Manage storage with the vCenter Plug-in

VCP

NetApp
November 18, 2025

Table of Contents

Manage storage with the vCenter Plug-in

Manage clusters

You can edit a cluster running Element software, manage SSH configuration, set protection domain monitoring, and shut down a cluster.

What you'll need

- At least one cluster must be added:
  - Add a cluster using Element Plug-in for vCenter 5.0 and later
  - Add a cluster using Element Plug-in for vCenter 4.10 and earlier

  ⓘ You must add at least one cluster to use the plug-in extension point functions.

- Current full Cluster Admin user credentials for the cluster.
- Firewall rules allow open network communication between the vCenter and the cluster MVIP on the following TCP ports:
  - Beginning with Element Plug-in for vCenter 5.0, on ports 443, 8333, and 8443.
  - For Element Plug-in for vCenter 4.10 or earlier, on ports 443 and 8443.

Options

- View cluster details
- Edit a cluster profile
- Remove a cluster profile
- Enable Encryption at Rest
- Disable Encryption at Rest
- Enable SSH
- Change the SSH time limit
- Disable SSH
- Set protection domain monitoring
- Shut down a cluster
- Expand your NetApp HCI infrastructure

View cluster details

You can view cluster details from the vCenter Plug-in extension point.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster you want to edit.

3. Select **Actions**.
4. Select **Details**.
5. Review the following information for all clusters:
    - **Cluster Name**: The name for the cluster.
    - **vCenter IP Address**: The IP address or FQDN of the vCenter Server to which the cluster is assigned.
    - **Unique ID**: Unique ID for the cluster.
    - **Management Virtual IP**: The management virtual IP address (MVIP).
    - **Storage Virtual**: The storage virtual IP address (SVIP).
    - **Status**: The status of the cluster.
    - **VVols**: The status of the VVols functionality on the cluster.
6. Review additional details for an individual cluster:
    - **MVIP Node ID**: The node that holds the master MVIP address.
    - **SVIP Node ID**: The node holding the master SVIP address.
    - **Element Version**: The version of NetApp Element software that the cluster is running.
    - **VASA 2 Status**: The status of the VASA Provider on Element cluster.
    - **VASA Provider URL**: The URL of the VASA Provider enabled on the Element cluster, when applicable.
    - **Encryption At Rest Status**: Possible values:
        - Enabling: Encryption at Rest is being enabled.
        - Enabled: Encryption at Rest is enabled.
        - Disabling: Encryption at Rest is being disabled.
        - Disabled: Encryption at Rest is disabled.
    - **Ensemble Nodes**: IPs of the nodes that are part of the database ensemble.
    - **Paired With**: The names of additional clusters that are paired with the local cluster.
    - **SSH Status**: The status of the secure shell. If enabled, the time remaining is displayed.

Edit a cluster profile

You can change the cluster User ID and password from the plug-in extension point.

> This procedure describes how to change the cluster admin user name and password used by the plug-in. You cannot change the cluster admin credentials from the plug-in. See managing cluster administrator user accounts for instructions on changing credentials for a cluster administrator account.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster.
3. Select **Actions**.

4. Select **Edit**.
5. Change any of the following:
   - User ID: The cluster administrator name.
   - Password: The cluster administrator password.

   > ⓘ You cannot change the IP address or FQDN of a cluster after a cluster is added. You also cannot change the assigned Linked Mode vCenter Server for an added cluster. To change the cluster address or associated vCenter Server, you must remove the cluster and add it again.

6. Select **OK**.

Remove a cluster profile

You can remove the profile of a cluster that you no longer want to manage from the vCenter Plug-in using the plug-in extension point.

If you set up a Linked Mode group and want to reassign a cluster to another vCenter Server, you can remove the cluster profile and add it again with a different linked vCenter Server IP.

> ⓘ
> - Beginning with Element vCenter plug-in 5.0, to use vCenter Linked Mode, you register the Element Plug-in from a separate management node for each vCenter Server that manages NetApp SolidFire storage clusters.
> - Using Element vCenter plug-in 4.10 and earlier to manage cluster resources from other vCenter Servers using vCenter Linked Mode is limited to local storage clusters only.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster you want to remove.
3. Select **Actions**.
4. Select **Remove**.
5. Confirm the action.

Enable Encryption at Rest

You can manually enable encryption at rest (EAR) functionality using the plug-in extension point.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Select the cluster on which you want to enable encryption at rest.

3. Select **Actions**.
4. In the resulting menu, select **Enable EAR**.
5. Confirm the action.

Disable Encryption at Rest

You can manually disable encryption at rest (EAR) functionality using the plug-in extension point.

Steps

1. In your vSphere Web Client, open the **Clusters** tabb:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Select the check box for the cluster.
3. Select **Actions**.
4. In the resulting menu, select **Disable EAR**.
5. Confirm the action.

Enable SSH

You can manually enable a Secure Shell (SSH) session using the plug-in extension point. Enabling SSH allows NetApp technical support engineers access to storage nodes for troubleshooting for the duration you determine.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster.
3. Select **Actions**.
4. Select **Enable SSH**.
5. Enter a duration for the SSH session to be enabled in hours up to a maximum of 720.

    ⓘ To continue, you need to enter a value.

6. Select **Yes**.

Change the SSH time limit

You can enter a new duration for an SSH session.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.

   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster.
3. Select **Actions**.
4. Select **Change SSH**.

   The dialog box displays the remaining time for the SSH session.

5. Enter a new duration for the SSH session in hours up to a maximum of 720.

   > To continue, you need to enter a value.

6. Select **Yes**.

Disable SSH

You can manually disable Secure Shell (SSH) access to nodes in the storage cluster using the plug-in extension point.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster.
3. Select **Actions**.
4. Select **Disable SSH**.
5. Select **Yes**.

Set protection domain monitoring

You can manually enable protection domain monitoring using the plug-in extension point. You can select a protection domain threshold based on node or chassis domains.

What you'll need

- The selected cluster must be monitored by Element 11.0 or later to use protection domain monitoring; otherwise, protection domain functions are not available.
- Your cluster must have more than two nodes to use the protection domains feature. Compatibility with two-node clusters is not available.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster.
3. Select **Actions**.

4. Select **Set Protection Domain Monitoring**.
5. Select a failure threshold:
    - **Node**: The threshold beyond which a cluster can no longer provide uninterrupted data during hardware failures at the node level. The node threshold is the system default.
    - **Chassis**: The threshold beyond which a cluster can no longer provide uninterrupted data during hardware failures at the chassis level.
6. Select **OK**.

After you have set monitoring preferences, you can monitor protection domains from the Reporting tab of the NetApp Element Management extension point.

Shut down a cluster

You can manually shut down all active nodes in a storage cluster using the plug-in extension point.

If you want to restart rather than shut down the cluster, you can select all nodes from the Cluster page in the NetApp Element Management extension point and perform a restart.

What you’ll need

You have stopped I/O and disconnected all iSCSI sessions.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster.
3. Select **Actions**.
4. Select **Shutdown**.
5. Confirm the action.

Expand your NetApp HCI infrastructure

You can manually expand your NetApp HCI infrastructure by adding nodes using NetApp HCI. A link to a NetApp HCI UI for scaling your system is provided from the plug-in extension point.

Additional links are provided from the Getting Started and Cluster pages:

- Beginning with Element vCenter plug-in 5.0, select NetApp Element Remote Plugin > Management.
- For Element vCenter plug-in 4.10 and earlier, select the NetApp Element Management extension point.

Steps

1. In your vSphere Web Client, open the **Clusters** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > Clusters**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > Clusters**.
2. Check the cluster.

3. Select **Actions**.
4. Select **Expand your NetApp HCI**.

Find more information

- NetApp HCI Documentation
- SolidFire and Element Resources page

Manage datastores

Using the NetApp Element Plug-in for VMware vCenter Server, you can manage datastores that are backed by Element volumes. You can create, extend, clone, share, or delete datastores. You can also use VAAI UNMAP to allow a cluster to reclaim freed block space from thinly provisioned VMFS datastores.

What you'll need

- To create and manage datastores, you must first create at least one user account.
- To use QoSSIOC service with datastores, you must first configure settings on the QoSSIOC Settings page from plug-in extension point.
  - Configure settings using Element vCenter plug-in 5.0 and later
  - Configure settings using Element vCenter plug-in 4.10 and earlier
- Because datastores are created using the highest VMFS version supported by the selected ESXi host, all cluster members should run the same version of vSphere and ESXi to avoid VMFS compatibility issues.

Options

- Create a datastore
- View the datastore list
- Extend a datastore
- Clone a datastore
- Share a datastore
- Perform VAAI UNMAP
- Delete a datastore

> Monitor datastore operations for completion using task monitoring in vSphere.

Create a datastore

You can create a datastore from the plug-in extension.

What you'll need

- At least one host must be connected to the vCenter Server.
- At least one cluster must be added and running.

> If you are using vCenter Linked Mode, be sure that you have added your cluster with the correct vCenter Server.

- At least one user account must be created.
- To use QoSSIOC service with datastores, you must first configure settings on the QoSSIOC Settings page from the plug-in extension point:
  - Configure settings using Element vCenter Plug-in 5.0 and later
  - Configure settings using Element vCenter Plug-in 4.10 and earlier

Steps

1. In your vSphere Web Client, open the **Management** tab:

   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. From the Datastore page, select **Create Datastore**.
3. Enter a name for the datastore.

   > 💡 Use a unique name for each datastore in a data center. For multiple cluster or vCenter Server environments, use descriptive naming best practices.

4. Select **Next**.
5. Select one or more required hosts for the datastore.

   > ⓘ You need at least one connected host before you can create a new datastore. If your host has multiple initiators, select an initiator or the host to select all initiators. If you are using vCenter Linked Mode, only hosts available to the vCenter Server to which the cluster is assigned are available to select.

6. Select **Next**.
7. In the **Configure Volume** pane, select an existing volume or create a new volume for the new datastore:

Select existing volume

If you select an existing volume, you must meet the following prerequisites:

- To use a volume access group:
  a. Create a new volume with 512e enabled.
  b. Add the volume to an access group that contains the one or more target host initiators.
- To use CHAP:
  a. Ensure CHAP is configured for each target host iSCSI adapter.
  b. Create a new volume with 512e enabled using one of the following options:
     - Use an account with the appropriate CHAP settings for each target host.
     - Create an account and configure the target and initiator secrets.
  c. View the volume details.
  d. Add the volume IQN to each target host iSCSI adapter static discovery table.

Create new volume

a. Enter a name for the volume that backs the datastore.

b. Select a user account from the account list.

c. Enter the total size of the volume you want to create.

> 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

By default, 512 byte emulation is set to ON for all the new volumes.

d. In the **Quality of Service** area, do one of the following:

   i. Under **Policy**, select an existing QoS policy.

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

> QoS policies are best for service environments, for example, with database, application, or infrastructure servers that rarely reboot and need constant equal access to storage. Custom QoSSIOC automation is best for light use VMs, such as virtual desktops or specialized kiosk-type VMs, that may be rebooted, powered on, or powered off daily or several times a day. QoSSIOC automation and QoS policies should not be used together.

> 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.

8. Select **Next**.

9. Configure the authorization type for host access by choosing one of the following:
   - **Use Volume Access Group**: Select to explicitly limit which initiators can see volumes.
   - **Use CHAP**: Select for secure secret-based access with no limits on initiators.
10. Select **Next**.
11. If you selected **Use Volume Access Group**, configure the volume access groups for the selected hosts.

    The volume access groups listed in **Required by Selected Initiators** are already associated with one or more of the host initiators you selected in an earlier step

    a. Select additional volume access groups or create new ones to associate with available initiators:
       - **Available**: Other volume access group options in the cluster.
       - **Create New Access Group**: Enter the name of the new access group and select **Add**.

    b. Select **Next**.

    c. In the **Configure Hosts' Access** pane, associate available host initiators (IQN or WWPN) with the volume access groups you selected in the previous pane. If a host initiator is already associated with a volume access group, the field is read-only for that initiator. If a host initiator does not have a volume access group association, select an option from the list next to the initiator.

    d. Select **Next**.
12. If you want to enable QoSSIOC automation, check **Enable QoS & SIOC** and then configure the QoSSIOC settings.

    > If you are using QoS policies, do not enable QoSSIOC. QoSSIOC will override and adjust QoS values for volume QoS settings.

    If the QoSSIOC service is not available, you must first configure QoSSIOC settings:
    - Configure settings using Element vCenter plug-in 5.0 and later
    - Configure settings using Element vCenter plug-in 4.10 and earlier

    a. Select **Enable QoS & SIOC**.

    b. Configure the **Burst Factor**.

       > The burst factor is a multiple of the IOPS limit (SIOC) setting for the VMDK. If you change the default, make sure to use a burst factor value that will not exceed the maximum burst limit for an Element volume when the burst factor value is multiplied by the IOPS limit for any VMDK.

    c. (Optional) Select **Override Default QoS** and configure the settings.

       > If the Override Default QoS setting is disabled for the datastore, the Shares and Limit IOPS values are automatically set based on the default SIOC settings of each VM.

       > Do not customize the SIOC share limit without also customizing the SIOC IOPS limit.

By default, the maximum SIOC disk shares are set to `Unlimited`. In a large VM environment such as VDI, this can lead to overcommitting maximum IOPS on the cluster. When you enable QoSSIOC, always check the Override Default QoS and set the Limit IOPS option to something reasonable.

13. Select **Next**.
14. Confirm the selections and click **Finish**.
15. To view the progress of the task, use Task Monitoring in vSphere. If the datastore does not appear in the list, refresh the view.

View the datastore list

You can view available datastores on the Datastores page from plug-in extension point.

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   If two or more clusters are added, select the cluster you want to use in the navigation bar.

2. Review the list of datastores.

   Datastores spanning multiple volumes (mixed datastores) are not listed. Datastore views show only datastores that are available on ESXi hosts from the selected NetApp Element cluster.

3. Review the following information:
   - **Name**: The name assigned to the datastore.
   - **Host Name(s)**: The address of each associated host device.
   - **Status**: The possible values `Accessible` or `Inaccessible` indicate whether or not the datastore is currently connected to vSphere.
   - **Type**: The VMware file system datastore type.
   - **Volume Name**: The name assigned to the associated volume.
   - **Volume NAA**: Globally unique SCSI device identifier for the associated volume in NAA IEEE Registered Extended format.
   - **Total Capacity (GB)**: Total formatted capacity of the datastore.
   - **Free Capacity (GB)**: Space that is available for the datastore.
   - **QoSSIOC Automation**: Indicates whether or not QoSSIOC automation is enabled. Possible values:
     - `Enabled`: QoSSIOC is enabled.
     - `Disabled`: QoSSIOC is not enabled.
     - `Max Exceeded`: Volume Max QoS has exceeded the limit value specified.

Extend a datastore

You can extend a datastore to increase volume size using the plug-in extension point. Extending the datastore also extends the VMFS volume related to that datastore.

Steps

1. In your vSphere Web Client, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    > If two or more clusters are added, select the cluster you want to use in the navigation bar.

2. From the Datastores page, select the check box for the datastore you want to extend.
3. Select **Actions**.
4. In the resulting menu, select **Extend**.
5. In the New Datastore Size field, enter the required size for the new datastore and select GB or GiB.

    > Extending the datastore will consume the entire volume's size. The new datastore size cannot exceed the unprovisioned space available on the selected cluster or the maximum volume size the cluster allows.

6. Select **OK**.
7. Refresh the page.

Clone a datastore

You can clone datastores using the plug-in, which includes mounting the new datastore to the desired ESXi server or cluster. You can name the datastore clone and configure its QoSSIOC, volume, host, and authorization type settings.

If virtual machines exist on the source datastore, virtual machines on the clone datastore will be brought into the inventory with new names.

Volume size for the clone datastore matches the size of the volume backing the source datastore. By default, 512 byte emulation is set to ON for all the new volumes.

What you'll need

- At least one host must be connected to vCenter Server.
- At least one cluster must be added and running.

    > If you are using vCenter Linked Mode, be sure that you have added your cluster with the correct vCenter Server.

- Available unprovisioned space must be equal to or more than the source volume size.
- At least one user account must be created.

Steps

1. In your vSphere Web Client, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    ⓘ If two or more clusters are added, select the cluster you want to use in the navigation bar.

2. From the **Datastores** page, select the check box for the datastore you want to clone.
3. Select **Actions**.
4. In the resulting menu, select **Clone**.

    ⓘ If you attempt to clone a datastore that contains virtual machines with attached disks not located on the selected datastore, copies of the virtual machines on the cloned datastore will not be added to the virtual machine inventory.

5. Enter a datastore name.

    💡 Use a unique name for each datastore in a data center. For multiple cluster or vCenter Server environments, use descriptive naming best practices.

6. Select **Next**.
7. Select one or more required hosts for the datastore.

    ⓘ You need at least one connected host before you can create a new datastore. If your host has multiple initiators, select an initiator or the host to select all initiators. If you are using vCenter Linked Mode, only hosts available to the vCenter Server to which the cluster is assigned are available to select.

8. Select **Next**.
9. In the **Configure Volume** pane, do the following:
    a. Enter a name for the new NetApp Element volume that backs the clone datastore.
    b. Select a user account from the account list.

        ⓘ You need at least one existing user account before you can create a volume.

    c. In the **Quality of Service** area, do one of the following:
        - Under **Policy**, select an existing QoS policy, if available.
        - Under **Custom Settings**, set customized minimum, maximum, and burst values for IOPS or use the default QoS values.

        💡 QoS policies are best for service environments, for example, with database, application, or infrastructure servers that rarely reboot and need constant equal access to storage. Custom QoSSIOC automation is best for light use VMs, such as virtual desktops or specialized kiosk-type VMs, that may be rebooted, powered on, or powered off daily or several times a day. QoSSIOC automation and QoS policies should not be used together.

> 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 **Next**.
11. Configure authorization type for host access by selecting one of the following options:
    - **Use Volume Access Group**: Select to explicitly limit which initiators can see volumes.
    - **Use CHAP**: Select for secure secret-based access with no limits on initiators.
12. Select **Next**.
13. If you selected **Use Volume Access Group**, configure the volume access groups for the selected hosts.

    The volume access groups listed in **Required by Selected Initiators** are already associated with one or more of the host initiators you selected in an earlier step.

    a. Select additional volume access groups or create new ones to associate with available initiators:
       - **Available**: Other volume access group options in the cluster.
       - **Create New Access Group**: Enter the name of the new access group and click **Add**.

    b. Select **Next**.

    c. In the **Configure Hosts' Access** pane, associate available host initiators (IQN or WWPN) with the volume access groups you selected in the previous pane.

       If a host initiator is already associated with a volume access group, the field is read-only for that initiator. If a host initiator does not have a volume access group association, select an option from the drop-down list next to the initiator.

    d. Select **Next**.
14. If you want to enable QoSSIOC automation, check the **Enable QoS & SIOC** box and then configure the QoSSIOC settings.

    > If you are using QoS policies, do not enable QoSSIOC. QoSSIOC will override and adjust QoS values for volume QoS settings.

    If the QoSSIOC service is not available, you must first configure settings on the QoSSIOC Settings page from the plug-in extension point:

    - Configure settings using Element vCenter plug-in 5.0 and later
    - Configure settings using Element vCenter plug-in 4.10 and earlier

    a. Select **Enable QoS & SIOC**.

    b. Configure the **Burst Factor**.

       > The burst factor is a multiple of the IOPS limit (SIOC) setting for the VMDK. If you change the default, make sure to use a burst factor value that will not exceed the maximum burst limit for a NetApp Element volume when the burst factor value is multiplied by the IOPS limit for any VMDK.

    c. **Optional**: Select **Override Default QoS** and configure the settings.

If the Override Default QoS setting is disabled for the datastore, the Shares and Limit IOPS values are automatically set based on the default SIOC settings of each VM.

> Do not customize the SIOC share limit without also customizing the SIOC IOPS limit.

> By default, the maximum SIOC disk shares are set to `Unlimited`. In a large VM environment such as VDI, this can lead to overcommitting maximum IOPS on the cluster. When you enable QoSSIOC, always check the Override Default QoS and set the Limit IOPS option to something reasonable.

15. Select **Next**.
16. Confirm the selections and select **Finish**.
17. Refresh the page.

Share a datastore

You can share a datastore with one or more hosts using the plug-in extension point.

Datastores can be shared only among hosts within the same data center.

What you'll need

- At least one cluster must be added and running.

  > If you are using vCenter Linked Mode, be sure that you have added your cluster with the correct vCenter Server.

- There must be more than one host under the selected data center.

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > If two or more clusters are added, select the cluster you want to use in the navigation bar.

2. From the **Datastores** page, select the check box for the datastore you want to share.
3. Select **Actions**.
4. In the resulting menu, select **Share**.
5. Configure authorization type for host access by selecting one of the following options:
   - **Use Volume Access Group**: Select this option to explicitly limit which initiators can see volumes.
   - **Use CHAP**: Select this option for secure secret-based access with no limits on initiators.
6. Select **Next**.
7. Select one or more required hosts for the datastore.

> You need at least one connected host before you can create a new datastore. If your host has multiple initiators, select an initiator or all initiators by selecting the host. If you are using vCenter Linked Mode, only hosts available to the vCenter Server to which the cluster is assigned are available to select.

8. Select **Next**.
9. If you selected Use **Volume Access Group**, configure the volume access groups for the selected hosts.

   The volume access groups listed in **Required by Selected Initiators** are already associated with one or more of the host initiators you selected in an earlier step.

   a. Select additional volume access groups or create new ones to associate with available initiators:
      - **Available**: Other volume access group options in the cluster.
      - **Create New Access Group**: Enter the name of the new access group and click **Add**.

   b. Select **Next**.

   c. In the **Configure Hosts' Access** pane, associate available host initiators (IQN or WWPN) with the volume access groups you selected in the previous pane.

      If a host initiator is already associated with a volume access group, the field is read-only for that initiator. If a host initiator does not have a volume access group association, select an option from the drop-down list next to the initiator.

10. Confirm the selections and select **Finish**.
11. Refresh the page.

Perform VAAI UNMAP

If you want a cluster to reclaim freed block space from thinly provisioned VMFS5 datastores, use the VAAI UNMAP feature.

What you’ll need

- Ensure that the datastore you are using for the task is VMFS5 or earlier. VAAI UNMAP is unavailable for VMFS6 because ESXi performs the task automatically
- Ensure that the ESXi host system settings are enabled for VAAI UNMAP:

  ```
  esxcli system settings advanced list -o/VMFS3/EnableBlockDelete
  ```

  The integer value must be set to 1 to enable.

- If the ESXi host system settings are not enabled for VAAI UNMAP, set the integer value to 1 with this command:

  ```
  esxcli system settings advanced set -i 1 -o /VMFS3/EnableBlockDelete
  ```

Steps

1. In your vSphere Web Client, open the **Management** tab:

   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.

    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    > If two or more clusters are added, select the cluster you want to use in the navigation bar.

2. From the **Datastores** page, select the check box for the datastore on which you want to use VAAI UNMAP..
3. In the resulting menu, select **Actions**.
4. Select **VAAI Unmap**.
5. Select a host by name or IP address.
6. Enter the host user name and password.
7. Confirm the selections and select **OK**.

Delete a datastore

You can delete a datastore using the plug-in extension point. This operation permanently deletes all the files associated with the VMs on the datastore that you want to delete. The plug-in does not delete datastores that contain registered VMs.

1. In your vSphere Web Client, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    > If two or more clusters are added, select the cluster you want to use in the navigation bar.

2. From the **Datastores** page, select the check box for the datastore you want to delete.
3. Select **Actions**.
4. In the resulting menu, select **Delete**.
5. (Optional) If you want to delete the NetApp Element volume that is associated with the datastore, select the **Delete associated volume** check box.

    > You can also choose to retain the volume and later associate it with another datastore.

6. Select **Yes**.

Find more information

- NetApp HCI Documentation
- SolidFire and Element Resources page

Manage volumes

Using the NetApp Element Plug-in for VMware vCenter Serverr, you can create, view, edit, delete, clone, backup or restore volumes for user accounts. You can also manage each volume on a cluster, and add or remove volumes in volume access groups.

Options

- Create a volume
- View volume details
- Edit a volume
- Clone a volume
- Back up or restore volumes
- Delete volumes
- Purge volumes
- Restore deleted volumes

Create a volume

You can create a new volume and associate the volume with a given account (every volume must be associated with an account). This association gives the account access to the volume through the iSCSI initiators using the CHAP credentials. You can also specify QoS settings for a volume during creation.

VMware requires 512e for disk resources. If 512e is not enabled, a VMFS cannot be created.

What you'll need

- At least one cluster must be added and running.
- A user account has been created.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster you intend to use for the task in the navigation bar.
3. Select the **Volumes** sub-tab.
4. From the **Active** view, select **Create Volume**.
5. Enter a name for the volume.

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

6. Enter the total size of the volume you want to create.

    > 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

    > By default, 512 byte emulation is set to ON for all the new volumes. VMware requires 512e for disk resources. If 512e is not enabled, a VMFS cannot be created.

7. Select a user account from the **Account** list.

8. In the **Quality of Service** area, do one of the following:
   - Under **Policy**, select an existing QoS policy, if available.
   - Under **Custom Settings**, set customized minimum, maximum, and burst values for IOPS or use the default QoS values.

     > ⓘ QoS policies are best for service environments, for example, with database, application, or infrastructure servers that rarely reboot and need constant equal access to storage. Custom QoSSIOC automation is best for light use VMs, such as virtual desktops or specialized kiosk-type VMs, that may be rebooted, powered on, or powered off daily or several times a day. QoSSIOC automation and QoS policies should not be used together.
     > After you enable datastore QoSSIOC settings, any QoS settings at the volume level are overridden.
     > 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.

9. Select **OK**.

View volume details

You can review general information for all active volumes on the cluster in the plug-in extension point. You can also see details for each active volume, including efficiency, performance, QoS, as well as associated snapshots.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Click the **Volumes** subtab.

   General information about active volumes is displayed.

4. Check a specific volume.
5. Select **Actions**.
6. Select **View details**.
7. Review the following information:
   - **Volume ID**: The system-generated ID for the volume.
   - **Volume Name**: The name assigned to the volume.
   - **Account**: The name of the account assigned to the volume.
   - **Access Groups**: The name of the volume access group to which the volume belongs.
   - **Access**: The type of access assigned to the volume when it was created.

     Possible values:

     - `Read/Write`: All reads and writes are accepted.

        - `Read Only`: All read activity allowed; no writes allowed.
        - `Locked`: Only Administrator access is allowed.
        - `ReplicationTarget`: Designated as a target volume in a replicated volume pair.
    - **Volume Paired**: Indicates whether or not the volume is part of a volume pairing.
    - **Size (GB)**: The total size in GB of the volume.
    - **Snapshots**: The number of snapshots created for the volume.
    - **QoS Policy**: The name of the user-defined QoS policy.
    - **512e**: Identifies if 512e is enabled on a volume. The value can be either Yes or No.
8. Review details for a specific volume as listed in these sections:
    - General Details section
    - Efficiency section
    - Performance section
    - Quality of Service section
    - Snapshots section

General Details section

- **Name**: The name assigned to the volume.
- **Volume ID**: The system-generated ID for the volume.
- **IQN**: The iSCSI Qualified Name of the volume.
- **Account ID**: The unique account ID of the associated account.
- **Account**: The name of the account assigned to the volume.
- **Access Groups**: The name of the volume access group to which the volume belongs.
- **Size**: The total size in bytes of the volume.
- **Volume Paired**:
  Indicates whether or not the volume is part of a volume pairing.
- **SCSI EUI Device ID**: Globally unique SCSI device identifier for the volume in EUI-64 based 16-byte format.
- **SCSI NAA Device ID**: The globally unique SCSI device identifier for the protocol endpoint in NAA IEEE Registered Extended Format.

Efficiency section

- **Compression**: The compression efficiency score for the volume.
- **Deduplication**: The deduplication efficiency score for the volume.
- **Thin Provisioning**: The thin provisioning efficiency score for the volume.
- **Last Updated**: The date and time of the last efficiency score.

Performance section

- **Account ID**: The unique account ID of the associated account.
- **Actual IOPS**:
  Current actual IOPS to the volume in the last 500 milliseconds.

- **Async Delay**: The length of time since the volume was last synced with the remote cluster.
- **Average IOP Size**: Average size in bytes of recent I/O to the volume in the last 500 milliseconds.
- **Burst IOPS Size**: The total number of IOP credits available to the user. When volumes are not using up to the Max IOPS, credits are accrued.
- **Client Queue Depth**: The number of outstanding read and write operations to the volume.
- **Last Updated**: The date and time of the last performance update.
- **Latency USec**: The average time, in microseconds, to complete operations to the volume in the last 500 milliseconds. A "0" (zero) value means there is no I/O to the volume.
- **Non-zero Blocks**: Total number of 4KiB blocks with data after the last garbage collection operation has completed.
- **Performance Utilization**: The percentage of cluster IOPS being consumed. For example, a 250K IOP cluster running at 100K IOPS would show 40% consumption.
- **Read Bytes**: The total cumulative bytes read from the volume since the creation of the volume.
- **Read Latency USec**: The average time, in microseconds, to complete read operations to the volume in the last 500 milliseconds.
- **Read Operations**: The total read operations to the volume since the creation of the volume.
- **Thin Provisioning**: The thin provisioning efficiency score for the volume.
- **Throttle**: A floating value between 0 and 1 that represents how much the system is throttling clients below their maxIOPS because of re-replication of data, transient errors and snapshots taken.
- **Total Latency USec**: The time, in microseconds, to complete read and write operations to a volume.
- **Unaligned Reads**: For 512e volumes, the number of read operations that were not on a 4k sector boundary. High numbers of unaligned reads may indicate improper partition alignment.
- **Unaligned Writes**: For 512e volumes, the number of write operations that were not on a 4k sector boundary. High numbers of unaligned writes may indicate improper partition alignment.
- **Used Capacity**: Percentage of used capacity.
- **Volume ID**: The system-generated ID for the volume.
- **Vol Access Groups**: The volume access group IDs that are associated with the volume.
- **Volume Utilization**: A percentage value that describes how much the client is using the volume.
  Possible values:
  - 0: Client is not using the volume.
  - 100: Client is using their max.
  - >100: Client is using their burst.
- **Write Bytes**: The total cumulative bytes written to the volume since the creation of the volume.
- **Write Latency USec**: The average time, in microseconds, to complete write operations to a volume in the last 500 milliseconds.
- **Write Operations**: The total cumulative write operations to the volume since the creation of the volume.
- **Zero Blocks**: Total number of 4KiB blocks without data after the last round of garbage collection operation has completed.

Quality of Service section

- **Policy**: The name of the QoS policy assigned to the volume.

- **I/O Size**: The size of the IOPS in KB.
- **Min IOPS**: The minimum number of sustained inputs and outputs per second (IOPS) that the cluster provides to a volume. The Min IOPS configured for a volume is the guaranteed level of performance for a volume. Performance does not drop below this level.
- **Max IOPS**: maximum number of sustained IOPS that the cluster provides to a volume. When cluster IOPS levels are critically high, this level of IOPS performance is not exceeded.
- **Burst IOPS**: The maximum number of IOPS allowed in a short burst scenario. If a volume has been running below the Max IOPS, burst credits are accumulated. When performance levels become very high and are pushed to maximum levels, short bursts of IOPS are allowed on the volume.
- **Max Bandwidth**: The maximum bandwidth permitted by the system to process larger block sizes.

Snapshots section

- **Snapshot ID**: System generated ID for the snapshot.
- **Snapshot Name**: User-defined name for the snapshot.
- **Create Date**: The date and time at which the snapshot was created.
- **Expiration Date**: day and time the snapshot will be deleted.
- **Size**: User-defined size of the snapshot in GB.

Edit a volume

You can change volume attributes such as QoS values, volume size, and the unit of measurement in which byte values are calculated. You can also change access levels and which account can access the volume. You can also modify account access for replication usage or to restrict access to the volume.

If you are using persistent volumes with the management node, do not modify the names of the persistent volumes.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Click the **Volumes** subtab.
4. From the **Active** view, check the volume.
5. Select **Actions**.
6. Select **Edit**.
7. **Optional**: In the **Volume Size** field, enter a different volume size in GB or GiB.

   > ⓘ You can increase, but not decrease, the size of the volume. If you are adjusting volume size for replication, you should 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.

8. **Optional**: Select a different user account.

9. **Optional**: Select a different access level of one of the following:
    - Read/Write
    - Read Only
    - Locked
    - Replication Target
10. In the **Quality of Service** area, do one of the following:
    - Under Policy, select an existing QoS policy, if available.
    - Under Custom Settings, set customized minimum, maximum, and burst values for IOPS or use the default QoS values.

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

    > QoS policies are best for service environments, for example, with database, application, or infrastructure servers that rarely reboot and need constant equal access to storage. Custom QoSSIOC automation is best for light use VMs, such as virtual desktops or specialized kiosk-type VMs, that may be rebooted, powered on, or powered off daily or several times a day. QoSSIOC automation and QoS policies should not be used together.
    >
    > After you enable datastore QoSSIOC settings, any QoS settings at the volume level are overridden.
    >
    > 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.

11. Select **OK**.

Clone a volume

You can create a clone of a volume 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. This 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.

What you’ll need

- At least one cluster must be added and running.
- At least one volume must be created.
- At least one user account must be created.
- Available unprovisioned space must be equal to or more than the source 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.

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

Operating systems differ in how they treat cloned volumes. ESXi will treat a cloned volume as a volume copy or snapshot volume. The volume will be an available device to use to create a new datastore. For more information on mounting clone volumes and handling snapshot LUNs, see VMware documentation about mounting a VMFS datastore copy and managing duplicate VMFS datastores.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Check the volume you want to clone.
4. Select **Actions**.
5. Select **Clone**.
6. Enter a volume name for the newly cloned volume.

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

7. Select a size in GB or GIB for the cloned 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

     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.

8. Select an account to associate with the newly cloned volume.
9. Select the one of the following access types for the newly cloned volume:
   - Read/Write
   - Read Only
   - Locked
10. Adjust 512e settings, if required.

    ⓘ By default, 512 byte emulation is enabled for all new volumes. VMware requires 512e for disk resources. If 512e is not enabled, a VMFS cannot be created and volume details are grayed out.

11. Select **OK**.

ⓘ 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.

Back up or restore volumes

You can configure the system to back up and restore the contents of a volume to and from an object store container that is external to NetApp Element software-based storage.

You can also back up and restore data to and from remote NetApp Element software-based systems. You can run a maximum of two backup or restore processes at a time on a volume.

Back up volumes

You can back up NetApp Element volumes to Element storage, as well as secondary object stores that are compatible with Amazon S3 or OpenStack Swift.

Back up a volume to an Amazon S3 object store

You can back up NetApp Element volumes to external object stores that are compatible with Amazon S3.

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.
4. From the **Active** view, check the volume.
5. Select **Actions**.
6. Select **Back Up to**.
7. Under **Back up volume to**, select **Amazon S3**.
8. Select an option under with the following data format:
   - Native: A compressed format readable only by NetApp Element software-based storage systems.
   - Uncompressed: An uncompressed format compatible with other systems.
9. In the **Host name** field, enter a host name to use to access the object store.
10. In the **Access key ID** field, enter an access key ID for the account.
11. In the **Secret access key** field, enter the secret access key for the account.
12. In the **Amazon S3 bucket** field, enter the S3 bucket in which to store the backup.
13. **Optional**: In the **Prefix** field, enter a prefix for the backup volume name.
14. **Optional**: In the **Nametag** field, enter a nametag to append to the prefix.
15. Select **OK**.

Back up a volume to an OpenStack Swift object store

You can back up NetApp Element volumes to external object stores that are compatible with OpenStack Swift.

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.
4. From the **Active** view, check the volume.
5. Select **Actions**.
6. Select **Back Up to**.
7. Under **Back up volume to**, select **OpenStack Swift**.
8. Select an option under with the following data format:
   - Native: A compressed format readable only by NetApp Element software-based storage systems.
   - Uncompressed: An uncompressed format compatible with other systems.
9. In the **URL** field, enter a URL to use to access the object store.
10. In the **User name** field, enter a user name for the account.
11. In the **Authentication key** field, enter the authentication key for the account.
12. In the **Container** field, enter the container in which to store the backup.
13. **Optional**: In the **Prefix** field, enter a prefix for the backup volume name.
14. **Optional**: In the **Nametag** field, enter a nametag to append to the prefix.
15. Select **OK**.

Back up a volume to a cluster running Element software

You can back up volumes residing on a cluster running NetApp Element software to a remote Element cluster.

When backing up or restoring from one cluster to another, the system generates a key to be used as authentication between the clusters.

This bulk volume write key enables the source cluster to authenticate with the destination cluster, providing security when writing to the destination volume. As part of the backup or restore process, you need to generate a bulk volume write key from the destination volume before starting the operation.

This is a two-part procedure:

- (Destination) Set up the backup volume
- (Source) Back up a volume

Set up the backup volume

1. From the vCenter and cluster where you want to place the volume backup, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.

4. From the **Active** view, check the volume.
5. Select **Actions**.
6. Select **Restore from**.
7. Under **Restore from**, select **NetApp Element**.
8. Select an option under with the following data format:
    - Native: A compressed format readable only by NetApp Element software-based storage systems.
    - Uncompressed: An uncompressed format compatible with other systems.
9. Click **Generate Key** to generate a bulk volume write key for the destination volume.
10. Copy the bulk volume write key to your clipboard to apply to later steps on the source cluster.

Back up a volume

1. From the vCenter and cluster that contains the source volume to be used for the backup, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.
4. From the **Active** view, check the volume.
5. Select **Actions**.
6. Select **Back Up to**.
7. Under **Back up volume to**, select **NetApp Element**.
8. Select the same option as the destination cluster with the following data format:
    - Native: A compressed format readable only by NetApp Element software-based storage systems.
    - Uncompressed: An uncompressed format compatible with other systems.
9. In the **Remote cluster MVIP** field, enter the management virtual IP address of the destination volume’s cluster.
10. In the **Remote cluster user name** field, enter the cluster administrator user name for the destination cluster.
11. In the **Remote cluster user password** field, enter the cluster administrator password for the destination cluster.
12. In the **Bulk volume write key** field, paste the key you generated on the destination cluster.
13. Select **OK**.

Restore volumes

When you restore a volume from a backup on an object store such as OpenStack Swift or Amazon S3, you need manifest information from the original backup process. If you are restoring a NetApp Element volume that was backed up on a NetApp Element-based storage system, the manifest information is not required. You can find the required manifest information for restoring from Swift and S3 in the Event Log on the Reporting tab.

Restore a volume from backup on an Amazon S3 object store

You can restore a volume from a backup on an Amazon S3 object store using the plug-in.

1. From the vCenter Plug-in, open the **Reporting** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Reporting**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Reporting**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Event Log** subtab.
4. Select the backup event that created the backup you need to restore.
5. Select **Details** for the event.
6. Select **View Details**.
7. Copy the manifest information to your clipboard.
8. Select **Management > Volumes**.
9. From the **Active** view, check the volume.
10. Select **Actions**.
11. Select **Restore from**.
12. Under **Restore from**, select **Amazon S3**.
13. Select an option with the following data format:
    - Native: A compressed format readable only by NetApp Element software-based storage systems.
    - Uncompressed: An uncompressed format compatible with other systems.
14. In the **Host name** field, enter a host name to use to access the object store.
15. In the **Access key ID** field, enter an access key ID for the account.
16. In the **Secret access key** field, enter the secret access key for the account.
17. In the **Amazon S3 bucket** field, enter the S3 bucket where the backup is stored.
18. Paste the manifest information into the **Manifest** field.
19. Select **OK**.

Restore a volume from backup on an OpenStack Swift object store

You can restore a volume from a backup on an OpenStack Swift object store using the plug-in.

1. From the vCenter Plug-in, open the **Reporting** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Reporting**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Reporting**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Event Log** subtab.
4. Select the backup event that created the backup you need to restore.
5. Select **Details** for the event.

6. Select **View Details**.
7. Copy the manifest information to your clipboard.
8. Select **Management > Volumes**.
9. From the **Active** view, check the volume.
10. Select **Actions**.
11. Select **Restore from**.
12. Under **Restore from**, select **OpenStack Swift**.
13. Select an option with the following data format:
    - Native: A compressed format readable only by NetApp Element software-based storage systems.
    - Uncompressed: A compressed format compatible with other systems.
14. In the **URL** field, enter a URL to use to access the object store.
15. In the **User name** field, enter a user name for the account.
16. In the **Authentication key** field, enter the authentication key for the account.
17. In the **Container** field, enter the name of the container in which the backup is stored.
18. Paste the manifest information into the **Manifest** field.
19. Select **OK**.

Restore a volume from backup on a cluster running Element software

You can restore a volume from a backup on a cluster running NetApp Element software. When backing up or restoring from one cluster to another, the system generates a key to be used as authentication between the clusters. This bulk volume write key allows the source cluster to authenticate with the destination cluster, providing security when writing to the destination volume. As part of the backup or restore process, you need to generate a bulk volume write key from the destination volume before starting the operation.

This is a two-part procedure:

- (Destination cluster) Select the volume to use for the restore
- (Source cluster) Restore the volume

Select the volume to use for the restore

1. From the vCenter and cluster where you want to restore the volume, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.
4. From the **Active** view, check the volume.
5. Select **Actions**.
6. Select **Restore from**.
7. Under **Restore from**, select **NetApp Element**.
8. Select an option under with the following data format:

    - Native: A compressed format readable only by NetApp Element software-based storage systems.
    - Uncompressed: An uncompressed format compatible with other systems.
9. Click **Generate Key** to generate a bulk volume write key for the destination volume.
10. Copy the bulk volume write key to your clipboard to apply to later steps on the source cluster.

Restore the volume

1. From the vCenter and cluster that contains the source volume to be used for the restore, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.
4. From the **Active** view, check the volume.
5. Select **Actions**.
6. Select **Back Up to**.
7. Under **Back up volume to**, select **NetApp Element**.
8. Select the option that matches the backup with the following data format:
    - Native: A compressed format readable only by NetApp Element software-based storage systems.
    - Uncompressed: An uncompressed format compatible with other systems.
9. In the **Remote cluster MVIP** field, enter the management virtual IP address of the destination volume's cluster.
10. In the **Remote cluster user name** field, enter the cluster administrator user name for the destination cluster.
11. In the **Remote cluster user password** field, enter the cluster administrator password for the destination cluster.
12. In the **Bulk volume write key** field, paste the key you generated on the destination cluster.
13. Select **OK**.

Delete volumes

You can delete one or more volumes from a NetApp Element cluster using the plug-in extension point.

The system does not immediately purge a deleted volume. A deleted volume can be restored for approximately eight hours.

You can restore a volume before the system purges it or manually purge the volume from the Deleted view in **Management** > **Volumes**. When you restore a volume, it comes back online and iSCSI connections are restored.

> 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 a volume used to create a snapshot is deleted, its associated snapshots are listed in the Inactive view on the Protection > Snapshots page. When the deleted source volumes are purged, the snapshots in Inactive view are also removed from the system.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.
4. Delete one or more volumes:
   a. From the **Active** view, check the volume you want to delete.
   b. Select **Actions**.
   c. Select **Delete**.

   ⓘ The plug-in does not allow a volume with a datastore to be deleted.
5. Confirm the action.

   The volume moves from the Active view to the Deleted view in the Volumes page.

Purge volumes

You can manually purge volumes after you have deleted them.

The system automatically purges deleted volumes eight hours after deletion. However, if you want to purge a volume before the scheduled purge time, you can perform a manual purge using the following steps.

ⓘ When a volume is purged, it is immediately and permanently removed from the system. All data in the volume is lost.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.
4. Select the view filter and select **Deleted** from the list.
5. Select one or more volumes you want to purge.
6. Select **Purge**.
7. Confirm the action.

Restore deleted volumes

You can restore a volume in the NetApp Element system if it has been deleted but not yet purged.

The system automatically purges a volume approximately eight hours after it has been deleted. If the system has purged the volume, you cannot restore it.

> ⓘ If a volume is deleted and then restored, ESXi will not detect the restored volume (and datastore if it exists). Remove the static target from the ESXi iSCSI adapter and rescan the adapter.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.
2. If two or more clusters are added, select the cluster in the navigation bar.
3. Select the **Volumes** subtab.
4. Select the view filter and select **Deleted** from the list.
5. Select one or more volumes you want to restore.
6. Select **Restore**.
7. Select the view filter and select **Active** from the list.
8. Verify that the volume or volumes and all connections are restored.

Find more information

- NetApp HCI Documentation
- SolidFire and Element Resources page

Create and manage user accounts

User accounts are used to control access to the storage resources on a NetApp Element software-based network.

Options

- Create an account
- Edit an account
- Delete an account

Create an account

You can create a unique user account to allow access to storage volumes.

What you'll need

- At least one cluster must be added and running.

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Accounts** sub-tab.
3. Select **Create Account**.
4. Enter a user name.

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

5. In the **CHAP Settings** section:
   a. Enter the initiator secret for CHAP node session authentication.
   b. Enter the target secret for CHAP node session authentication.

   > Initiator and target secrets must differ. If these fields are left blank, the system generates the authentication credentials.

6. Click **OK** to create the account.

Edit an account

You can edit a user account to change the status or the CHAP secrets. Changing CHAP settings can cause lost connectivity between a host and its associated volumes.

About this task

If you are using persistent volumes with the management node, do not modify the account name of the account associated with these volumes.

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Accounts** sub-tab.
3. Select the check box for the account you want to edit.
4. Select **Actions**.
5. In the resulting menu, select **Edit**.

6. Change the following as required:
    a. Edit the access status of the account.

        Changing the access to **Locked** terminates all iSCSI connections to the account, and the account is no longer accessible. Volumes associated with the account are maintained; however, the volumes are not iSCSI-discoverable.

    b. Edit the initiator secret or target secret credentials used for node session authentication.

        If you do not change the credentials, they remain the same. If you make the credentials fields blank, the system generates new passwords.

7. Click **OK**.

Delete an account

You can delete user accounts using the plug-in extension point.

What you'll need

Delete and purge any volumes associated with the account or reassign the volumes to another account.

If you are using persistent volumes with the management node, do not delete the account associated with these volumes.

Steps

1. In your vSphere Web Client, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Accounts** sub-tab.
3. Select the check box for the account you want to delete.
4. Click **Actions**.
5. In the resulting menu, select **Delete**.
6. Confirm the action.

Find more information

- NetApp HCI Documentation
- SolidFire and Element Resources page

Create and manage volume access groups

A volume access group is a collection of volumes that users can access using either iSCSI initiators or FC initiators.

You can create access groups by mapping iSCSI initiator IQNs or FC WWPNs in a collection of volumes. Each IQN that you add to an access group can access each volume in the group without requiring CHAP authentication. Each WWPN that you add to an access group enables FC network access to the volumes in the access group.

Options

- Create an access group
- Edit an access group
- Add volumes to an access group
- Remove volumes from an access group
- Delete an access group

Create an access group

You can create volume access groups with one or more initiators. Mapping Fibre Channel (WWPN) or iSCSI (IQN) client initiators to the volumes in a volume access group enables secure data I/O between a network and a volume.

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Access Groups** sub-tab.
3. Select **Create Access Group**.
4. Enter a name for the volume access group.

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

5. Select an unassigned IQN or WWPN from the **Select an Initiator** drop-down list and click **Add Initiator**.

   Initiators may be added or deleted after the volume access group has been created.

6. Click **OK** to create the access group.

Edit an access group

You can edit volume access group names or add or remove initiators from the plug-in extension point.

Steps

1. In your vSphere Web Client, open the **Management** tab:

- Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
- For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

> If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Access Groups** sub-tab.
3. Select the check box for the volume access group you want to edit.
4. Select **Actions**.
5. In the resulting menu, select **Edit**.
6. Change the following as required:
   a. Modify the access group name.
   b. Add or remove initiators.

   > If you are removing an initiator, click the trash icon to remove it. When you remove the initiator, it can no longer access the volumes in that volume access group. Normal account access to the volume is not disrupted.

7. Select **OK**.

Add volumes to an access group

You can add volumes to a volume access group. Each volume can belong to more than one volume access group; you can see the groups that each volume belongs to from the Active volumes view.

What you'll need

- At least one cluster must be added and running.
- At least one access group exists.
- At least one active volume exists.

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Volumes** subtab.
3. Select the check box for each volume that you want to add to an access group.
4. Select **Actions**.
5. Select **Add to Access Group**.
6. Confirm the details and select a volume access group from the list.

7. Select **OK**.

Remove volumes from an access group

You can remove volumes from an access group.

When you remove a volume from an access group, the group no longer has access to that volume.

> Removing a volume from an access group can disrupt host access to the volume.

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.
2. Select the **Volumes** subtab.
3. Select the check box for each volume that you want to remove from an access group.
4. Select **Actions**.
5. Select **Remove from Access Group**.
6. Confirm the details and select the volume access group that you no longer want to have access to each selected volume.
7. Select **OK**.

Delete an access group

You can delete volume access groups using the plug-in extension point. You do not need to delete initiator IDs or disassociate volumes from the volume access group prior to deleting the group. After you delete the access group, group access to the volumes is discontinued.

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.
2. Select the **Access Groups** sub-tab.
3. Select the check box for the access group you want to delete.
4. Select **Actions**.
5. In the resulting menu, select **Delete**.
6. Confirm the action.

Find more information

- NetApp HCI Documentation
- SolidFire and Element Resources page

Create and manage initiators

Initiators enable external clients access to volumes in a cluster, serving as the entry point for communication between clients and volumes.

You can create, edit, 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.

Options

- Create an initiator
- Edit an initiator
- Add initiators to an access group
- Delete an initiator

Create an initiator

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

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Initiators** sub-tab.
3. Select **Create Initiator**.
4. To create a single initiator:
   a. Select **Create a Single Initiator**.
   b. Enter the IQN or WWPN for the initiator in the **IQN/WWPN** field.

      The accepted format of an initiator IQN is `iqn.yyyy-mm` where y and m are digits followed by text that 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
```

c. Enter a friendly name for the initiator in the **Alias** field.

5. To create multiple initiators:
   a. Select **Create Multiple Initiators**.
   b. Do one of the following:
      - Click **Scan Hosts** to scan vSphere hosts for initiator values not defined in the NetApp Element cluster.
      - Enter a list of IQNs or WWPNs in the text box, and select **Add Initiators**.
   c. (Optional) Under the **Alias** heading, select the field for each entry to add an alias.
   d. (Optional) Remove an initiator from the list, as required.
6. Click **OK** to create the initiator.

Edit an initiator

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

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.
2. Select the **Initiators** sub-tab.
3. Select the check box for the initiator you want to edit.
4. Select **Actions**.
5. In the resulting menu, select **Edit**.
6. Enter a new alias for the initiator in the **Alias** field.
7. Click **OK**.

Add initiators to an access group

You can add initiators to an access group to allow access to volumes in the volume access group without requiring CHAP authentication. When you add an initiator to a volume access group, the initiator has access to all volumes in that volume access group.

Steps

1. In your vSphere Web Client, open the **Management** tab:

    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Initiators** sub-tab.
3. Select the check boxes for the initiators you want to add to an access group.
4. Select **Actions**.
5. In the resulting menu, select **Add to Access Group**.
6. In the **Add to Access Group** dialog box, choose an access group from the drop-down list.
7. Click **OK**.

Delete an initiator

You can delete an initiator after it is no longer needed. 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. In your vSphere Web Client, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the **Initiators** sub-tab.
3. Select the check box for the initiators you want to delete.
4. Select **Actions**.
5. In the resulting menu, select **Delete**.
6. Confirm the action.

Find more information

- NetApp HCI Documentation
- SolidFire and Element Resources page

Set up and manage QoSSIOC for Element volumes and VMware datastores

You can set up QoSSIOC automation for individual volumes and datastores controlled by the plug-in. QoSSIOC is automatic quality of service (QoS) based on Storage I/O Control

(SIOC) settings of all VMs on a standard datastore.

The QoSSIOC service on the management node communicates with vCenter and monitors VM activity on datastores. QoSSIOC adjusts QoS values on standard Element volumes when virtual machine events occur, such as power on or power off events, guest restarts or shutdown, or reconfiguration activity. QoSSIOC is an optional feature and is not required for the plug-in to manage storage clusters.

QoSSIOC is available only with standard datastores. It does not work with virtual volumes (VVols).

> ⓘ You cannot enable virtual volumes (VVols) functionality or make VVols available to vSphere using the QoSSIOC Settings page. See Element Plug-in for vCenter Server documentation about configuring VVols functionality for more information.

For Linked Mode, the Element vCenter plug-in registers all vCenter Servers using the QoSSIOC settings you provide on a single vCenter Server.

Using the vCenter Plug-in, you can configure and manage QoSSIOC by completing the following tasks:

Setup tasks

- Configure QoSSIOC settings
- Enabling QoSSIOC automation on datastores

Management tasks

- Monitor VM performance tiering with QoSSIOC events
- Edit QoSSIOC settings
- Change the QoSSIOC service password
- Disable QoSSIOC automation for a datastore
- Clear QoSSIOC settings

Enabling QoSSIOC automation on datastores

You can enable QoSSIOC automation and customize virtual machine disk (VMDK) performance levels for datastores after you enable the QoSSIOC service for the plug-in.

What you'll need

You have configured the QoSSIOC service settings on the QoSSIOC Settings page and the **QoSSIOC Status** field displays `UP`.

- Configure settings using Element vCenter plug-in 5.0 and later
- Configure settings using Element vCenter plug-in 4.10 and earlier

About this task

QoSSIOC is available only with standard datastores. It does not work with virtual volumes (VVols). QoSSIOC adjusts QoS values on standard Element volumes when virtual machine events occur, such as power on or power off events, guest restarts or shutdown, or reconfiguration activity.

> ⓘ If you are using QoS policies, do not enable QoSSIOC. QoSSIOC will override and adjust QoS values for any volume QoS settings regardless of policy.

Steps

1. In your vSphere Web Client, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Click the status button in the **QoSSIOC Automation** column for the selected datastore.

   > Ensure that the datastore does not have QoSSIOC integration enabled on another vCenter to prevent unexpected changes in QoS.

3. Select **Enable QoS & SIOC**.
4. Configure the **Burst Factor**.

   The burst factor is a multiple of the IOPS limit (SIOC) setting for the VMDK. If you change the default, make sure to use a burst factor value that will not exceed the maximum burst limit for a NetApp Element software-based volume when the burst factor value is multiplied by the IOPS limit for any VMDK.

5. (Optional) Select **Override Default QoS** and configure the settings.

   If the Override Default QoS setting is disabled for the datastore, the Shares and Limit IOPS values are automatically set based on the default SIOC settings of each VM.

   > Do not customize the SIOC share limit without also customizing the SIOC IOPS limit.

   > By default, the maximum SIOC disk shares are set to Unlimited. In a large VM environment such as VDI, this can lead to overcommitting maximum IOPS on the cluster. When you enable QoSSIOC, always check the Override Default QoS and set the Limit IOPS option to something reasonable.

6. Click **OK**.

   When you enable the QoSSIOC Automation for a datastore, the button changes from `Disabled` to `Enabled`.

Edit QoSSIOC settings

You can change the QoSSIOC and vCenter credentials of an active Element management node.

Steps

1. In your vSphere Web Client, open the **QoSSIOC Settings** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > QoSSIOC Settings**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > QoSSIOC Settings**.

2. Select **Actions**.
3. In the resulting menu, select **Edit**.
4. In the **Edit QoSSIOC Settings** dialog box, change any of the following:
    - **QoSSIOC User ID**: The user ID for the QoSSIOC service. The QoSSIOC service default user ID is `admin`. For NetApp HCI, the user ID is the same one entered during installation using the NetApp Deployment Engine.
    - **QoSSIOC Password**: The password for the Element QoSSIOC service. The QoSSIOC service default password is `solidfire`. If you have not created a custom password, you can create one from the registration utility UI (`https://[management node IP]:9443`).

        > For NetApp HCI deployments, the default password is randomly generated during installation. To determine the password, see procedure 4 in this KB article.

    - **vCenter User ID**: The user name for the vCenter admin with full Administrator role privileges.
    - **vCenter Password**: The password for the vCenter admin with full Administrator role privileges.
5. Select **OK**.
   The QoSSIOC Status field displays `UP` when the plug-in can successfully communicate with the service.

> See this KB to troubleshoot if the status is any of the following:
> * `Down`: QoSSIOC is not enabled.
> * `Not Configured`: QoSSIOC settings have not been configured.
> * `Network Down`: vCenter cannot communicate with the QoSSIOC service on the network. The
> mNode and SIOC service might still be running.

> After you have configured valid QoSSIOC settings for the management node, these settings become the default. The QoSSIOC settings revert to the last known valid QoSSIOC settings until you provide valid QoSSIOC settings for a new management node. You must clear the QoSSIOC settings for the configured management node before setting the QoSSIOC credentials for a new management node.

Change the QoSSIOC service password

You can change the password for the QoSSIOC service on the management node using the registration utility UI.

What you'll need

- Your management node is powered on.

About this task

This process describes how to change the QoSSIOC password only. If you want to change the QoSSIOC user name, you can do so from the QoSSIOC Settings page.

Steps

1. In your vSphere Web Client, open the **QoSSIOC Settings** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > QoSSIOC Settings**.

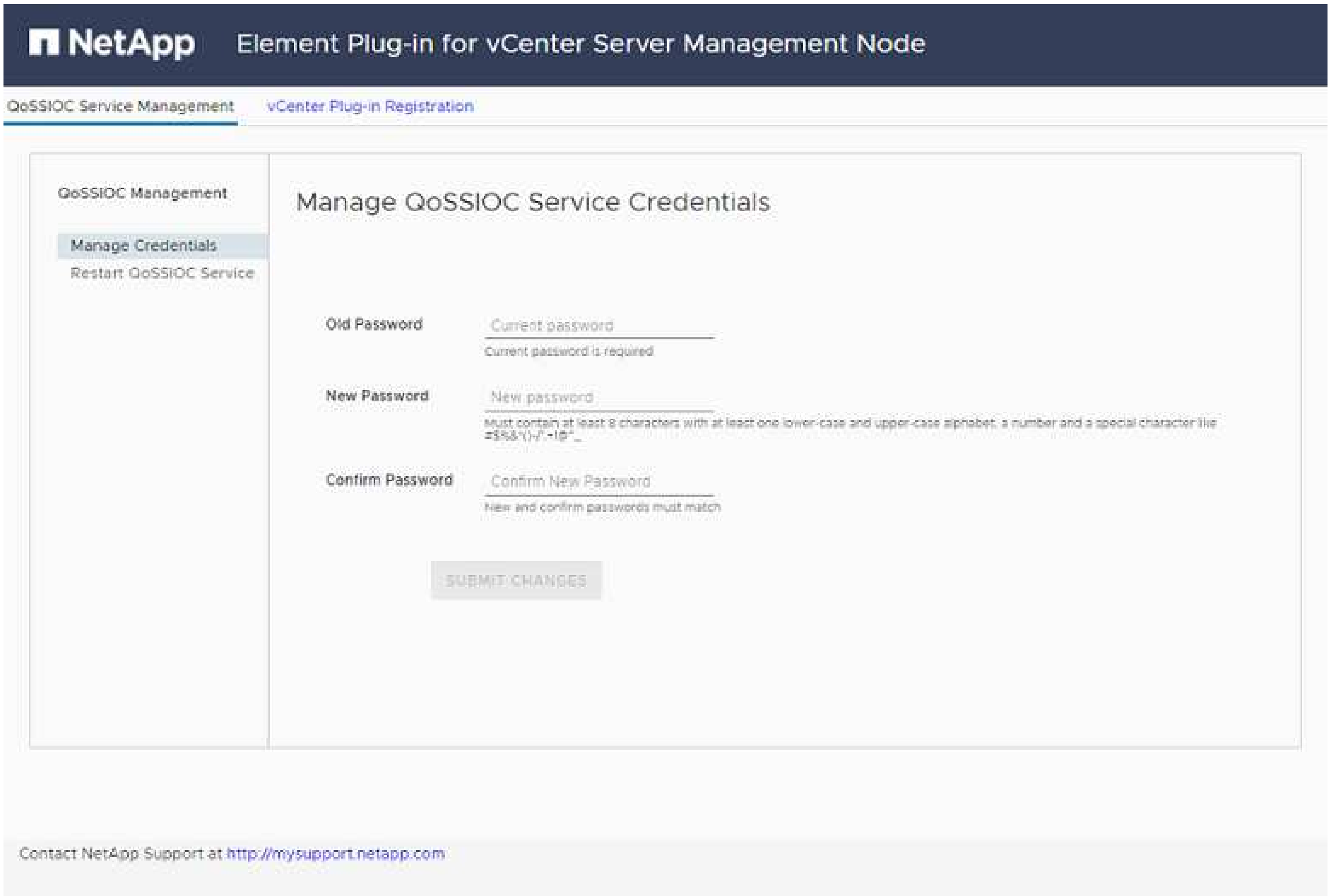
- For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > QoSSIOC Settings**.

2. Select **Actions**.
3. In the resulting menu, select **Clear**.
4. Confirm the action.

   The **QoSSIOC Status** field displays `Not Configured` after the process is complete.

5. Enter the IP address for your management node in a browser, including the TCP port for registration: `https://[management node IP]:9443`.

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


NetApp
Element Plug-in for vCenter Server Management Node
QoSSIOC Service Management
vCenter Plug-in Registration
QoSSIOC Management
Manage Credentials
Restart QoSSIOC Service
SUBMIT CHANGES

Manage QoSSIOC Service Credentials

Old Password: Current password
Current password is required

New Password: New password
Must contain at least 8 characters with at least one lower-case and upper-case alphabet, a number and a special character like =$%&'()-/*.~!@^_

Confirm Password: Confirm New Password
New and confirm passwords must match

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

6. Enter the following information:
   a. **Old Password**: The current password of the QoSSIOC service. If you have not yet assigned a password, type the default password of `solidfire`.

      For NetApp HCI deployments, the default password is randomly generated during installation. To determine the password, see procedure 4 in this KB article.

   b. **New Password**: The new password for the QoSSIOC service.
   c. **Confirm Password**: Enter the new password again.
7. Select **Submit Changes**.

ⓘ The QoSSIOC service automatically restarts after you submit changes.

8. In your vSphere Web Client, select **NetApp Element Configuration > QoSSIOC Settings**.
9. Select **Actions**.
10. In the resulting menu, select **Configure**.
11. In the **Configure QoSSIOC Settings** dialog box, enter the new password in the **QoSSIOC Password** field.
12. Select **OK**.

    The **QoSSIOC Status** field displays `UP` when the plug-in can successfully communicate with the service.

Disable QoSSIOC automation for a datastore

You can disable QoSSIOC integration for a datastore.

Steps

1. In your vSphere Web Client, open the **Management** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Select the button in the **QoSSIOC Automation** column for the selected datastore.
3. Clear the **Enable QoS & SIOC** check box to disable the integration.

    Clearing the Enable QoS & SIOC check box automatically disables the Override Default QoS option.

4. Select **OK**.

Clear QoSSIOC settings

You can clear the QoSSIOC configuration details for the Element storage management node (mNode). You must clear the settings for the configured management node before configuring the credentials for a new management node or changing the QoSSIOC service password. Clearing the QoSSIOC settings removes active QoSSIOC from the vCenter, cluster, and datastores.

Steps

1. In your vSphere Web Client, open the **QoSSIOC Settings** tab:
    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Configuration > QoSSIOC Settings**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Configuration > QoSSIOC Settings**.
2. Select **Actions**.
3. In the resulting menu, select **Clear**.
4. Confirm the action.

The **QoSSIOC Status** field displays `Not Configured` after the process is complete.

Find more information

- NetApp HCI Documentation
- 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.

Using the plug-in extension point, you can configure and manage QoSSIOC by completing the following tasks:

- Create a QoS policy
- Apply a QoS policy to volumes
- Change the QoS policy association 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.

> ⓘ QoSSIOC automation and QoS policies should not be used together. If you are using QoS policies, do not enable QoSSIOC. QoSSIOC will override and adjust QoS values for volume QoS settings.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   > ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Click the **QoS Policies** sub-tab.
3. Click **Create QoS Policy**.
4. Enter the **Policy Name**.

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

5. Enter the minimum IOPS, maximum IOPS, and burst IOPS values.
6. Click **OK**.

Apply a QoS policy to volumes

You can apply an existing QoS policy to multiple volumes. Use this process when you want to bulk apply a policy to one or more volumes.

What you'll need

The QoS policy you want to bulk apply has been created.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Click the **Volumes** sub-tab.
3. Select the check box for each volume to which you want to apply a QoS policy.
4. Click **Actions**.
5. In the resulting menu, select **Apply QoS Policy**.
6. In the dialog box, select the QoS policy from the drop-down list to apply to the selected volumes.
7. Click **OK**.

Change the QoS policy association of a volume

You can remove a QoS policy association from a volume or select a different QoS policy or custom QoS.

What you'll need

The volume you want to modify is associated with a QoS policy.

Steps

1. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Click the **Volumes** sub-tab.
3. Select the check box for a volume that contains a QoS policy you want to modify.
4. Click **Actions**.

5. In the resulting menu, select **Edit**.
6. In the dialog box under **Quality of Service**, select a new QoS policy or custom settings to apply to the volume.
7. If you chose custom settings, modify the **Min IOPS**, **Max IOPS**, and **Burst IOPS** values.

   ⓘ You can also click **Reset Default QoS** to restore default IOPS values.

8. Click **OK**.

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. From the vCenter Plug-in, open the **Management** tab:
   - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
   - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

   ⓘ If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Click the **QoS Policies** sub-tab.
3. Select the check box for the QoS policy you want to edit.
4. Click **Actions**.
5. In the resulting menu, select **Edit**.
6. In the **Edit QoS Policy** dialog box, modify the following properties as needed:
   - **Policy Name**: The user-defined name for the QoS policy.
   - **Min IOPS**: The minimum number of IOPS guaranteed for the volume.
   - **Max IOPS**: The maximum number of IOPS allowed for the volume.
   - **Burst IOPS**: The maximum number of IOPS allowed over a short period of time for the volume. Default = 15,000.

     ⓘ You can also click Reset Default QoS to restore default IOPS values.

7. Click **OK**.

Delete a QoS policy

You can delete a QoS policy if it is no longer needed. When you delete a QoS policy, all volumes associated 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. From the vCenter Plug-in, open the **Management** tab:

    - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Management**.
    - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management**.

    > If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.

2. Click the **QoS Policies** sub-tab.
3. Select the check box for the QoS policy you want to delete.
4. Click **Actions**.
5. In the resulting menu, select **Delete**.
6. Confirm the action.

Find more information

- NetApp HCI Documentation
- SolidFire and Element Resources page

Copyright information

Trademark information