.14, if you have clusters running Element 12.0 or later, you can see the firmware bundle version for these clusters. If the nodes in a cluster have different firmware versions on them, you can see **Multiple** in the **Firmware Bundle Version** column.

e. Custom protection domains: If custom protection domains are in use on the cluster, you can see custom protection domain assignments for each node in the cluster. If custom protection domains are not enabled, this column does not appear.

5. You can manipulate the information on these pages in several ways:
   a. To filter the list of items in the results, select the **Filter** icon and select the filters. You can also enter text for the filter.
   b. To show or hide columns, select the **Show/Hide Columns** icon.
   c. To download the table, select the **Download** icon.

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

Find more information

- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Resources page

Monitor volumes on your storage cluster

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

You can also see details on active and deleted volumes.

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

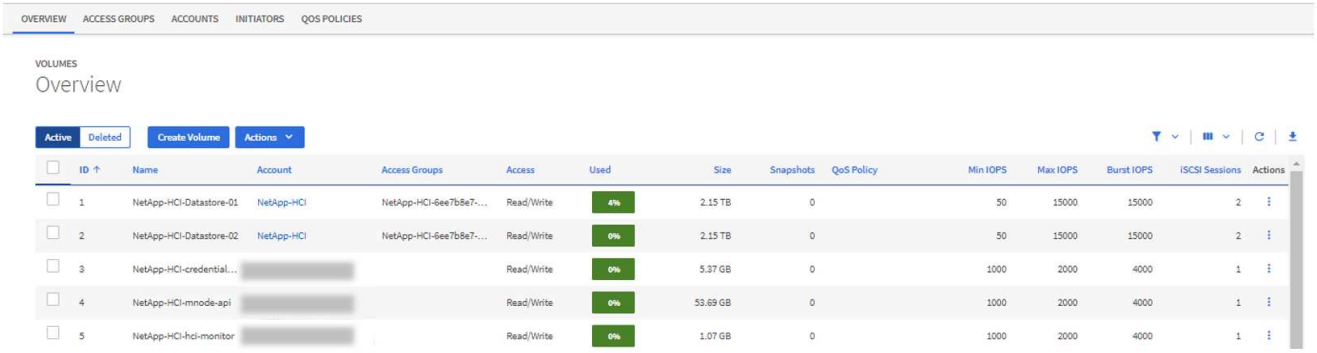
You can access this information only if you have NetApp Hybrid Cloud Control administrative privileges.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the SolidFire all-flash storage cluster administrator credentials.
3. In the left navigation blue box, select the SolidFire all-flash storage installation.
4. In the left navigation, select the cluster and select **Storage** > **Volumes**.



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

   a. Filter the results by selecting the **Filter** icon.
   b. Hide or show columns by selecting the **Hide/Show** icon.
   c. Refresh data by selecting the **Refresh** icon.
   d. Download a CSV file by selecting on the **Download** icon.

6. Monitor the Used capacity column. If Warning, Error, or Critical thresholds are reached, the color represents the used capacity status:
   a. Warning - Yellow
   b. Error - Orange
   c. Critical - Red
7. From the Volumes view, select the tabs to see additional details about the volumes:
   a. **Access Groups**: You can see the volume access groups that are mapped from initiators to a collection of volumes for secured access.

      See information about volume access groups.

   b. **Accounts**: You can see the user accounts, which enable clients to connect to volumes on a node. When you create a volume, it is assigned to a specific user account.

      See information about SolidFire all-flash storage system user accounts.

   c. **Initiators**: You can see the iSCSI initiator IQN or Fibre Channel WWPNs for the volume. Each IQN added to an access group can access each volume in the group without requiring CHAP authentication. Each WWPN added to an access group enables Fibre Channel network access to the volumes in the access group.
   d. **QoS Policies**: You can see the QoS policy applied to the volume. A QoS policy applies standardized settings for minimum IOPS, maximum IOPS, and burst IOPS to multiple volumes.

      See information about performance and QoS policies.

Find more information

- SolidFire and Element documentation

- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Resources page

Collect logs for troubleshooting

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

What you'll need

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

Log collection options

Choose one of the following options:

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

Use NetApp Hybrid Cloud Control to collect logs

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

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the Element storage cluster administrator credentials.
3. From the Dashboard, select the menu on the upper right.
4. Select **Collect Logs**.

   If you have collected logs before, you can download the existing log package, or begin a new log collection.

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

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

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

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

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

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

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

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

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

Use the REST API to collect logs

You can use REST API to collect Element logs.

Steps

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

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

   b. Select **Authorize** and complete the following:
      i. Enter the cluster user name and password.
      ii. Enter the client ID as `mnode-client` if the value is not already populated.
      iii. Select **Authorize** to begin a session.
2. Collect logs from Element:
   a. Select **POST /bundle**.
   b. Select **Try it out**.
   c. Change the values of the following parameters in the **Request body** field depending on which type of logs you need to collect and for what time range:

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

Parameter	Type	Description
`storageNodeIds`	UUID array	If `storageLogs` is set to `true`, populate this parameter with the storage cluster node IDs to limit log collection to those specific storage nodes. Use the `GET https://[management node IP]/logs/1/bundle/options` endpoint to see all possible node IDs you can use.

d. Select **Execute** to begin log collection.
The response should return a response similar to the following:

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

3. Check on the status of the log collection task:
   a. Select **GET /bundle**.
   b. Select **Try it out**.
   c. Select **Execute** to return a status of the collection task.
   d. Scroll to the bottom of the response body.

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

   e. Copy the file name at the end of the `downloadLink` attribute.
4. Download the collected log package:
   a. Select **GET /bundle/{filename}**.
   b. Select **Try it out**.
   c. Paste the file name you copied earlier into the `filename` parameter text field.
   d. Select **Execute**.

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

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

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

Find more information

- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Resources page