



NetApp Element Plug-in for VMware vCenter Server documentation VCP

NetApp
March 06, 2024

This PDF was generated from <https://docs.netapp.com/us-en/vcp/index.html> on March 06, 2024. Always check docs.netapp.com for the latest.

Table of Contents

NetApp Element Plug-in for VMware vCenter Server documentation	1
NetApp Element Plug-in for VMware vCenter Server product overview	2
NetApp components related to the plug-in	2
Common URLs	2
Find more information	3
Release Notes	4
What's new in NetApp Element Plug-in for VMware vCenter Server	4
Additional release information	5
Concepts	8
NetApp Element Plug-in for VMware vCenter Server 5.0 or later	8
NetApp Element Plug-in for VMware vCenter Server 4.10 or earlier	12
User accounts	15
Protection domains	15
Linked Mode and the vCenter Plug-in	16
QoSSIOC	19
Virtual volumes (vVols)	20
Requirements for the NetApp Element Plug-in for VMware vCenter Server	22
vSphere compatibility and best practices	24
NetApp Element support	24
Network port requirements	24
(Optional) Create a "VCP role" in vCenter	24
Find more information	27
Install and configure the NetApp Element Plug-in for vCenter Server	28
Install and configure Element Plug-in 5.0 and later for vCenter Server 7.0 and later	28
Install and configure Element Plug-in 4.10 and earlier	34
Upgrade the plug-in	43
Find more information	43
Manage storage with the vCenter Plug-in	44
Manage clusters	44
Manage datastores	50
Manage volumes	61
Create and manage user accounts	76
Create and manage volume access groups	78
Create and manage initiators	82
Set up and manage QoSSIOC for Element volumes and VMware datastores	84
Create and manage volume QoS policies	90
Manage cluster hardware and virtual networks	94
Manage cluster hardware and virtual networks overview	94
Add and manage drives	94
Add and manage nodes	96
Create and manage virtual networks	100
Monitor system performance	104
Monitor system performance with Reporting options	104

Monitor overall cluster health on the Overview page	104
Monitor system alerts	106
Monitor event logs for troubleshooting	123
Monitor volume performance	125
Monitor iSCSI sessions to determine connection status	126
Monitor VM performance tiering with QoSSIOC events	127
Protect data with the vCenter Plug-in	129
Protect data with the NetApp Element Plug-in for VMware vCenter Server	129
Create and manage volume snapshots in vCenter Server	129
Create and manage group snapshots in vCenter Server	136
Create snapshot schedules	140
Perform remote replication between clusters	144
Configure and manage virtual volumes	160
Setup tasks	160
Management tasks	160
Enable virtual volumes functionality on the NetApp Element cluster	160
Register the VASA provider with vCenter	161
Create a storage container and associated VVol datastore	162
Monitor virtual volume resources	163
Create a VVol datastore for a storage container	165
Delete a storage container	165
Find more information	166
Unregister the vCenter Plug-in	167
Find more information	168
Remove the vCenter Plug-in	169
Find more information	170
Troubleshoot the vCenter Plug-in	171
Plug-in registration successful but icons do not appear in web client	171
Errors after NetApp Element Plug-in for VMware vCenter Server 4.8 or later upgrade with VMware vCenter Server 6.7U1	172
Error registering plug-in using Registration UI	173
Error updating plug-in using Registration UI	173
Error message that NetApp extension cannot be upgraded	173
Removing plug-in completes successfully but icons remain	173
Plug-in cannot be unregistered or removed after admin password change	174
Plug-in management tasks fail or volumes are not accessible to ESXi host	174
Failure occurs during vCenter Plug-in use on Firefox 59.0.2 browsers	174
Delete datastore operation fails	175
Cluster pair cannot connect using a pairing key	175
Error message for QoSSIOC status	175
QoSSIOC service shown as available but is unavailable	175
QoSSIOC is enabled for datastore but unavailable	176
Earlier versions of NetApp Element Plug-in for VMware vCenter Server documentation	177
Legal notices	178
Copyright	178

Trademarks	178
Patents	178
Privacy policy	178
Open source	178

NetApp Element Plug-in for VMware vCenter Server documentation

NetApp Element Plug-in for VMware vCenter Server product overview

The NetApp Element Plug-in for VMware vCenter Server is a web-based tool integrated with the VMware vSphere Web Client user interface (UI). The plug-in is an extension and alternative scalable, user-friendly interface for VMware vSphere that can manage and monitor storage clusters running **NetApp Element software** software.

You can use the plug-in user interface to discover and configure clusters, and to manage, monitor, and allocate storage from cluster capacity to configure datastores and virtual datastores (for virtual volumes). A cluster appears on the network as a single local group that is represented to hosts and administrators by virtual IP addresses. You can also monitor cluster activity with real-time reporting, including error and alert messaging for any event that might occur while performing various operations.

NetApp components related to the plug-in

- **Registration utility:** A tool that allows you to manage the [QoSSIOC](#) service and plug-in registration with vCenter.



Beginning with Element Plug-in for vCenter 5.0, you register the Element Plug-in from a separate management node for each vCenter Server that manages NetApp SolidFire storage clusters.

- **Management services:** Microservices that include the QoSSIOC service for the vCenter Plug-in. Upgrades to the plug-in are released as part of a management services bundle.



Learn more about [management services releases](#).

- **Management node (mNode):** A virtual machine that runs in parallel with one or more Element software-based storage clusters. As of the Element 11.3 release, management services are hosted on the management node, allowing for quicker updates of select software services outside of major releases.

Common URLs

In addition to vSphere, these are some of the common URLs you use with vCenter plug-in:

URL	Description
<code>https://[management node IP address]:9443</code>	Register the vCenter Plug-in package in the vSphere Web Client.
<code>https://[management node IP address]:442</code>	From the management node per-node UI, access network and cluster settings and utilize system tests and utilities. Learn more .
<code>https://[management node IP address]</code>	Access NetApp Hybrid Cloud Control to upgrade your management services, or expand, monitor, and manage your installation. Learn more .

URL	Description
<code>https://[management node IP address]/mnode</code>	Manually update management services or manage assets using the REST API UI from the management node. Learn more.
<code>https://[storage cluster MVIP address]</code>	Access the NetApp Element software UI.

Find more information

- [NetApp HCI Documentation](#)
- [NetApp HCI Resources page](#)
- [SolidFire and Element Resources page](#)
- [NetApp Element Configuration extension point](#)
- [NetApp Element Configuration extension point](#)
- [NetApp Element Remote Plugin extension point](#)

Release Notes

What's new in NetApp Element Plug-in for VMware vCenter Server

NetApp Element Plug-in for vCenter Server 5.2 contains supportability improvements and an enhancement to the custom Protection Domains display.

With version 5.2, the plug-in displays the Custom Protection Domain Health information when a custom Protection Domain is configured on an Element software cluster. [Learn more.](#)

Element vCenter plug-in 5.2 is available with the 2.24.40 release of management services.

NetApp Element Plug-in for vCenter Server 5.1

NetApp Element Plug-in for vCenter Server 5.1 provides security and performance improvements. [Learn more.](#)

NetApp Element Plug-in for vCenter Server 5.0

NetApp Element Plug-in for vCenter Server 5.0 contains the remote plug-in architecture which is designed to integrate the plug-in functionality into a vSphere Client without having to run inside the vCenter Server. The remote architecture supports plug-in isolation and enables scale-out of plug-ins that operate in large vSphere environments. The remote Element Plug-in is deployed in a docker container inside a management node along with management services. [Learn more.](#)

Element vCenter plug-in 5.0 supports VMware vSphere 8.0, 7.0, and 7.0 Update 1, 2 and 3 including vCenter Server, ESXi, and vSphere HTML5 Web Client.

Element vCenter plug-in 5.0 is available with the 2.22.7 release of management services. If you do not use the plug-in, this is an optional upgrade because all other services and functionalities are identical to version 2.21.61. For information on the latest management services updates, see [Management Services Release Notes 2.21.61](#).

NetApp Element Plug-in for vCenter Server 4.10

Element vCenter plug-in 4.10 contains resolved issues, including security vulnerabilities, that might significantly reduce disruptions seen during upgrades and enhance daily operation in some environments. In version 4.10 of the plug-in, the online help links have transitioned to this [documentation link](#). To access the online help links from within the plug-in, you must have network access.

Element vCenter plug-in 4.10 is available with the 2.21.61 release of management services.

NetApp Element Plug-in for vCenter Server 4.9

NetApp Element Plug-in for vCenter Server 4.9 restores support for vSphere 6.5, including vCenter Server, ESXi, and vSphere HTML5 Web Client.

Element vCenter plug-in 4.9 is available with the 2.20.69 release of management services.

NetApp Element Plug-in for vCenter Server 4.8

Element vCenter plug-in 4.8 contains security improvements, memory utilization improvements, and third-party library upgrades.

Element vCenter plug-in 4.8 is available with the 2.19 release of management services.

NetApp Element Plug-in for vCenter Server 4.7

Element vCenter plug-in 4.7 contains important security improvements that further develop improvements made in the [recent management services 2.17.56 patch](#) release.

With version 4.7, the plug-in now supports components of vSphere 7.0 Update 2, including vCenter Server, ESXi, and vSphere HTML5 Web Client.

Element vCenter plug-in 4.7 is available with the 2.18 release of management services.

NetApp Element Plug-in for vCenter Server 4.6

With version 4.6, the plug-in now supports components of vSphere 7.0 Update 1, including vCenter Server, ESXi, and vSphere HTML5 Web Client.

Element vCenter plug-in 4.6 is available with the 2.16 release of management services.

Find more information

- [Earlier versions of NetApp Element Plug-in documentation](#)
- [Hybrid Cloud Control and Management Services Release Notes KB](#)
- [NetApp HCI Documentation](#)
- [SolidFire and Element Resources page](#)

Additional release information

You can find links to the latest and earlier release notes for various components of the NetApp HCI and Element storage environment.



You will be prompted to log in using your NetApp Support Site credentials.

NetApp HCI

- [NetApp HCI 1.10 Release Notes](#)
- [NetApp HCI 1.9P1 Release Notes](#)
- [NetApp HCI 1.9 Release Notes](#)
- [NetApp HCI 1.8P1 Release Notes](#)
- [NetApp HCI 1.8 Release Notes](#)
- [NetApp HCI 1.7P1 Release Notes](#)

NetApp Element software

- [NetApp Element Software 12.7 Release Notes](#)
- [NetApp Element Software 12.5 Release Notes](#)
- [NetApp Element Software 12.3.2 Release Notes](#)
- [NetApp Element Software 12.3.1 Release Notes](#)
- [NetApp Element Software 12.3 Release Notes](#)
- [NetApp Element Software 12.2 Release Notes](#)
- [NetApp Element Software 12.0 Release Notes](#)
- [NetApp Element Software 11.8 Release Notes](#)
- [NetApp Element Software 11.7 Release Notes](#)
- [NetApp Element Software 11.5.1 Release Notes](#)
- [NetApp Element Software 11.3P1 Release Notes](#)

Management services

- [Management Services Release Notes KB](#)

NetApp Element Plug-in for VMware vCenter Server

- [vCenter Plug-in 5.2 Release Notes](#) *NEW*
- [vCenter Plug-in 5.1 Release Notes](#)
- [vCenter Plug-in 5.0 Release Notes](#)
- [vCenter Plug-in 4.10 Release Notes](#)
- [vCenter Plug-in 4.9 Release Notes](#)
- [vCenter Plug-in 4.8 Release Notes](#)
- [vCenter Plug-in 4.7 Release Notes](#)
- [vCenter Plug-in 4.6 Release Notes](#)
- [vCenter Plug-in 4.5 Release Notes](#)
- [vCenter Plug-in 4.4 Release Notes](#)
- [vCenter Plug-in 4.3 Release Notes](#)

Compute firmware

- [Compute Firmware Bundle 2.146 Release Notes](#)
- [Compute Firmware Bundle 2.76 Release Notes](#)
- [Compute Firmware Bundle 2.27 Release Notes](#)
- [Compute Firmware Bundle 12.2.109 Release Notes](#)

Storage firmware

- [Storage Firmware Bundle 2.146 Release Notes](#)

- [Storage Firmware Bundle 2.99.2 Release Notes](#)
- [Storage Firmware Bundle 2.76 Release Notes](#)
- [Storage firmware Bundle 2.27 Release Notes](#)
- [H610S BMC 3.84.07 Release Notes](#)

Concepts

NetApp Element Plug-in for VMware vCenter Server 5.0 or later

Remote plug-in architecture overview

Beginning with NetApp Element Plug-in for vCenter Server 5.0, the plug-in architecture changes from local to remote. With the introduction of the remote architecture, the plug-in is no longer deployed inside a vCenter server. For Element Plug-in for vCenter Server 4.10 or earlier, the plug-in deployment remains local to the vCenter server to which it is registered.

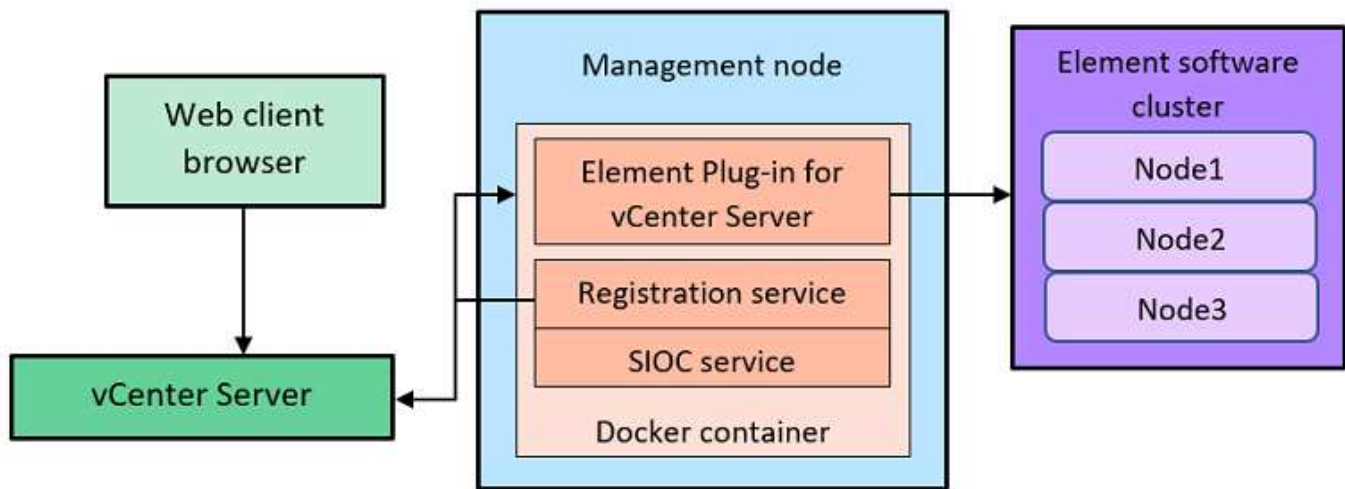
This page describes the implementation of the remote NetApp Element Plug-in for vCenter Server.

The vSphere Client remote plug-in architecture is designed to integrate plug-in functionality into the vSphere Client without having to run inside the vCenter Server. The remote plug-in architecture supports plug-in isolation, enables scale-out of plug-ins that operate in large vSphere environments, and provides the following benefits:

- The plug-in is protected from interference by unstable or compromised plug-ins loaded on the same vSphere Client.
- Plug-in compatibility is robust across vCenter Server upgrades.
- An incompatible plug-in does not interfere with vCenter Server operation.
- You can deploy a number of plug-in versions within the same vSphere environment.
- The remote plug-in user interface only needs to communicate with a single back-end server.
- Deployed plug-in topology is well defined and easy to understand which supports troubleshooting.

Remote Element Plug-in for vCenter Server high level architecture

Using NetApp Hybrid Cloud Control, the remote Element Plug-in is deployed in a docker container inside a management node along with management services.



The remote Element Plug-in vCenter Server, registration service, and storage I/O control (SIOC) service share the same docker service but listen on different ports.

Description	Port
Remote Element Plug-in vCenter Server	8333
Registration service	9443
SIOC Service	8443

Remote Element Plug-in communication paths overview

You must first register the remote plug-in with the vCenter Server using the registration service running on a management node (<https://<mnode-ip>:9443/>). On the registration page, you can see the vCenter server username, password, and the `plugin.json` manifest file path.



The default path is populated in the UI. No action is required.

If the details provided are correct, the registration service registers the plug-in with vCenter Server and enters the vCenter details in the plug-in server database.

After registration completes, the plug-in server downloads the `plugin.json` manifest file and initiates the remote plug-in deployment which involves configuring the remote plug-in as an extension with the `vsphere-ui` client. After the deployment completes, you can access the **NetApp Element Remote Plugin** extension point from the `vsphere-ui` web client.

All communication from the plug-in UI occurs through the vCenter Server which runs a reverse proxy service using HTTPS protocol that is responsible for forwarding the requests for the remote plug-in service. The plug-in server interacts with the SIOC service using HTTPS basic authentication and an Element cluster using the Element Java software development kit (SDK).

Find more information

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

NetApp Element Remote Plugin extension point

Beginning with NetApp Element vCenter plug-in 5.0, you can access the remote Element Plug-in by using the NetApp Element Remote Plugin extension point, which enables you to configure and manage clusters, nodes, and drives and view cluster information.

The following tabs are available from the NetApp Element Remote Plugin extension point:

- [Getting Started](#)
- [Configuration](#)
- [Management](#)
- [About](#)

Getting Started

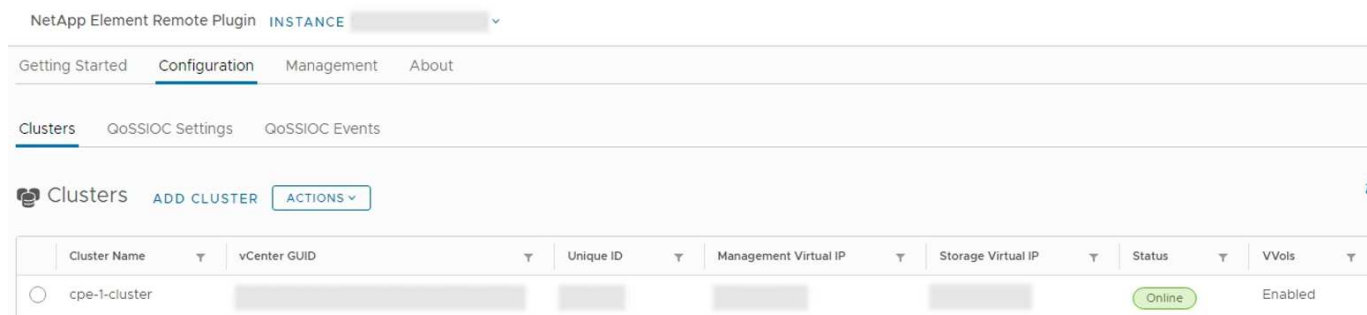
The Getting Started tab introduces the extension points for the plug-in and the actions that can be performed. You can hide the Getting Started pages from each page or restore them from the **About** tab.

Configuration

The **Configuration** tab allows you to add and manage clusters, and configure management node settings for QoSSIOC.



Your vSphere Web Client might differ slightly from what is shown in the following image depending on the version of vSphere installed.



The following tabs are available from the **Configuration** tab:

- **Clusters:** Manages the NetApp Element clusters controlled by the plug-in. You can also enable, disable, or configure cluster-specific features.
- **QoSSIOC Settings:** Configures your credentials for the QoSSIOC service on the management node to communicate with vCenter.
- **QoSSIOC Events:** Displays information about all detected QoSSIOC events.

Management

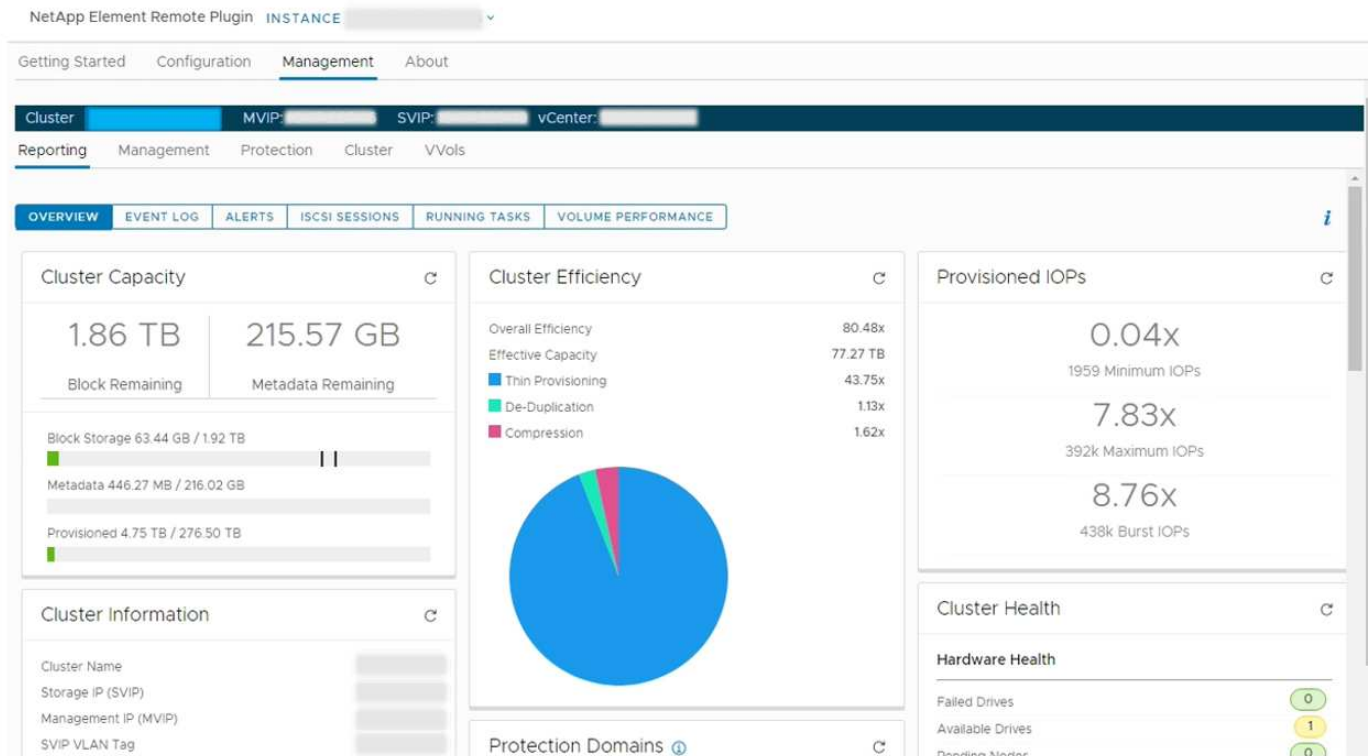
Using the **Management** tab, you can perform the following activities:

- View cluster information

- Manage datastores, volumes, user accounts, access groups, and initiators
- Manage individual group snapshots and add and manage drives and nodes



Your vSphere Web Client might differ slightly from what is shown in the following image depending on the version of vSphere installed.



The cluster navigation bar allows you to quickly switch between clusters that have been added to the plug-in:

- **Cluster:** If two or more clusters are added, ensure that the cluster you intend to use for management tasks is selected in the navigation bar. Select other added clusters from the drop-down list.
- **MVIP:** The management virtual IP address of the selected cluster.
- **SVIP:** The storage virtual IP address of the selected cluster.
- **vCenter:** The vCenter Server which the selected cluster can access. The cluster is assigned access to a vCenter Server when the cluster is added to the plug-in.

The following tabs are available from the **Management** tab:

- **Reporting:** Displays information about cluster components and provides a cluster performance overview. You can also find information about events, alerts, iSCSI sessions, running tasks, and performance volumes from the tab.
- **Management:** Create and manage datastores, volumes, user accounts, access groups, and initiators. You can also perform backup operations, clones, and snapshots. QoS policies are available to be created and managed using NetApp Element software 10 or later.
- **Protection:** Manage individual and group snapshots. You can also create schedules for snapshot creation, pair clusters for real-time replication, and manage volume pairs.
- **Cluster:** Add and manage drives and nodes. You can also create and manage VLANs.
- **VVols:** Manage virtual volumes and their associated storage containers, protocol endpoints, and bindings.

About

Displays plug-in version information and provides a service bundle download option.


Find more information


- [NetApp Element Plug-in for vCenter Server overview](#)
- [NetApp HCI Documentation](#)
- [SolidFire and Element Resources page](#)

NetApp Element Plug-in for VMware vCenter Server 4.10 or earlier

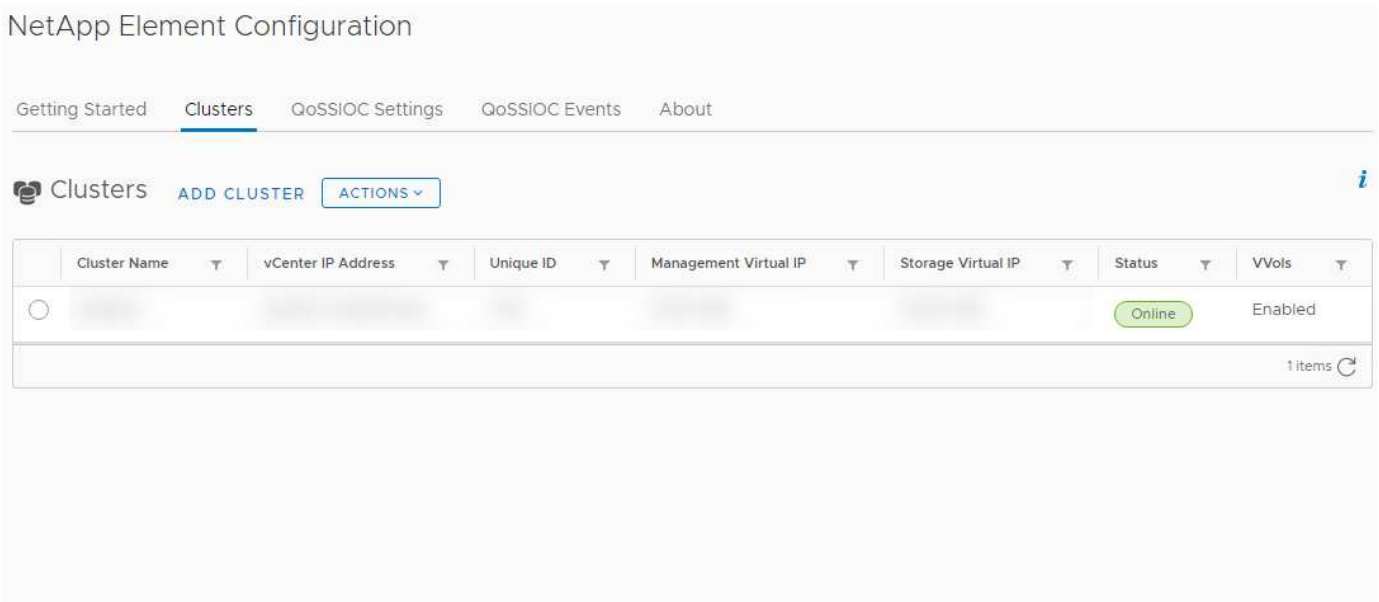
NetApp Element Configuration extension point

The NetApp Element Configuration extension point enables you to add and manage clusters, assign storage clusters to vCenter Servers for Linked Mode, and configure management node settings for QoSSIOC.

- 

Using NetApp Element Plug-in for VMware vCenter Server to manage cluster resources from other vCenter Servers using [vCenter Linked Mode](#) is limited to local storage clusters only.
- 

Your vSphere Web Client might differ slightly from what is shown in the following image depending on the version of vSphere installed.



The following tabs are available from the NetApp Element Configuration extension point:

- **Getting Started:** Introduces the extension points for the plug-in and the actions that can be performed. You can hide Getting Started pages from each page or restore them from the **About** tab in the NetApp Element Configuration extension point.
- **Clusters:** Manages the NetApp Element clusters controlled by the plug-in. You can also enable, disable, or configure cluster-specific features.

- **QoSSIOC Settings:** Configures your credentials for the QoSSIOC service on the management node to communicate with vCenter.
- **QoSSIOC Events:** Displays information about all detected QoSSIOC events.
- **About:** Displays plug-in version information and provides a service bundle download option.

Find more information

- [NetApp Element Management extension point](#)
- [NetApp Element Plug-in for VMware vCenter Server overview](#)
- [NetApp HCI Documentation](#)
- [SolidFire and Element Resources page](#)

NetApp Element Management extension point

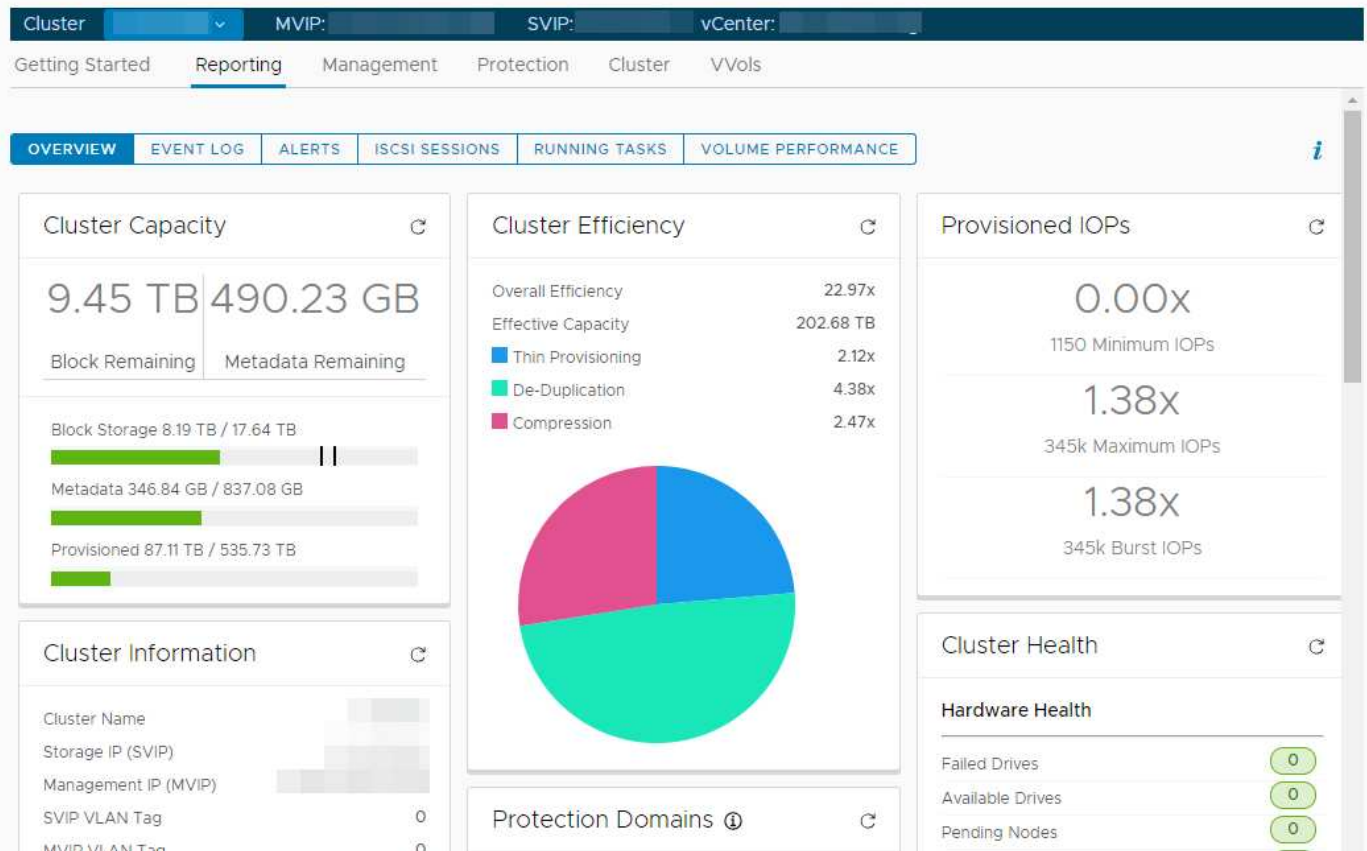
The NetApp Element Management extension point enables you to view cluster information, manage datastores, volumes, user accounts, access groups, and initiators, manage individual group snapshots, and add and manage drives and nodes.



Using NetApp Element Plug-in for VMware vCenter Server to manage cluster resources from other vCenter Servers using [vCenter Linked Mode](#) is limited to local storage clusters only.



Your vSphere Web Client might differ slightly from what is shown in the following image depending on the version of vSphere installed.



The cluster navigation bar allows you to quickly switch between clusters that have been added to the plug-in:

- **Cluster:** If two or more clusters are added, ensure that the cluster you intend to use for management tasks is selected in the navigation bar. Select other added clusters from the drop-down list.
- **MVIP:** The management virtual IP address of the selected cluster.
- **SVIP:** The storage virtual IP address of the selected cluster.
- **vCenter:** The vCenter Server which the selected cluster can access. The cluster is assigned access to a vCenter Server when the cluster is added to the plug-in.

The following tabs are available from the NetApp Element Management extension point:

- **Getting Started:** Introduces the extension points for the plug-in and the actions that can be performed. You can hide Getting Started pages from each page or restore them from the **About** tab in the NetApp Element Management extension point.
- **Reporting:** Displays information about cluster components and provides a cluster performance overview. You can also find information about events, alerts, iSCSI sessions, running tasks, and volume performance from the tab.
- **Management:** Create and manage datastores, volumes, user accounts, access groups, and initiators. You can also perform backup operations, clones, and snapshots. QoS policies are available to be created and managed using NetApp Element software 10 or later.
- **Protection:** Manage individual and group snapshots. You can also create schedules for snapshot creation, pair clusters for real-time replication, and manage volume pairs.
- **Cluster:** Add and manage drives and nodes. You can also create and manage VLANs.

- **VVols:** Manage virtual volumes and their associated storage containers, protocol endpoints, and bindings.

Find more information

- [NetApp Element Configuration extension point](#)
- [NetApp Element Plug-in for VMware vCenter Server overview](#)
- [NetApp HCI Documentation](#)
- [SolidFire and Element Resources page](#)

User accounts

User accounts control access to the storage resources on a NetApp Element software-based network. At least one user account is required before a volume can be created.

When you create a volume, it is assigned to an account. If you have created a virtual volume, the account is the storage container. The account contains the CHAP authentication required to access the volumes assigned to it.

An account can have up to 2000 volumes assigned to it, but a volume can belong to only one account.

Find more information

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

Protection domains

A protection domain is a node or a set of nodes grouped together such that any node or all nodes in

the domain might fail without causing the cluster to lose data availability. The protection domains feature allows you to monitor a cluster's resource capacity to ensure the cluster is still capable of healing from a failure event. You can select monitoring at either a node or chassis domain level:

- **Node level** defines each protection domain per individual node, with each node potentially located across chassis.
- **Chassis level** defines each protection domain by nodes that share a chassis.

A chassis domain requires more potential capacity resources than a node domain to be resilient to failure. When a protection domain threshold is exceeded, a cluster no longer has sufficient capacity to heal from failure while also maintaining uninterrupted data availability.

[Learn more about custom Protection Domains.](#)

Find more information

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

Linked Mode and the vCenter Plug-in

You can use the NetApp Element Plug-in for VMware vCenter Server to manage cluster resources from other vCenter Servers using vCenter Linked Mode.

Element Plug-in for vCenter 5.0 or later

Beginning with Element Plug-in 5.0, you register the Element Plug-in from a separate management node for each vCenter Server that manages NetApp SolidFire storage clusters.

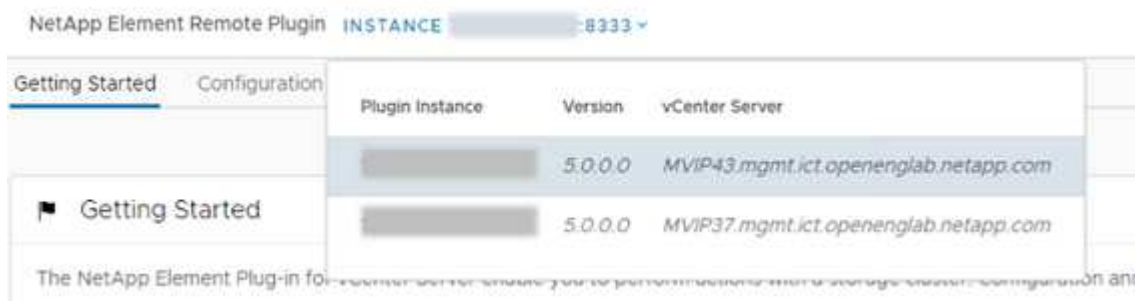
Example

- Register vCenter1: `https://[mnode1]:9443/solidfire-mnode/registration`
- Register vCenter2: `https://[mnode2]:9443/solidfire-mnode/registration`

To set up storage cluster management in a vSphere Linked Mode environment, you can use the following procedure to manually add the storage clusters.

Steps

1. Deploy the Element Plug-in by registering the plug-in from a separate management node for each vCenter Server in the Linked Mode environment that uses the plug-in.
2. Use the Element Plug-in.
 - a. Log in to the web client of any vCenter Server in the Linked Mode environment.
 - b. On the **NetApp Element Remote Plugin** line, select the **Instance** list.



The screenshot shows the 'NetApp Element Remote Plugin' web interface. At the top, there is a tab labeled 'INSTANCE' with a dropdown menu showing '8333'. Below this, there is a table with the following columns: 'Plugin Instance', 'Version', and 'vCenter Server'. The table contains two rows of data. The first row has a greyed-out instance ID, version '5.0.0.0', and vCenter Server 'MVIP43.mgmt.ict.openenglab.netapp.com'. The second row has another greyed-out instance ID, version '5.0.0.0', and vCenter Server 'MVIP37.mgmt.ict.openenglab.netapp.com'. To the left of the table, there is a sidebar with a 'Getting Started' section and a 'Configuration' section. The 'Getting Started' section is currently selected and shows a 'Getting Started' link. Below the sidebar, there is a text area that says 'The NetApp Element Plug-in for vCenter Server enables you to perform management tasks on storage clusters associated with the selected vCenter Server environment.'

Plugin Instance	Version	vCenter Server
[REDACTED]	5.0.0.0	MVIP43.mgmt.ict.openenglab.netapp.com
[REDACTED]	5.0.0.0	MVIP37.mgmt.ict.openenglab.netapp.com

- c. Select the vCenter Server that you want to work with.

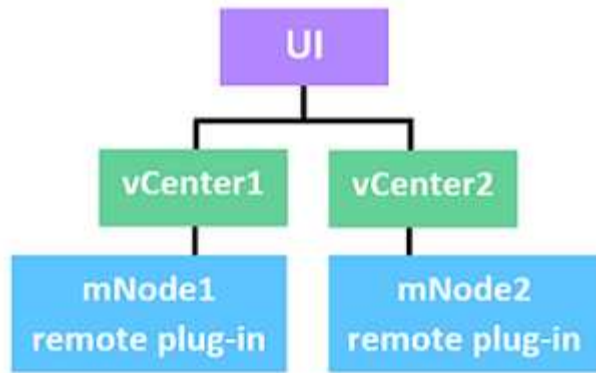
After you have selected the target vCenter Server, you can add and manage the clusters for that vCenter Server environment.



You can only view and manage the storage clusters associated with the selected vCenter Server.

Example

You have vCenter1 and vCenter2 in Linked Mode and storage cluster1 and storage cluster2. You want vCenter1 to manage cluster1 and vCenter2 to manage cluster2.



After registering the plug-in with a separate management node for each vCenter Server, set up the storage cluster management.

Steps

1. Log in to the web client of any vCenter Server in the Linked Mode environment.
2. On the **NetApp Element Remote Plugin** line, select the **Instance** list.
3. To manage cluster1 from the vCenter1 web client, select **vCenter1** from the list.
4. Add cluster1 to the Element Plug-in inventory.
5. On the **NetApp Element Remote Plugin** line, select the **Instance** list
6. To manage cluster2 from the vCenter2 web client, select **vCenter2** from the list.
7. Add cluster2 to the Element Plug-in inventory.

Element Plug-in for vCenter 4.10 or earlier

For Element Plug-in 4.10 or earlier, you can only manage the storage cluster in the Element Plug-in when you are logged in to the destination vCenter web client.

To set up storage cluster management in a vSphere Linked Mode environment, you can use the following procedure to manually add the storage clusters.

Steps

1. Register the plug-in with each vCenter Server in the Linked Mode environment that uses the plug-in.
2. Log in once to the vSphere Web Client for each linked vCenter Server.

Logging in initiates installation of the plug-in on the web client.

3. Log in to the web client of the destination vCenter that you want to manage the storage cluster.
4. Add the storage cluster to the Element Plug-in inventory.

Example

You have vCenter1 and vCenter2 in Linked Mode and storage cluster1 and storage cluster2. You want vCenter1 to manage cluster1 and vCenter2 to manage cluster2. To set up the storage cluster management, after registering the plug-in with each vCenter Server, you perform the following steps:

1. Log in to the vCenter1 web client.
2. To manage cluster1 from the vCenter1 web client, add cluster1 to the Element Plug-in inventory.
3. Log in to the vCenter2 web client.

4. To manage cluster2 from the vCenter2 web client, add cluster2 to the Element Plug-in inventory.

Find more information

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

QoSSIOC

The NetApp Element Plug-in for VMware vCenter Server enables, as an optional setting, automatic quality of service (QoS) based on Storage I/O Control (SIOC) settings of all VMs on a standard datastore. QoS and SIOC integration (QoSSIOC), which can be enabled for any standard datastore, runs a scan of all SIOC settings on all associated VMs.

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. The QoSSIOC service uses the sum of all SIOC reservations or shares and the sum of IOPS limits to determine minimum and maximum QoS for the underlying volume of each datastore. A configurable burst factor is also available.

The following items should be considered before using QoSSIOC automation:

- 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.
- QoSSIOC 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 is less suitable for service environments, for example, with database, application, or infrastructure servers that rarely reboot and need constant equal access to storage. QoS policies are best suited for these environments.
- QoSSIOC is available only with standard datastores. It does not work with virtual volumes (VVols).



When SIOC settings for a VMDK are at the default shares level of Normal and the default IOPS limit of Unlimited, the Shares and Limit IOPS values contribute toward the total QoS for the underlying volume. If the SIOC settings for the VMDK are not at default levels, SIOC shares contribute to Min QoS and SIOC IOPS limit values contribute to Max QoS for the underlying volume.



It is possible to set a reservation value through vSphere API. If a reservation value is set for a VMDK, shares are ignored and the reservation value is used instead.



[SolidFire Active IQ](#) has a QoS recommendations page that provides advice on optimal configuration and set up of QoS settings.

Find more information

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

Virtual volumes (vVols)

vSphere Virtual Volumes is a storage paradigm for VMware that moves much of the storage management for vSphere from the storage system to VMware vCenter. With Virtual Volumes (vVols), you can allocate storage according to the requirements of individual virtual machines.

Bindings

The NetApp Element cluster chooses an optimal protocol endpoint, creates a binding that associates the ESXi host and virtual volume with the protocol endpoint, and returns the binding to the ESXi host. After it is bound, the ESXi host can perform I/O operations with the bound virtual volume.

Protocol endpoints

VMware ESXi hosts use logical I/O proxies known as protocol endpoints to communicate with virtual volumes. ESXi hosts bind virtual volumes to protocol endpoints to perform I/O operations. When a virtual machine on the host performs an I/O operation, the associated protocol endpoint directs I/O to the virtual volume with which it is paired.

Protocol endpoints in a NetApp Element cluster function as SCSI administrative logical units. Each protocol endpoint is created automatically by the cluster. For every node in a cluster, a corresponding protocol endpoint is created. For example, a four-node cluster will have four protocol endpoints.

iSCSI is the only supported protocol for NetApp Element software. Fibre Channel protocol is not supported. Protocol endpoints cannot be deleted or modified by a user, are not associated with an account, and cannot be added to a volume access group. You can review protocol endpoint information using the plug-in extension point:

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

Storage containers

Storage containers are logical constructs that map to NetApp Element accounts and are used for reporting and resource allocation. They pool raw storage capacity or aggregate storage capabilities that the storage system can provide to virtual volumes. A VVol datastore that is created in vSphere is mapped to an individual storage container. A single storage container has all available resources from the NetApp Element cluster by default. If more granular governance for multi-tenancy is required, multiple storage containers can be created.

Storage containers function like traditional accounts and can contain both virtual volumes and traditional volumes. A maximum of four storage containers per cluster is supported. A minimum of one storage container is required to use VVols functionality. You can create, delete, and view details about storage containers using the plug-in extension point:

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

You can also discover storage containers in vCenter during VVols creation.

VASA provider

To make vSphere aware of the vVol feature on the NetApp Element cluster, the vSphere admin must register the NetApp Element VASA Provider with vCenter. The VASA provider is the out-of-band control path between vSphere and the Element cluster. It is responsible for executing requests on the Element cluster on behalf of vSphere, such as creating VMs, making VMs available to vSphere, and advertising storage capabilities to vSphere.

The VASA provider runs as part of the cluster master in Element software. The cluster master is a highly available service that fails over to any node in the cluster as needed. If the cluster master fails over, the VASA provider moves with it, ensuring high availability for the VASA provider. All provisioning and storage management tasks use the VASA provider, which handles any changes needed on the Element cluster.



For Element software 12.5 and earlier, do not register more than one NetApp Element VASA provider to a single vCenter instance. Where a second NetApp Element VASA provider is added, this renders all VVOL datastores inaccessible.



VASA support for up to 10 vCenters is available as an upgrade patch if you have already registered a VASA provider with your vCenter. To install, follow the directions in the VASA39 manifest and download the .tar.gz file from the [NetApp Software Downloads](#) site. The NetApp Element VASA provider uses a NetApp certificate. With this patch, the certificate is used unmodified by vCenter to support multiple vCenters for VASA and VVols use. Do not modify the certificate. Custom SSL certificates are not supported by VASA.

Find more information

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

Requirements for the NetApp Element Plug-in for VMware vCenter Server

Before you use NetApp Element Plug-in for VMware vCenter Server to manage your NetApp HCI or SolidFire all-flash array storage, you must verify that your system meets the requirements for plug-in use.

For vCenter Servers 8.0 and 7.0, you can [create a "VCP role" in vCenter](#) for an Element plug-in user account, and assign permissions to register or upgrade the Element Plug-in for vCenter Server and perform Element plug-in administration tasks.

Element Plug-in for vCenter 5.0 or later

Verify that your system meets the requirements for use of Element vCenter plug-in 5.0 or later.

VMware vSphere prerequisites

VMware vSphere 8.0 and 7.0 including vCenter and ESXi with software iSCSI adapter and iSCSI networking configured, is required to use the Element vCenter plug-in.

VMware vSphere versions supported by the plug-in

The plug-in supports the following major versions of VMware software:

- vSphere 8.0 Update 1 including vCenter Server, ESXi, and VMFS5 and VMFS6 datastores
- vSphere 7.0 and 7.0 Update 1, 2 and 3 including vCenter Server, ESXi, and VMFS5 and VMFS6 datastores



VMware vSphere 6.5 and 6.7 reached end of support status on October 15, 2022. Beginning with Element Plug-in 5.0, vSphere 6.5 and 6.7 are no longer supported. For details, see this [article](#).

Element Plug-in for vCenter 4.10 or earlier

Verify that your system meets the requirements for use of Element vCenter plug-in 4.10 or earlier.

VMware vSphere prerequisites

VMware vSphere 7.0, 6.7, or 6.5 including vCenter and ESXi with software iSCSI adapter and iSCSI networking configured, is required to use the Element vCenter plug-in.

VMware vSphere versions supported by the plug-in

The plug-in supports the following major versions of VMware software:

- vSphere 7.0 and 7.0 Update 1 and 2 including vCenter Server, ESXi, and VMFS5 and VMFS6 datastores
- vSphere 7.0 Update 3 including vCenter Server, ESXi, and VMFS5 and VMFS6 datastores using Spring Framework 4



When you upgrade to VMware vCenter Server 7.0 U3, the Element Plug-in fails to deploy. To resolve this issue using Spring Framework 4, see [this KB article](#).

- vSphere 6.7 and 6.7 Update 1 and 3, including vCenter Server, ESXi, and VMFS5 and VMFS6 datastores



The plug-in is not compatible with version 6.7 U2 build 13007421 of the HTML5 vSphere Web Client and other 6.7 U2 builds released prior to update 2a (build 13643870). It is compatible with the version 6.7 U2 vSphere Web Client for Flash/FLEX.

- vSphere 6.5, including vCenter Server, ESXi, and VMFS5 and VMFS6 datastores



The plug-in is not compatible with version 6.5 for Element Plug-in for vCenter 4.6, 4.7, and 4.8.



End of vSphere 6.0 support

VMware vSphere 6.0 reached end of support status on March 12, 2020. Beginning with NetApp HCI 1.8 and Element 12, vSphere 6.0 is no longer supported. For details, see this [product communiqué](#).

vSphere compatibility and best practices

Consider the following capabilities and recommendations before using the plugin:

- vCenter high availability (VCHA) is not supported.
- 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.
- The vSphere HTML5 Web Client and Flash Web Client have separate databases that cannot be combined. Clusters added in one client will not be visible in the other. If you intend to use both clients, add your clusters in both.

NetApp Element support

The plug-in supports the following major versions:

- Element 12.x
- Element 11.x

Network port requirements

You need to allow some TCP ports through your datacenter's edge firewall so that you can manage the system remotely and allow clients outside of your datacenter to connect to resources. For a comprehensive list of ports used in NetApp HCI and SolidFire systems, see this [page](#).

(Optional) Create a "VCP role" in vCenter

For vCenter Servers 8.0 and 7.0, you can create a "VCP role" in vCenter for an Element plug-in user account, and assign permissions to register or upgrade the Element Plug-in for vCenter Server and perform Element plug-in administration tasks.

Steps

1. Log into the vSphere Web Client as an administrator.
2. Select **Administration**.
3. Select **Single Sign On > Users and Groups**.
4. Select the **Users** tab and from the **Domain** list, select the target domain.
5. Select **Add**.
6. Complete the fields in the **Add User** screen, and select **Add**.

Add User



Username *	<input type="text" value="vcpuser"/>
Password *	<input type="password" value="....."/> ⓘ
Confirm Password *	<input type="password" value="....."/>
First Name	<input type="text" value="vcp"/>
Last Name	<input type="text" value="user"/>
Email	<input type="text"/>
Description	<input type="text" value="User account for VCP administration"/>

CANCEL

ADD

7. Select **Access Control** > **Roles**, and select **New**.
8. In the **New role** screen, complete the following steps:
 - a. Under **Role name**, enter "VCProle".
 - b. Enter a description.
 - c. From the **Show** list, select the permissions for your vCenter Server version:
 - i. Select the permissions for vCenter Server 8.0:
 - Cryptographic operations > Register VM
 - Datastore > Select All
 - Extension > Select All
 - Host > Configuration > Change settings
 - Host > Configuration > Connection
 - Host > Configuration > Maintenance
 - Host > Configuration > Storage partition configuration
 - Host > Configuration > System Management
 - Host > Configuration > System resources
 - Privilege.Task.Update.Task.Update.label > privilege.Task.Update.Task.Update.label
 - Tasks > Select All

- Virtual machine > Edit Inventory > Register
 - VM storage policies > VM storage policies view permissions > View VM storage policies
- ii. Select the permissions for vCenter Server 7.x:
- Cryptographic operations > Register VM
 - Datastore > Select All
 - Extension > Select All
 - Host > Configuration > Change settings
 - Host > Configuration > Connection
 - Host > Configuration > Maintenance
 - Host > Configuration > Storage partition configuration
 - Host > Configuration > System Management
 - Host > Configuration > System Resources
 - Plugin > Select All
 - Scheduled task > Select All
 - Storage Views > Select All
 - Tasks > Select All
- d. Select **Create**.

New Role ✕

Role name

VCProle

Description

Role permissions for the VCP user

Show All

Alarms
AutoDeploy
Certificate Authority
Certificate Management
Certificates
Cns
Compute Policy
Content Library
Cryptographic operations
Datacenter
Datastore

Select all

Show All

Select a category to view its privileges

CANCEL

CREATE

9. Select **Global Permissions**, and select **Add**.
10. In the **Add Permission** screen, complete the following steps:

- a. Select the target domain from the **Domain** list.
- b. In the **User/Group** field, enter the Element plug-in user ID.
- c. Select **VCProle** from the **Role** list.
- d. Select **Propagate to children** and select **OK**.

Add Permission

Global Permission Root

X

Domain

netapp.eng

▼

User/Group

Q vcpuser

Role

VCProle

▼

☒ Propagate to children

You can now log into the vSphere Web Client using the "vcpuser" account.

Find more information

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

Install and configure the NetApp Element Plug-in for vCenter Server

Install and configure Element Plug-in 5.0 and later for vCenter Server 7.0 and later

Beginning with NetApp Element Plug-in for vCenter Server 5.0, you can install the most recent version of the Element Plug-in directly to your vCenter and access the plug-in with the vSphere Web Client.

After installation is complete, you can use the quality of service based on storage I/O control (QoSSIOC) service as well as other services of the vCenter Plug-in.

Read and complete each step to install and begin using the plug-in:

- [Prepare for installation](#)
- [Install the management node](#)
- [Register the plug-in with vCenter](#)
- [Access the plug-in and verify successful installation](#)
- [Add storage clusters for use with the plug-in](#)
- [Configure QoSSIOC settings using the plug-in](#)
- [Configure user accounts](#)
- [Create datastores and volumes](#)

Prepare for installation

Before you begin the installation, review [pre-deployment requirements](#).

Install the management node

You can manually [install the management node](#) for your cluster running NetApp Element software using the appropriate image for your configuration.

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

Register the plug-in with vCenter

Deploying the vCenter Plug-in package in the vSphere Web Client involves registering the package as an extension on vCenter Server. After registration is complete, the plug-in is available to any vSphere Web Client that connects to your vSphere environment.

What you'll need

- You have vCenter Administrator role privileges to register a plug-in.
- You have deployed a management node OVA running Element software 12.3.x or later.
- Your management node is powered on with its IP address or DHCP address configured.

- You are using an SSH client or web browser (Chrome 56 or later or Firefox 52 or later).
- Your firewall rules allow open [network communication](#) between the vCenter and the storage cluster MVIP on TCP ports 443, 8443, 8333, and 9443. Port 9443 is used for registration and can be closed after registration is complete. If you have enabled virtual volumes functionality on the cluster, ensure TCP port 8444 is also open for VASA provider access.

About this task

You must register the vCenter Plug-in on every vCenter Server where you need to use the plug-in.

For Linked Mode environments, you must register separate plug-ins with each vCenter Server in the environment to keep MOB data in sync and to be able to upgrade the plug-in. When a vSphere Web Client connects to a vCenter Server where your plug-in is not registered, the plug-in is not visible to the client.



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.

Steps

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

https://<managementNodeIP>:9443

The registration UI displays the Manage QoSIO 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

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

SUBMIT CHANGES

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

2. **Optional:** Change the password for the QoSSIOC service before registering the vCenter Plug-in:
 - a. For the Old Password, enter the current password of the QoSSIOC service. If you have not yet assigned a password, type the default password:

solidfire

b. Select **Submit Changes**.



After you submit changes, the QoSSIOC service automatically restarts.

3. Select **vCenter Plug-in Registration**.

The screenshot shows the NetApp Element Plug-in for vCenter Server Management Node interface. The page title is "vCenter Plug-in - Registration". On the left, there is a sidebar with the following options: "Manage vCenter Plug-in", "Register Plug-in" (highlighted), "Update Plug-in", "Unregister Plug-in", and "Registration Status". The main content area contains the following fields and instructions:

- vCenter Address:** vCenter Server Address. Enter the IPv4, IPv6 or DNS name of the vCenter server to register plug-in on.
- vCenter User Name:** vCenter Admin User Name. Ensure this user is a vCenter user that has administrative privileges for registration.
- vCenter Password:** vCenter Admin Password. The password for the vCenter user name entered.
- ☐ **Customize URL:** Select to customize the Zip file URL.
- Plug-in Zip URL:** <https://10.117.227.44:8333/vcp-01/plugin.json>. URL of XML initialization file.

At the bottom of the main content area is a **REGISTER** button. At the bottom of the page is a footer that says "Contact NetApp Support at <http://mysupport.netapp.com>".

4. Enter the following information:

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



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

- The vCenter Administrator password.

5. Select **Register**.

6. (Optional) Verify registration status:

a. Select **Registration Status**.

b. Enter the following information:

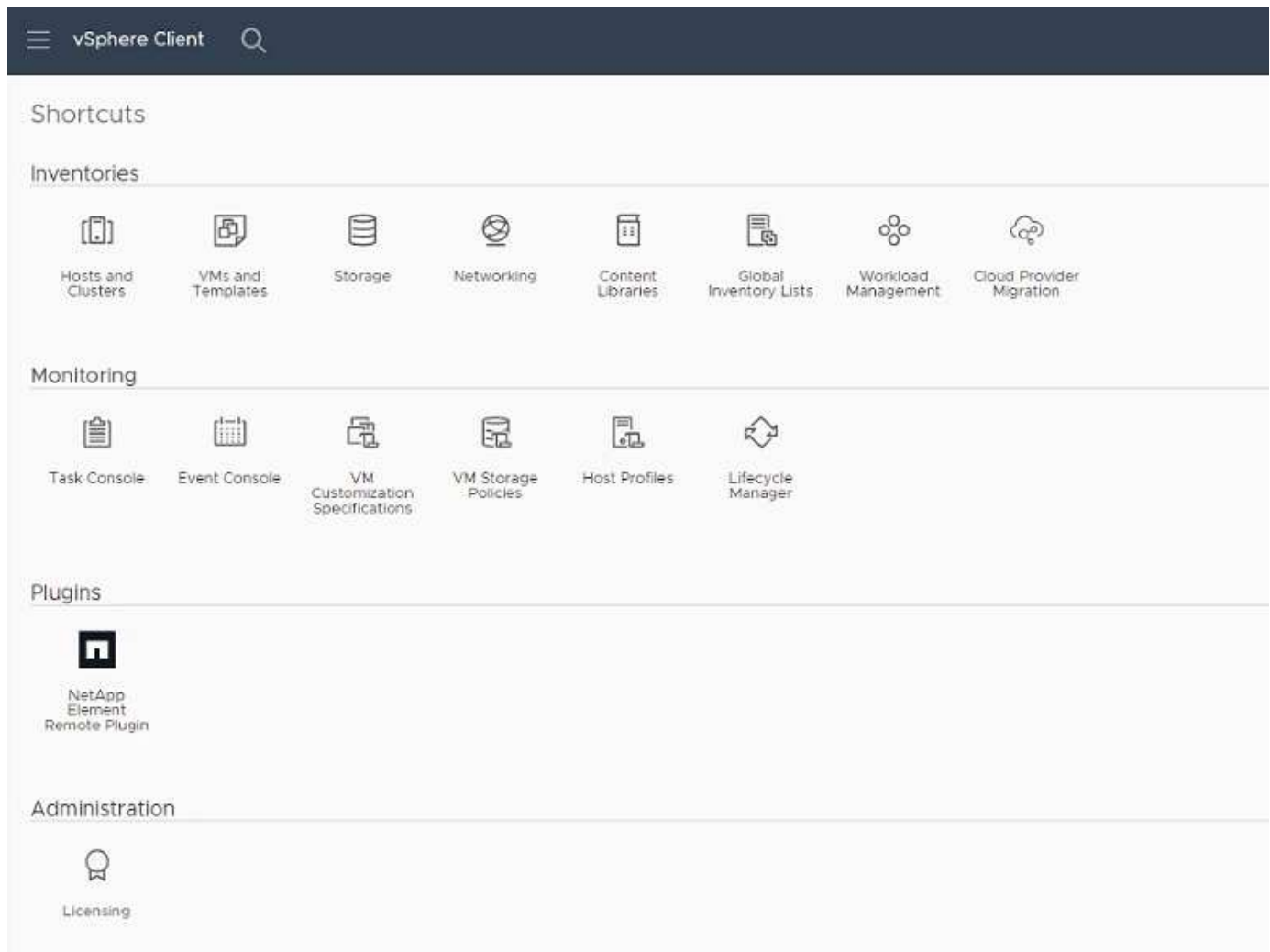
- The IPv4 address or the FQDN of the vCenter service on which you are registering your plug-in
- The vCenter Administrator user name
- The vCenter Administrator password

c. Select **Check Status** to verify that the new version of the plug-in is registered on the vCenter Server.

7. In the vSphere Web Client, look for the following completed tasks in the task monitor to ensure installation has completed: Download plug-in and Deploy plug-in.

Access the plug-in and verify successful installation

After successful installation or upgrade the NetApp Element Remote Plugin extension point appears in the Shortcuts tab of the vSphere Web Client in the side panel.



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

Add storage clusters for use with the plug-in

You can add and manage a cluster running Element software using the NetApp Element Remote Plugin extension point.

What you'll need

- At least one cluster must be available and its IP or FQDN address known.
- Current full Cluster Admin user credentials for the cluster.
- Firewall rules allow open [network communication](#) between the vCenter and the cluster MVIP on TCP ports 443, 8333, and 8443.



You must add at least one cluster to use Management functions.

About this task

This procedure describes how to add a cluster profile so that the cluster can be managed by the plug-in. You cannot modify cluster administrator credentials using the plug-in.

See [managing cluster administrator user accounts](#) for instructions on changing credentials for a cluster administrator account.

Steps

1. Select **NetApp Element Remote Plugin > Configuration > Clusters**.
2. Select **Add Cluster**.
3. Enter the following information:
 - **IP address/FQDN**: Enter the cluster MVIP address.
 - **User ID**: Enter a cluster administrator user name.
 - **Password**: Enter a cluster administrator password.
 - **vCenter Server**: If you set up a Linked Mode group, select the vCenter Server you want to access the cluster. If you're not using Linked Mode, the current vCenter Server is the default.



- The hosts for a cluster are exclusive to each vCenter Server. Be sure that the vCenter Server you select has access to the intended hosts. You can remove a cluster, reassign it to another vCenter Server, and add it again if you decide later to use different hosts.
- 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.

4. Select **OK**.

When the process completes, the cluster appears in the list of available clusters and can be used in the NetApp Element Management extension point.

Configure QoSSIOC settings using the plug-in

You can set up automatic quality of service based on Storage I/O Control ([QoSSIOC](#)) for individual volumes and datastores controlled by the plug-in. To do so, you configure QoSSIOC and vCenter credentials that will enable the QoSSIOC service to communicate with vCenter.

About this task

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.

Steps

1. Select **NetApp Element Remote Plugin > Configuration > QoSSIOC Settings**.
2. Select **Actions**.
3. In the resulting menu, select **Configure**.
4. In the **Configure QoSSIOC Settings** dialog box, enter the following information:
 - **mNode IP Address/FQDN**: The IP address of the management node for the cluster that contains the QoSSIOC service.
 - **mNode Port**: The port address for the management node that contains the QoSSIOC service. The default port is 8443.
 - **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](https://[management node IP]:9443)).
 - **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 the QoSSIOC service is enabled, you can configure QoSSIOC performance on individual datastores.

Configure user accounts

To enable access to volumes, you'll need to create at least one [user account](#).

Create datastores and volumes

You can create [datastores](#) and [Element volumes](#) to start allocating storage.

Find more information

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

Install and configure Element Plug-in 4.10 and earlier

You can install NetApp Element Plug-in for VMware vCenter Server 4.10 or earlier directly to your vCenter and access the plug-in with the vSphere Web Client.

After installation is complete, you can use the quality of service based on storage I/O control (QoSSIOC) service as well as other services of the vCenter Plug-in.

Read and complete each step to install and begin using the plug-in:

- [Prepare for installation](#)
- [Install the management node](#)
- [Register the plug-in with vCenter](#)
- [Modify vCenter properties for a dark site HTTP server](#)
- [Access the plug-in and verify successful installation](#)
- [Add storage clusters for use with the plug-in](#)
- [Configure QoSSIOC settings using the plug-in](#)
- [Configure user accounts](#)
- [Create datastores and volumes](#)

Prepare for installation

Before you begin the installation, review [pre-deployment requirements](#).

Install the management node

You can manually [install the management node](#) for your cluster running NetApp Element software using the appropriate image for your configuration.

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

Register the plug-in with vCenter

Deploying the vCenter Plug-in package in the vSphere Web Client involves registering the package as an extension on vCenter Server. After registration is complete, the plug-in is available to any vSphere Web Client that connects to your vSphere environment.

What you'll need

- For vSphere 6.5 and 6.7, ensure you have logged out of the vSphere Web Client. The web client for these versions will not recognize updates made during this process to your plug-in if you do not log out. For vSphere 7.0, you do not need to log out of the web client.
- You have vCenter Administrator role privileges to register a plug-in.
- You have deployed a management node OVA running Element software 11.3 or later.
- Your management node is powered on with its IP address or DHCP address configured.
- You are using an SSH client or web browser (Chrome 56 or later or Firefox 52 or later).
- Your firewall rules allow open [network communication](#) between the vCenter and the storage cluster MVIP

on TCP ports 443, 8443, and 9443. Port 9443 is used for registration and can be closed after registration is complete. If you have enabled virtual volumes functionality on the cluster, ensure TCP port 8444 is also open for VASA provider access.

About this task

You must register the vCenter Plug-in on every vCenter Server where you need to use the plug-in.

For Linked Mode environments, the plug-in must be registered with each vCenter Server in the environment to keep MOB data in sync and to be able to upgrade the plug-in. When a vSphere Web Client connects to a vCenter Server where your plug-in is not registered, the plug-in is not visible to the client.



Using NetApp Element Plug-in for vCenter Server to manage cluster resources from other vCenter Servers using [vCenter Linked Mode](#) is limited to local storage clusters only.

Steps

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

`https://<managementNodeIP>:9443`

The registration 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

Manage QoSSIOC Service Credentials

Old Password Current password is required

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 @\$%&'()*~+-_!@#\$%^&*~10'

Confirm Password New and confirm passwords must match

SUBMIT CHANGES

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

2. **Optional:** Change the password for the QoSSIOC service before registering the vCenter Plug-in:
 - a. For the Old Password, enter the current password of the QoSSIOC service. If you have not yet assigned a password, type the default password:

`solidfire`

b. Select **Submit Changes**.



After you submit changes, the QoSSIOC service automatically restarts.

3. Select **vCenter Plug-in Registration**.

The screenshot shows the NetApp Element Plug-in for vCenter Server Management Node interface. The page title is "vCenter Plug-in - Registration". On the left, there is a sidebar with "Manage vCenter Plug-in" and a list of options: "Register Plug-in" (selected), "Update Plug-in", "Unregister Plug-in", and "Registration Status". The main content area contains the following fields and instructions:

- Register version**: A dropdown menu showing "4.5.0". Below it, text states: "Register version 4.5.0 of the NetApp Element Plug-in for vCenter Server with your vCenter server. The Plug-in will not be deployed until a fresh vCenter login after registration."
- vCenter Address**: A text field with the placeholder "vCenter Server Address". Below it, text states: "Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on."
- vCenter User Name**: A text field with the placeholder "vCenter Admin User Name". Below it, text states: "Ensure this user is a vCenter user that has administrative privileges for registration."
- vCenter Password**: A text field with the placeholder "vCenter Admin Password". Below it, text states: "The password for the vCenter user name entered."
- Customize URL**: A checkbox labeled "Customize URL". Below it, text states: "Select to customize the Zip file URL."
- Plug-in Zip URL**: A text field with the placeholder "https://10.117.227.12:9443/solidfire-plugin-4.5.0-bin.zip". Below it, text states: "URL of XML initialization file."

At the bottom of the main content area is a "REGISTER" button. At the bottom of the page, there is a footer that says "Contact NetApp Support at <http://mysupport.netapp.com>".

4. Enter the following information:

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



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

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



Most installations use the default path. To customize the URL if you are using an HTTP or HTTPS server (dark site) or have modified the ZIP file name or network settings, select **Custom URL**. For additional steps if you intend to customize a URL, see [Modify vCenter properties for a dark site HTTP server](#).

5. Select **Register**.

6. (Optional) Verify registration status:

a. Select **Registration Status**.

b. Enter the following information:

- The IPv4 address or the FQDN of the vCenter service on which you are registering your plug-in
- The vCenter Administrator user name
- The vCenter Administrator password

c. Select **Check Status** to verify that the new version of the plug-in is registered on the vCenter Server.

7. (For vSphere 6.5 and 6.7 users) Log in to the vSphere Web Client as a vCenter Administrator.



This action completes the installation in the vSphere Web Client. If the vCenter Plug-in icons are not visible from vSphere, see [troubleshooting documentation](#).

8. In the vSphere Web Client, look for the following completed tasks in the task monitor to ensure installation has completed: Download plug-in and Deploy plug-in.

Modify vCenter properties for a dark site HTTP server

If you intend to customize a URL for an in-house (dark site) HTTP server during vCenter Plug-in registration, you must modify the vSphere Web Client properties file `webclient.properties`. You can use vCSA or Windows to make the changes.

What you'll need

Permissions to download software from the NetApp Support Site.

Steps using vCSA

1. SSH into the vCenter Server:

```
Connected to service
* List APIs: "help api list"
* List Plugins: "help pi list"
* Launch BASH: "shell"
Command>
```

2. Enter `shell` in the command prompt to access root:

```
Command> shell
Shell access is granted to root
```

3. Stop the VMware vSphere Web Client service:

```
service-control --stop vsphere-client
service-control --stop vsphere-ui
```

4. Change the directory:

```
cd /etc/vmware/vsphere-client
```

5. Edit the `webclient.properties` file and add `allowHttp=true`.

6. Change the directory:

```
cd /etc/vmware/vsphere-ui
```

7. Edit the `webclient.properties` file and add `allowHttp=true`.

8. Start the VMware vSphere Web Client service:

```
service-control --start vsphere-client  
service-control --start vsphere-ui
```



After you have completed the registration procedure, you can remove `allowHttp=true` from the files you modified.

9. Reboot vCenter.

Steps using Windows

1. Change the directory from a command prompt:

```
cd c:\Program Files\VMware\vCenter Server\bin
```

2. Stop the VMware vSphere Web Client service:

```
service-control --stop vsphere-client  
service-control --stop vsphere-ui
```

3. Change the directory:

```
cd c:\ProgramData\VMware\vCenterServer\cfg\vsphere-client
```

4. Edit the `webclient.properties` file and add `allowHttp=true`.

5. Change the directory:

```
cd c:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui
```

6. Edit the `webclient.properties` file and add `allowHttp=true`.

7. Change the directory from a command prompt:

```
cd c:\Program Files\VMware\vCenter Server\bin
```

8. Start the VMware vSphere Web Client service:

```
service-control --start vsphere-client  
service-control --start vsphere-ui
```

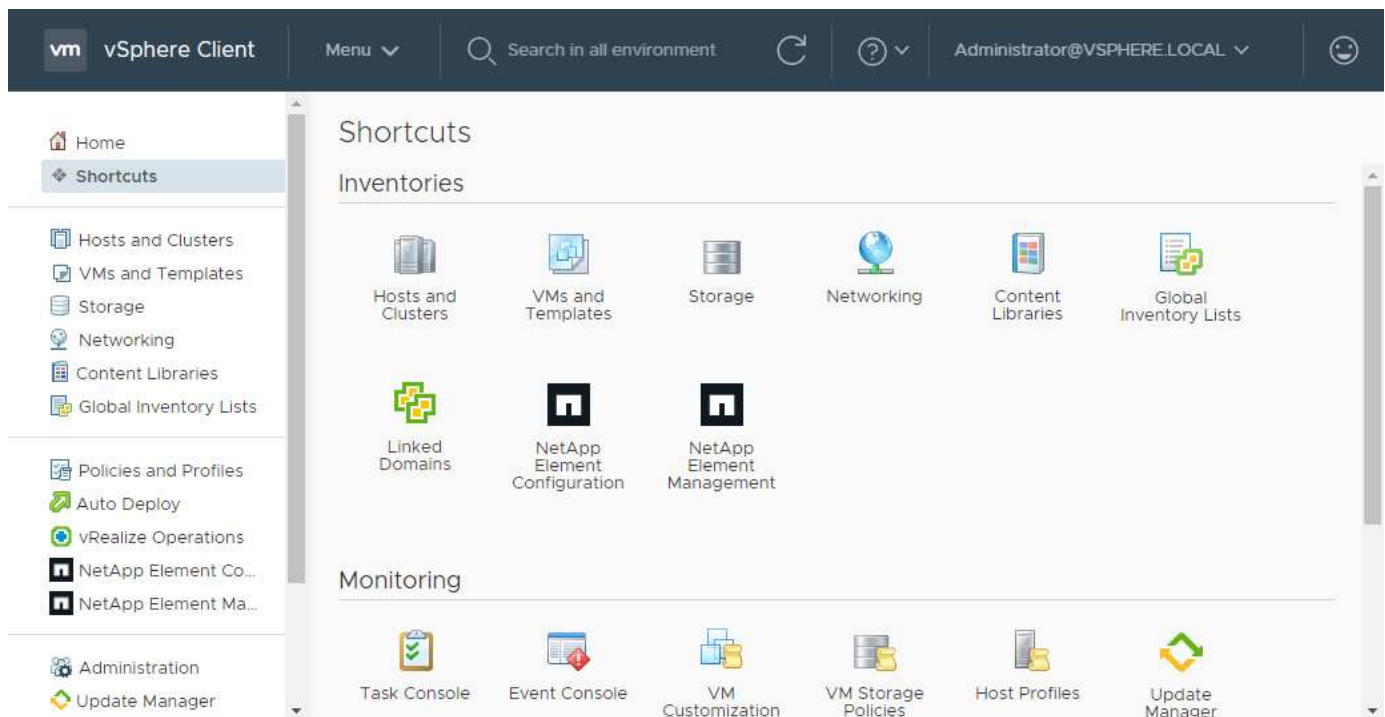


After you have completed the registration procedure, you can remove `allowHttp=true` from the files you modified.

9. Reboot vCenter.

Access the plug-in and verify successful installation

After successful installation or upgrade, NetApp Element Configuration and Management extension points appear in the Shortcuts tab of the vSphere Web Client and in the side panel.



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

Add storage clusters for use with the plug-in

You can add a cluster running Element software using the NetApp Element Configuration extension point so that it can be managed by the plug-in.

After a connection has been established to the cluster, the cluster can then be managed using the NetApp Element Management extension point.

What you'll need

- At least one cluster must be available and its IP or FQDN address known.
- Current full Cluster Admin user credentials for the cluster.
- Firewall rules allow open [network communication](#) between the vCenter and the cluster MVIP on TCP ports 443 and 8443.



You must add at least one cluster to use the NetApp Element Management extension point functions.

About this task

This procedure describes how to add a cluster profile so that the cluster can be managed by the plug-in. You cannot modify cluster administrator credentials using the plug-in.

See [managing cluster administrator user accounts](#) for instructions on changing credentials for a cluster administrator account.



The vSphere HTML5 web client and Flash web client have separate databases that cannot be combined. Clusters added in one client will not be visible in the other. If you intend to use both clients, add your clusters in both.

Steps

1. Select **NetApp Element Configuration > Clusters**.
2. Select **Add Cluster**.
3. Enter the following information:
 - **IP address/FQDN**: Enter the cluster MVIP address.
 - **User ID**: Enter a cluster administrator user name.
 - **Password**: Enter a cluster administrator password.
 - **vCenter Server**: If you set up a Linked Mode group, select the vCenter Server you want to access the cluster. If you're not using Linked Mode, the current vCenter Server is the default.



- The hosts for a cluster are exclusive to each vCenter Server. Be sure that the vCenter Server you select has access to the intended hosts. You can remove a cluster, reassign it to another vCenter Server, and add it again if you decide later to use different hosts.
- Using NetApp Element Plug-in for vCenter Server to manage cluster resources from other vCenter Servers using [vCenter Linked Mode](#) is limited to local storage clusters only.

4. Select **OK**.

When the process completes, the cluster appears in the list of available clusters and can be used in the NetApp Element Management extension point.

Configure QoSSIOC settings using the plug-in

You can set up automatic quality of service based on Storage I/O Control ([QoSSIOC](#)) for individual volumes and datastores controlled by the plug-in. To do so, you configure QoSSIOC and vCenter credentials that will enable the QoSSIOC service to communicate with vCenter.

About this task

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.

Steps

1. Select **NetApp Element Configuration > QoSSIOC Settings**.
2. Select **Actions**.
3. In the resulting menu, select **Configure**.
4. In the **Configure QoSSIOC Settings** dialog box, enter the following information:
 - **mNode IP Address/FQDN**: The IP address of the management node for the cluster that contains the QoSSIOC service.
 - **mNode Port**: The port address for the management node that contains the QoSSIOC service. The default port is 8443.
 - **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`).
 - **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 the QoSSIOC service is enabled, you can configure QoSSIOC performance on individual datastores.

Configure user accounts

To enable access to volumes, you'll need to create at least one [user account](#).

Create datastores and volumes

You can create [datastores and Element volumes](#) to start allocating storage.

Find more information

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

Upgrade the plug-in

You can upgrade the NetApp Element Plug-in for vCenter Server by following the steps described for your installation. NetApp Element vCenter plug-in 5.2 is available outside of Element and NetApp HCI releases as part of a management services bundle.



- Beginning with Element Plug-in for vCenter 5.0, only VMware vSphere 8.0 and 7.0 are supported.
- When you upgrade from Element Plug-in for vCenter 4.x to 5.x, the clusters already configured with the plug-in are lost because the data cannot be copied from a vCenter instance to a remote plug-in. You must re-add the clusters to the remote plug-in. This is a one-time activity when upgrading from a local to a remote plug-in.

Steps

To upgrade the plug-in, follow the instructions in the upgrade documentation for your product:

- [Upgrade your NetApp HCI system](#)
- [Upgrade your SolidFire all-flash storage system](#)

Find more information

- [vCenter Plug-in 5.2 Release Notes](#)
- [Hybrid Cloud Control and Management Services Release Notes](#)
- [NetApp HCI Documentation](#)
- [NetApp HCI Resources page](#)
- [SolidFire and Element Resources page](#)

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.



This feature is unavailable in SolidFire Enterprise SDS clusters.

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** 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 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.



This feature is unavailable in SolidFire Enterprise SDS clusters.

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.



This feature is unavailable in SolidFire Enterprise SDS clusters.

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.



This feature is unavailable in SolidFire Enterprise SDS clusters.

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.



This feature is unavailable in SolidFire Enterprise SDS clusters.

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.



This feature is unavailable in SolidFire Enterprise SDS clusters.

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 QoS SIOC, 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:

- Enter a name for the new NetApp Element volume that backs the clone datastore.
- 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 QoS SIOC, 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 Server, 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](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.

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](#)

Manage cluster hardware and virtual networks

Manage cluster hardware and virtual networks overview

From the Cluster tab in the plug-in extension point, you can view and change cluster-wide settings and perform cluster-specific tasks for drives, nodes, and VLANs.

Options

- [Add and manage drives](#)
- [Add and manage nodes](#)
- [Create and manage virtual networks](#)

Add and manage drives

You can add drives to a cluster, view existing drives, and remove drives using the plug-in extension point.

- [Add available drives to a cluster](#)
- [View drive details](#)
- [Remove a drive](#)

Add available drives to a cluster

You can add drives to a cluster using the plug-in extension point. When you add a node to the cluster or install new drives in an existing node, the drives automatically register as `Available`. You must add the drives to the cluster before each drive can participate in the cluster.

About this task

Drives are not displayed in the Available list when the following conditions exist:

- Drives are in an `Active`, `Removing`, `Erasing`, or `Failed` state.
- The node of which the drive is a part is in `Pending` state.

Steps

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



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 **Drives** sub-tab, select **Available** from the drop-down list to view the list of available drives.
3. Add drives as follows:
 - a. Select the check box for each drive you want to add.

b. Click **Add Drives**.

4. Review the details of the drives you are intending to add and confirm the action.

View drive details

You can view a list of the active drives in the cluster using the Active view on the Drives page of the Cluster tab from the plug-in extension point. You can change the view by selecting available options using the drop-down filter.

About this task

When you first initialize a cluster, the active drives list is empty. You can add drives that are unassigned to a cluster and listed in the Available tab after a new cluster is created.

Steps

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

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



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 **Drives** sub-tab.

3. Select the **Active** view.

4. View the details of the drives that are currently active in the system.

You can view information such as drive IDs, the capacity and status of each drive, and information about the node the drive resides in.

Remove a drive

You can remove a drive from a cluster using the plug-in extension point. You might do this when reducing cluster capacity or preparing to replace drives nearing the end of their service life. Removing a drive takes the drive offline. Any data on the drive is removed and migrated to other drives in the cluster before the drive is removed from the cluster. The data migration to other active drives in the system can take a few minutes to an hour depending on capacity utilization and active I/O on the cluster.

About this task

When you remove a drive in a `Failed` state, the drive is not returned to `Available` or `Active` states. Instead, the drive is unavailable for use in the cluster.

Steps

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

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



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 **All** from the drop-down list to view the complete list of drives.
3. Remove drives as follows:
 - a. Select the check box for each drive you want to remove.
 - b. Click **Remove Drives**.
4. Confirm the action.



If there is not enough capacity to remove active drives before removing a node, an error message appears when you confirm the drive removal.

Find more information

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

Add and manage nodes

Using the plug-in, you can add [storage nodes](#) when a cluster is created or when more storage is needed. You can also add storage nodes running Element software. You must add NetApp HCI compute nodes outside of the plug-in in vSphere.

- [Add a node to a cluster](#)
- [View node details](#)
- [Restart a node](#)
- [Shut down a node](#)
- [Remove a node from a cluster](#)

Add a node to a cluster

You can add storage nodes to your cluster using the vCenter Plug-in.

What you'll need

- The node you are adding has been set up, powered on, and configured.
- Both the major or minor version numbers of the software on each node in a cluster must match for the software to be compatible. For example, Element 9.0 is not compatible with version 9.1.



If the node you are adding has a different major or minor version of NetApp Element software than the version running on the cluster, the cluster asynchronously updates the node to the version of NetApp Element software running on the cluster master. After the node is updated, it automatically adds itself to the cluster. During this asynchronous process, the node will be in a `pendingActive` state.

About this task

Nodes require initial configuration when they are first powered on. When the node has been set up and configured, it registers itself on the cluster identified when the node was configured and appears in the list of pending nodes on the **Cluster > Nodes** page of the plugin extension point.

You can add nodes of smaller or larger capacities to an existing cluster.

The procedure is the same for adding FC nodes or storage nodes that are running NetApp Element software.

Steps

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



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 **Nodes** sub-tab.
3. Select **Pending** from the drop-down list to view the list of nodes.
4. To add one or more nodes, perform the following steps:
 - a. Select the check box for each node you want to add.
 - b. Click **Add Node**.
5. Review the details of the nodes you are intending to add and confirm the action.

When the action is complete, the node appears in the list of active nodes for the cluster.

View node details

You can view a list of the nodes in the cluster on the Nodes page of the Cluster tab from the plug-in extension point. You must select Active view to see the list of active nodes. You can change the view by selecting Pending, PendingActive, and All options using the drop-down filter.

Steps

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



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 **Nodes** sub-tab.
3. Select the **Active** view.
4. View the details of the nodes in the storage cluster.

You can view information such as node IDs, the name and state of each node, configured IOPS, node type, the number of active drives in each node, and networking information about each node.

Restart a node

You can restart one or more active nodes in a cluster using the plug-in extension point.

What you'll need

You have stopped I/O and disconnected all iSCSI sessions if you are restarting more than one node simultaneously.

About this task

To restart the cluster, you can select all cluster nodes and perform a restart.



This method restarts all networking services on a node, causing temporary loss of networking connectivity.



This feature is unavailable in SolidFire Enterprise SDS clusters.

Steps

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



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 **Nodes** sub-tab.
 - a. From the **Active** view, select the check box for each node you want to restart.
 - b. Click **Actions**.
 - c. Select **Restart**.
3. Confirm the action.

Shut down a node

You can shut down one or more active nodes in a cluster using the plug-in extension point. To shut down the cluster, you can select all cluster nodes and perform a simultaneous shutdown.

What you'll need

You have stopped I/O and disconnected all iSCSI sessions if you are restarting more than one node simultaneously.



About this task

This feature is unavailable in SolidFire Enterprise SDS clusters.

Steps

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

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



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 **Nodes** sub-tab.

- From the **Active** view, select the check box for each node you want to shut down.
- Click **Actions**.
- Select **Shutdown**.

3. Confirm the action.



If a node has been down longer than 5.5 minutes under any type of shutdown condition, the NetApp Element software determines that the node is not coming back to join the cluster. Double Helix data protection begins the task of writing single replicated blocks to another node to replicate the data. Depending on the length of time a node is shut down, its drives might need to be added back to the cluster after the node is brought back online.

Remove a node from a cluster

You can remove nodes from a cluster without service interruption when their storage is no longer needed or they require maintenance.

What you'll need

You have removed all the drives in the node from the cluster. You cannot remove a node until the `RemoveDrives` process has completed and all data has been migrated away from the node.

About this task

At least two FC nodes are required for FC connectivity in a NetApp Element cluster. If only one FC node is connected, the system triggers alerts in the Event Log until you add another FC node to the cluster, even though all FC network traffic continues to operate with only one FC node.

Steps

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



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 **Nodes** sub-tab.

3. To remove one or more nodes, perform the following steps:

- From the **Active** view, select the check box for each node you want to remove.
- Click **Actions**.
- Select **Remove**.

4. Confirm the action.

Any nodes removed from a cluster appear in the list of Pending nodes.

Find more information

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

Create and manage virtual networks

You can add a new virtual network to a cluster configuration to enable a multi-tenant environment connection to a cluster running NetApp Element software, and manage the virtual network using the vCenter Plug-in.

- [Create a virtual network](#)
- [View virtual network details](#)
- [Edit a virtual network](#)
- [Delete a virtual network](#)

Create a virtual network

You can add a new virtual network to a cluster configuration.

What you'll need

- ESXi hosts have a single iSCSI software adapter.
- Hosts or switches are configured for the VLAN.
- You have identified the block of IP addresses that will be assigned to the virtual networks on the cluster nodes.
- You have identified a storage network IP (SVIP) address that will be used as an endpoint for all NetApp Element storage traffic.

The following criteria should be considered for this configuration:



- VRF can only be enabled at the time of creating a VLAN. If you want to switch back to non-VRF, you must delete and re-create the VLAN.
- VLANs that are not VRF-enabled require initiators to be in the same subnet as the SVIP.
- VLANs that are VRF-enabled do not require initiators to be in the same subnet as the SVIP, and routing is supported.

About this task

When a virtual network is added, an interface for each node is created and each requires a virtual network IP address. The number of IP addresses you specify when creating a new virtual network must be equal to or greater than the number of nodes in the cluster. Virtual network addresses are bulk provisioned by and assigned to individual nodes automatically. You do not need to manually assign virtual network addresses to the nodes in the cluster.

Steps

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

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



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 **Network** sub-tab.
3. Select **Create VLAN**.
4. In the **Create VLAN** dialog box, enter a name for the VLAN.
5. Enter an integer for the VLAN tag.
6. Enter the Storage Virtual IP (SVIP) address for the storage cluster.
7. Adjust the netmask, as needed.

The default is 255.255.255.0.

8. Optional: Enter a description for the VLAN.
9. Optional: Select the **Enable Virtual Routing and Forwarding** check box.



Virtual routing and forwarding (VRF) allows multiple instances of a routing table to exist in a router and work simultaneously. This functionality is available for storage networks only.

- a. Enter an IP address of a gateway of the virtual network.

10. Select the hosts that you want to include in the VLAN.



Note: If you are using vCenter Linked Mode, only hosts available to the vCenter Server to which the cluster is assigned are available to select.

11. Configure the IP address blocks for the storage nodes as follows:



Note: A minimum of one IP address block must be created.

- a. Click **Create Block**.
- b. Enter the starting address for the IP range.
- c. Enter the number of IP addresses to include in the address block.



The total number of IP addresses must match the number of nodes in the storage cluster.

- d. Click outside the entry to accept the values.

12. Click **OK** to create the VLAN.

View virtual network details

You can view network information for VLANs on the Network page of the Cluster tab from the plug-in extension point.

Steps

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



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 **Nodes** sub-tab.
3. Select the **Active** view.
4. View the details of the nodes in the storage cluster.

You can view information such as the ID and name of each VLAN, the tag associated with each VLAN, the SVIP assigned to each VLAN, and the IP range used for each VLAN.

Edit a virtual network

You can change VLAN attributes, such as VLAN name, netmask, and size of the IP address blocks.

About this task

The VLAN Tag and SVIP cannot be modified for a VLAN. The gateway attribute can only be modified for VRF VLANs. If any iSCSI, remote replication, or other network sessions exist, the modification might fail.

Steps

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



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 **Network** sub-tab.
3. Select the check box for the VLAN you want to edit.
4. Click **Actions**.
5. In the resulting menu, click **Edit**.
6. In the resulting menu, enter the new attributes for the VLAN.
7. Click **Create Block** to add a non-continuous block of IP addresses for the virtual network.
8. Click **OK**.

Delete a virtual network

You can permanently delete a VLAN object and its block of IPs. Address blocks that were assigned to the VLAN are disassociated with the virtual network and can be reassigned to another virtual network.

Steps

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

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



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 **Network** sub-tab.
3. Select the check box for the VLAN you want to delete.
4. Click **Actions**.
5. In the resulting menu, click **Delete**.
6. Confirm the action.

Monitor system performance

Monitor system performance with Reporting options

You can view information about the cluster's components and performance by using the Reporting pages of the NetApp Element Plug-in for VMware vCenter Server.

Using the vCenter Plug-in, you can monitor cluster components and performance in the following ways:

- [Monitor overall cluster health on the Overview page](#)
- [Monitor system alerts](#)
- [Monitor event logs for troubleshooting](#)
- [Monitor volume performance](#)
- [Monitor iSCSI sessions to determine connection status](#)
- [Monitor VM performance tiering with QoSSIOC events](#)

Find more information

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

Monitor overall cluster health on the Overview page

You can view high-level cluster information for the selected cluster, including overall capacity, efficiency, and performance, on the Overview page of the Reporting tab from the NetApp Element Management extension point of the NetApp Element Plug-in for VMware vCenter Server.

Steps

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. Monitor the data on the **Overview** page.

Reporting Overview page data

The following data appears on the Reporting Overview page:

- **Cluster Capacity:** The capacity remaining for block storage, metadata, and provisioned space. Move the pointer over the progress bar to see threshold information.
- **Cluster Information:** Information specific to the cluster, such as cluster name, the version of NetApp Element software running on the cluster, MVIP and SVIP addresses, and the number of nodes, 4k IOPS, volumes, and sessions on the cluster.
 - **Cluster Name:** The name for the cluster.

- **Storage IP (SVIP):** The storage virtual IP address (SVIP).
- **Management IP (MVIP):** The management virtual IP address (MVIP).
- **SVIP VLAN Tag:** The VLAN identifier for the master SVIP address.
- **MVIP VLAN Tag:** The VLAN identifier for the master MVIP address.
- **Node Count:** The number of active nodes in the cluster.
- **Cluster 4K IOPS:** The number of 4096 (4K) blocks that can be read/written by the cluster in a second.
- **Element OS Version:** The version of the NetApp Element software that the cluster is running.
- **Volume Count:** The total number of volumes, excluding virtual volumes, on the cluster.
- **Virtual Volume Count:** The total number of virtual volumes on the cluster.
- **iSCSI Sessions:** The iSCSI sessions that are connected to the cluster.
- **Fibre Channel Sessions:** The Fibre Channel sessions that are connected to the cluster.
- **Cluster Efficiency:** Overall system capacity that is being utilized that takes into account thin provisioning, deduplication, and compression. The calculated benefit achieved on the cluster is calculated by comparing what the capacity utilization would be without thin provisioning, deduplication, and compression on a traditional storage device.
- **Protection Domains:** A summary of protection domains monitoring for the cluster.



The protection domains feature is not compatible with two-node clusters.

- **Protection Domains Monitoring Level:** The protection domain resiliency levels as selected by the user. Possible values are Chassis or Node. Green indicates that the cluster is capable of the selected monitoring level. Red indicates that the cluster is no longer capable of the selected monitoring level and corrective action is needed.
- **Remaining Block Capacity:** Indicates the percentage of block capacity that is remaining to maintain the selected resiliency level.
- **Metadata Capacity:** Indicates if there is sufficient metadata capacity to heal from failure while also maintaining uninterrupted data availability. Normal (green) indicates that the cluster has sufficient metadata to maintain the selected monitoring level. Full (red) indicates that the cluster is no longer capable of the selected monitoring level and corrective action is needed.
- **Custom Protection Domain Health:** Displays the custom Protection Domain health status for the cluster when a custom Protection Domain is configured on the cluster.

The following data indicates the protection available against the failure of one of the custom Protection Domains for the cluster.

- **Protection Level:** Indicates the overall protection level status.
- **Block Capacity:** Indicates the current protection level status of the block services subsystem.

It also indicates the total capacity threshold at which resiliency is lost.

- **Metadata Capacity:** Indicates the current protection level status of the metadata services subsystem.
- **Ensemble Nodes:** Indicates the current protection level status of the ensemble members subsystem.
- **Provisioned IOPS:** A summary of how volume IOPS might be overprovisioned on the cluster. Provisioned IOPS calculations are determined by the sum of the total minimum IOPS, maximum IOPS, and burst IOPS for all volumes on the cluster divided by the maximum IOPS rated for the cluster.



For example, if there are four volumes in the cluster, each with minimum IOPS of 500, maximum IOPS of 15,000, and burst IOPS of 15,000, the total number of minimum IOPS would be 2,000, total maximum IOPS would be 60,000, and total burst IOPS would be 60,000. If the cluster is rated at maximum IOPS of 50,000, then the calculations would be the following:

Minimum IOPS: $2000/50000 = 0.04x$

Maximum IOPS: $60000/50000 = 1.20x$

Burst IOPS: $60000/50000 = 1.20x$ 1.00x

1.00x is the baseline at which provisioned IOPS is equal to the rated IOPS for the cluster.

- **Cluster Health:** The hardware, capacity, and security components of the health of the cluster. Color codes indicate the following:
 - **Green:** Healthy
 - **Yellow:** Critical
 - **Red:** Error
- **Cluster Input/Output:** The I/O currently running on the cluster. The values are calculated based on the previous I/O measurement against the current I/O measurements. These are the measurements shown in the graph:
 - **Total:** The combined read and write IOPS occurring in the system.
 - **Read:** The number of read IOPS occurring.
 - **Write:** The number of write IOPS.
- **Cluster Throughput:** The bandwidth activity for read, write, and total bandwidth on the cluster:
 - **Total:** The total MB/s used for both read and write activity in the cluster.
 - **Read:** The read activity in MB/s for the cluster.
 - **Write:** The write activity in MB/s for the cluster.
- **Performance Utilization:** The percentage of cluster IOPS being consumed. For example, a 250K IOPS cluster running at 100K IOPS would show 40% consumption.

Find more information

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

Monitor system alerts

You can monitor alerts, which are information, warnings, or errors that indicate how well the cluster is running.

Alerts are cluster faults or errors and are reported as they occur. Most errors resolve themselves automatically; however, some might require manual intervention. The system reports alert error codes with each alert on the Alerts page. Error codes help you determine what component of the system experienced the alert and why the alert was generated. See [System alerts list](#) for a descriptions and remediation steps.

After you resolve the issue, the system polls itself and identifies the issue as resolved. Then, all information about the alert including the date it was resolved is moved to the Resolved view.

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. Select **Reporting > Alerts**.
3. Monitor the following cluster alert information:
 - **ID**: Unique ID for a cluster alert.
 - **Severity**
 - **warning**: A minor issue that might soon require attention. System upgrades are still allowed at this severity level.
 - **error**: A failure that might cause performance degradation or loss of high availability (HA). Errors generally should not affect service otherwise.
 - **critical**: A serious failure that affects service. The system is unable to serve API or client I/O requests. Operating in this state could lead to potential loss of data.
 - **bestPractice**: A recommended system configuration best practice is not being used.
 - **Type**
 - **node**: Fault affecting an entire node.
 - **drive**: Fault affecting an individual drive.
 - **cluster**: Fault affecting the entire cluster.
 - **service**: Fault affecting a service on the cluster.
 - **volume**: Fault affecting a volume on the cluster.
 - **Node**: Node ID for the node that this fault refers to. Included for node and drive faults, otherwise set to - (dash).
 - **Drive ID**: Drive ID for the drive that this fault refers to. Included for drive faults, otherwise set to - (dash).
 - **Error Code**: A descriptive code that indicates what caused the fault.
 - **Details**: Detailed description of the fault.
 - **Time**: This heading is visible only in the Active filter view. The date and time the fault was logged.
 - **Resolution Date**: This heading is visible only in the Resolved filter view. The date and time the fault was resolved.
4. To validate that the issue was resolved, look for it in the Resolved view.

Find more information

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

System alerts list

The system reports error codes with each alert that help you determine what component of the system experienced the alert and why the alert was generated. You can view the error codes using the plug-in extension point:

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

The following list outlines the different types of system alerts.

- **authenticationServiceFault**

The Authentication Service on one or more cluster nodes is not functioning as expected.

Contact NetApp Support for assistance.

- **availableVirtualNetworkIPAddressesLow**

The number of virtual network addresses in the block of IP addresses is low.

To resolve this fault, add more IP addresses to the block of virtual network addresses.

- **blockClusterFull**

There is not enough free block storage space to support a single node loss. See the `GetClusterFullThreshold` API method for details on cluster fullness levels. This cluster fault indicates one of the following conditions:

- `stage3Low` (Warning): User-defined threshold was crossed. Adjust Cluster Full settings or add more nodes.
- `stage4Critical` (Error): There is not enough space to recover from a 1-node failure. Creation of volumes, snapshots, and clones is not allowed.
- `stage5CompletelyConsumed` (Critical)¹: No writes or new iSCSI connections are allowed. Current iSCSI connections will be maintained. Writes will fail until more capacity is added to the cluster.

To resolve this fault, purge or delete volumes or add another storage node to the storage cluster.

- **blocksDegraded**

Block data is no longer fully replicated due to a failure.

Severity	Description
Warning	Only two complete copies of the block data are accessible.
Error	Only a single complete copy of the block data is accessible.
Critical	No complete copies of the block data are accessible.

Note: The warning status can only occur on a Triple Helix system.

To resolve this fault, restore any offline nodes or block services, or contact NetApp Support for assistance.

- **blockServiceTooFull**

A block service is using too much space.

To resolve this fault, add more provisioned capacity.

- **blockServiceUnhealthy**

A block service has been detected as unhealthy:

- Severity = Warning: No action is taken. This warning period will expire in `cTimeUntilBSIsKilledMSec=330000` milliseconds.
- Severity = Error: The system is automatically decommissioning data and re-replicating its data to other healthy drives.
- Severity = Critical: There are failed block services on several nodes greater than or equal to the replication count (2 for double helix). Data is unavailable and bin syncing will not finish.

Check for network connectivity issues and hardware errors. There will be other faults if specific hardware components have failed. The fault will clear when the block service is accessible or when the service has been decommissioned.

- **BmcSelfTestFailed**

The Baseboard Management Controller (BMC) failed a self-test.

Contact NetApp support for assistance.

During an upgrade to Element 12.5 or later, the `BmcSelfTestFailed` fault is not generated for a node that has a preexisting failed BMC, or when a node's BMC fails during the upgrade. The BMCs that fail the self-tests during the upgrade will issue a `BmcSelfTestFailed` warning fault after the entire cluster completes the upgrade.

- **clockSkewExceedsFaultThreshold**

Time skew between the Cluster master and the node which is presenting a token exceeds the recommended threshold. Storage cluster cannot correct the time skew between the nodes automatically.

To resolve this fault, use NTP servers that are internal to your network, rather than the installation defaults. If you are using an internal NTP server, contact NetApp Support for assistance.

- **clusterCannotSync**

There is an out-of-space condition and data on the offline block storage drives cannot be synced to drives that are still active.

To resolve this fault, add more storage.

- **clusterFull**

There is no more free storage space in the storage cluster.

To resolve this fault, add more storage.

- **clusterIOPSAreOverProvisioned**

Cluster IOPS are over provisioned. The sum of all minimum QoS IOPS is greater than the expected IOPS of the cluster. Minimum QoS cannot be maintained for all volumes simultaneously.

To resolve this issue, lower the minimum QoS IOPS settings for volumes.

- **CpuThermalEventThreshold**

The number of CPU thermal events on one or more CPUs exceeds the configured threshold.

If no new CPU thermal events are detected within ten minutes, the warning will resolve itself.

- **disableDriveSecurityFailed**

The cluster is not configured to enable drive security (Encryption at Rest), but at least one drive has drive security enabled, meaning that disabling drive security on those drives failed. This fault is logged with “Warning” severity.

To resolve this fault, check the fault details for the reason why drive security could not be disabled. Possible reasons are:

- The encryption key could not be acquired, investigate the problem with access to the key or the external key server.
- The disable operation failed on the drive, determine whether the wrong key could possibly have been acquired.

If neither of these are the reason for the fault, the drive might need to be replaced.

You can attempt to recover a drive that does not successfully disable security even when the correct authentication key is provided. To perform this operation, remove the drive(s) from the system by moving it to Available, perform a secure erase on the drive and move it back to Active.

- **disconnectedClusterPair**

A cluster pair is disconnected or configured incorrectly.

Check network connectivity between the clusters.

- **disconnectedRemoteNode**

A remote node is either disconnected or configured incorrectly.

Check network connectivity between the nodes.

- **disconnectedSnapMirrorEndpoint**

A remote SnapMirror endpoint is disconnected or configured incorrectly.

Check network connectivity between the cluster and the remote SnapMirrorEndpoint.

- **driveAvailable**

One or more drives are available in the cluster. In general, all clusters should have all drives added and none in the available state. If this fault appears unexpectedly, contact NetApp Support.

To resolve this fault, add any available drives to the storage cluster.

- **driveFailed**

The cluster returns this fault when one or more drives have failed, indicating one of the following

conditions:

- The drive manager cannot access the drive.
- The slice or block service has failed too many times, presumably because of drive read or write failures, and cannot restart.
- The drive is missing.
- The master service for the node is inaccessible (all drives in the node are considered missing/failed).
- The drive is locked and the authentication key for the drive cannot be acquired.
- The drive is locked and the unlock operation fails.

To resolve this issue:

- Check network connectivity for the node.
- Replace the drive.
- Ensure that the authentication key is available.

• **driveHealthFault**

A drive has failed the SMART health check and as a result, the drive's functions are diminished. There is a Critical severity level for this fault:

- Drive with serial: <serial number> in slot: <node slot><drive slot> has failed the SMART overall health check.

To resolve this fault, replace the drive.

• **driveWearFault**

A drive's remaining life has dropped below thresholds, but it is still functioning. There are two possible severity levels for this fault: Critical and Warning:

- Drive with serial: <serial number> in slot: <node slot><drive slot> has critical wear levels.
- Drive with serial: <serial number> in slot: <node slot><drive slot> has low wear reserves.

To resolve this fault, replace the drive soon.

• **duplicateClusterMasterCandidates**

More than one storage cluster master candidate has been detected.

Contact NetApp Support for assistance.

• **enableDriveSecurityFailed**

The cluster is configured to require drive security (Encryption at Rest), but drive security could not be enabled on at least one drive. This fault is logged with "Warning" severity.

To resolve this fault, check the fault details for the reason why drive security could not be enabled. Possible reasons are:

- The encryption key could not be acquired, investigate the problem with access to the key or the external key server.

- The enable operation failed on the drive, determine whether the wrong key could possibly have been acquired.

If neither of these are the reason for the fault, the drive might need to be replaced.

You can attempt to recover a drive that does not successfully enable security even when the correct authentication key is provided. To perform this operation, remove the drive(s) from the system by moving it to Available, perform a secure erase on the drive and move it back to Active.

- **ensembleDegraded**

Network connectivity or power has been lost to one or more of the ensemble nodes.

To resolve this fault, restore network connectivity or power.

- **exception**

A fault reported that is other than a routine fault. These faults are not automatically cleared from the fault queue.

Contact NetApp Support for assistance.

- **failedSpaceTooFull**

A block service is not responding to data write requests. This causes the slice service to run out of space to store failed writes.

To resolve this fault, restore block services functionality to allow writes to continue normally and failed space to be flushed from the slice service.

- **fanSensor**

A fan sensor has failed or is missing.

To resolve this fault, replace any failed hardware.

- **fibreChannelAccessDegraded**

A Fibre Channel node is not responding to other nodes in the storage cluster over its storage IP for a period of time. In this state, the node will then be considered unresponsive and generate a cluster fault.

Check network connectivity.

- **fibreChannelAccessUnavailable**

All Fibre Channel nodes are unresponsive. The node IDs are displayed.

Check network connectivity.

- **fibreChannelActiveIxl**

The IxL Nexus count is approaching the supported limit of 8000 active sessions per Fibre Channel node.

- Best practice limit is 5500.
- Warning limit is 7500.
- Maximum limit (not enforced) is 8192.

To resolve this fault, reduce the IxL Nexus count below the best practice limit of 5500.

- **fibreChannelConfig**

This cluster fault indicates one of the following conditions:

- There is an unexpected Fibre Channel port on a PCI slot.
- There is an unexpected Fibre Channel HBA model.
- There is a problem with the firmware of a Fibre Channel HBA.
- A Fibre Channel port is not online.
- There is a persistent issue configuring Fibre Channel passthrough.

Contact NetApp Support for assistance.

- **fibreChannelIOPS**

The total IOPS count is approaching the IOPS limit for Fibre Channel nodes in the cluster. The limits are:

- FC0025: 450K IOPS limit at 4K block size per Fibre Channel node.
- FCN001: 625K OPS limit at 4K block size per Fibre Channel node.

To resolve this fault, balance the load across all available Fibre Channel nodes.

- **fibreChannelStaticIxL**

The IxL Nexus count is approaching the supported limit of 16000 static sessions per Fibre Channel node.

- Best practice limit is 11000.
- Warning limit is 15000.
- Maximum limit (enforced) is 16384.

To resolve this fault, reduce the IxL Nexus count below the best practice limit of 11000.

- **fileSystemCapacityLow**

There is insufficient space on one of the filesystems.

To resolve this fault, add more capacity to the filesystem.

- **fileSystemIsReadOnly**

A filesystem has moved into read-only mode.

Contact NetApp Support for assistance.

- **fipsDrivesMismatch**

A non-FIPS drive has been physically inserted into a FIPS capable storage node or a FIPS drive has been physically inserted into a non-FIPS storage node. A single fault is generated per node and lists all drives affected.

To resolve this fault, remove or replace the mismatched drive or drives in question.

- **fipsDrivesOutOfCompliance**

The system has detected that Encryption at Rest was disabled after the FIPS Drives feature was enabled. This fault is also generated when the FIPS Drives feature is enabled and a non-FIPS drive or node is present in the storage cluster.

To resolve this fault, enable Encryption at Rest or remove the non-FIPS hardware from the storage cluster.

- **fipsSelfTestFailure**

The FIPS subsystem has detected a failure during the self test.

Contact NetApp Support for assistance.

- **hardwareConfigMismatch**

This cluster fault indicates one of the following conditions:

- The configuration does not match the node definition.
- There is an incorrect drive size for this type of node.
- An unsupported drive has been detected. A possible reason is that the installed Element version does not recognize this drive. Recommend updating the Element software on this node.
- There is a drive firmware mismatch.
- The drive encryption capable state does not match the node.

Contact NetApp Support for assistance.

- **idPCertificateExpiration**

The cluster's service provider SSL certificate for use with a third-party identity provider (IdP) is nearing expiration or has already expired. This fault uses the following severities based on urgency:

Severity	Description
Warning	Certificate expires within 30 days.
Error	Certificate expires within 7 days.
Critical	Certificate expires within 3 days or has already expired.

To resolve this fault, update the SSL certificate before it expires. Use the UpdateIdpConfiguration API method with `refreshCertificateExpirationTime=true` to provide the updated SSL certificate.

- **inconsistentBondModes**

The bond modes on the VLAN device are missing. This fault will display the expected bond mode and the bond mode currently in use.

- **inconsistentMtus**

This cluster fault indicates one of the following conditions:

- Bond1G mismatch: Inconsistent MTUs have been detected on Bond1G interfaces.

- Bond10G mismatch: Inconsistent MTUs have been detected on Bond10G interfaces.

This fault displays the node or nodes in question along with the associated MTU value.

- **inconsistentRoutingRules**

The routing rules for this interface are inconsistent.

- **inconsistentSubnetMasks**

The network mask on the VLAN device does not match the internally recorded network mask for the VLAN. This fault displays the expected network mask and the network mask currently in use.

- **incorrectBondPortCount**

The number of bond ports is incorrect.

- **invalidConfiguredFibreChannelNodeCount**

One of the two expected Fibre Channel node connections is degraded. This fault appears when only one Fibre Channel node is connected.

To resolve this fault, check the cluster network connectivity and network cabling, and check for failed services. If there are no network or service problems, contact NetApp Support for a Fibre Channel node replacement.

- **irqBalanceFailed**

An exception occurred while attempting to balance interrupts.

Contact NetApp Support for assistance.

- **kmipCertificateFault**

- Root Certification Authority (CA) certificate is nearing expiration.

To resolve this fault, acquire a new certificate from the root CA with expiration date at least 30 days out and use `ModifyKeyServerKmp` to provide the updated root CA certificate.

- Client certificate is nearing expiration.

To resolve this fault, create a new CSR using `GetClientCertificateSigningRequest`, have it signed ensuring the new expiration date is at least 30 days out, and use `ModifyKeyServerKmp` to replace the expiring KMIP client certificate with the new certificate.

- Root Certification Authority (CA) certificate has expired.

To resolve this fault, acquire a new certificate from the root CA with expiration date at least 30 days out and use `ModifyKeyServerKmp` to provide the updated root CA certificate.

- Client certificate has expired.

To resolve this fault, create a new CSR using `GetClientCertificateSigningRequest`, have it signed ensuring the new expiration date is at least 30 days out, and use `ModifyKeyServerKmp` to replace the expired KMIP client certificate with the new certificate.

- Root Certification Authority (CA) certificate error.

To resolve this fault, check that the correct certificate was provided, and, if needed, reacquire the certificate from the root CA. Use `ModifyKeyServerKmip` to install the correct KMIP client certificate.

- Client certificate error.

To resolve this fault, check that the correct KMIP client certificate is installed. The root CA of the client certificate should be installed on the EKS. Use `ModifyKeyServerKmip` to install the correct KMIP client certificate.

- **kmipServerFault**

- Connection failure

To resolve this fault, check that the External Key Server is alive and reachable via the network. Use `TestKeyServerKimp` and `TestKeyProviderKmip` to test your connection.

- Authentication failure

To resolve this fault, check that the correct root CA and KMIP client certificates are being used, and that the private key and the KMIP client certificate match.

- Server error

To resolve this fault, check the details for the error. Troubleshooting on the External Key Server might be necessary based on the error returned.

- **memoryEccThreshold**

A large number of correctable or uncorrectable ECC errors have been detected. This fault uses the following severities based on urgency:

Event	Severity	Description
A single DIMM <code>cErrorCount</code> reaches <code>cDimmCorrectableErrWarnThreshold</code> .	Warning	Correctable ECC memory errors above threshold on DIMM: <Processor> <DIMM Slot>
A single DIMM <code>cErrorCount</code> stays above <code>cDimmCorrectableErrWarnThreshold</code> until <code>cErrorFaultTimer</code> expires for the DIMM.	Error	Correctable ECC memory errors above threshold on DIMM: <Processor> <DIMM>
A memory controller reports <code>cErrorCount</code> above <code>cMemCtrlCorrectableErrWarnThreshold</code> , and <code>cMemCtrlCorrectableErrWarnDuration</code> is specified.	Warning	Correctable ECC memory errors above threshold on memory controller: <Processor> <Memory Controller>

A memory controller reports cErrorCount above cMemCtrlrCorrectableErrWarnThreshold until cErrorFaultTimer expires for the memory controller.	Error	Correctable ECC memory errors above threshold on DIMM: <Processor> <DIMM>
A single DIMM reports a uErrorCount above zero, but less than cDimmUncorrectableErrFaultThreshold.	Warning	Uncorrectable ECC memory error(s) detected on DIMM: <Processor> <DIMM Slot>
A single DIMM reports a uErrorCount of at least cDimmUncorrectableErrFaultThreshold.	Error	Uncorrectable ECC memory error(s) detected on DIMM: <Processor> <DIMM Slot>
A memory controller reports a uErrorCount above zero, but less than cMemCtrlrUncorrectableErrFaultThreshold.	Warning	Uncorrectable ECC memory error(s) detected on memory controller: <Processor> <Memory Controller>
A memory controller reports a uErrorCount of at least cMemCtrlrUncorrectableErrFaultThreshold.	Error	Uncorrectable ECC memory error(s) detected on memory controller: <Processor> <Memory Controller>

To resolve this fault, contact NetApp Support for assistance.

- **memoryUsageThreshold**

Memory usage is above normal. This fault uses the following severities based on urgency:



See the **Details** heading in the error fault for more detailed information on the type of fault.

Severity	Description
Warning	System memory is low.
Error	System memory is very low.
Critical	System memory is completely consumed.

To resolve this fault, contact NetApp Support for assistance.

- **metadataClusterFull**

There is not enough free metadata storage space to support a single node loss. See the GetClusterFullThreshold API method for details on cluster fullness levels. This cluster fault indicates one of

the following conditions:

- **stage3Low (Warning)**: User-defined threshold was crossed. Adjust Cluster Full settings or add more nodes.
- **stage4Critical (Error)**: There is not enough space to recover from a 1-node failure. Creation of volumes, snapshots, and clones is not allowed.
- **stage5CompletelyConsumed (Critical)**1; No writes or new iSCSI connections are allowed. Current iSCSI connections will be maintained. Writes will fail until more capacity is added to the cluster. Purge or delete data or add more nodes.

To resolve this fault, purge or delete volumes or add another storage node to the storage cluster.

- **mtuCheckFailure**

A network device is not configured for the proper MTU size.

To resolve this fault, ensure that all network interfaces and switch ports are configured for jumbo frames (MTUs up to 9000 bytes in size).

- **networkConfig**

This cluster fault indicates one of the following conditions:

- An expected interface is not present.
- A duplicate interface is present.
- A configured interface is down.
- A network restart is required.

Contact NetApp Support for assistance.

- **noAvailableVirtualNetworkIPAddresses**

There are no available virtual network addresses in the block of IP addresses.

- **virtualNetworkID # TAG(###)** has no available storage IP addresses. Additional nodes cannot be added to the cluster.

To resolve this fault, add more IP addresses to the block of virtual network addresses.

- **nodeHardwareFault (Network interface <name> is down or cable is unplugged)**

A network interface is either down or the cable is unplugged.

To resolve this fault, check network connectivity for the node or nodes.

- **nodeHardwareFault (Drive encryption capable state mismatches node's encryption capable state for the drive in slot <node slot><drive slot>)**

A drive does not match encryption capabilities with the storage node it is installed in.

- **nodeHardwareFault (Incorrect <drive type> drive size <actual size> for the drive in slot <node slot><drive slot> for this node type - expected <expected size>)**

A storage node contains a drive that is the incorrect size for this node.

- **nodeHardwareFault (Unsupported drive detected in slot <node slot><drive slot>; drive statistics and health information will be unavailable)**

A storage node contains a drive it does not support.

- **nodeHardwareFault (The drive in slot <node slot><drive slot> should be using firmware version <expected version>, but is using unsupported version <actual version>)**

A storage node contains a drive running an unsupported firmware version.

- **nodeMaintenanceMode**

A node has been placed in maintenance mode. This fault uses the following severities based on urgency:

Severity	Description
Warning	Indicates that the node is still in maintenance mode.
Error	Indicates that maintenance mode has failed to disable, most likely due to failed or active standbys.

To resolve this fault, disable maintenance mode once maintenance completes. If the Error level fault persists, contact NetApp Support for assistance.

- **nodeOffline**

Element software cannot communicate with the specified node. Check network connectivity.

- **notUsingLACPBondMode**

LACP bonding mode is not configured.

To resolve this fault, use LACP bonding when deploying storage nodes; clients might experience performance issues if LACP is not enabled and properly configured.

- **ntpServerUnreachable**

The storage cluster cannot communicate with the specified NTP server or servers.

To resolve this fault, check the configuration for the NTP server, network, and firewall.

- **ntpTimeNotInSync**

The difference between storage cluster time and the specified NTP server time is too large. The storage cluster cannot correct the difference automatically.

To resolve this fault, use NTP servers that are internal to your network, rather than the installation defaults. If you are using internal NTP servers and the issue persists, contact NetApp Support for assistance.

- **nvramDeviceStatus**

An NVRAM device has an error, is failing, or has failed. This fault has the following severities:

Severity	Description
----------	-------------

Warning	<p>A warning has been detected by the hardware. This condition may be transitory, such as a temperature warning.</p> <ul style="list-style-type: none"> • nvmLifetimeError • nvmLifetimeStatus • energySourceLifetimeStatus • energySourceTemperatureStatus • warningThresholdExceeded
Error	<p>An Error or Critical status has been detected by the hardware. The cluster master attempts to remove the slice drive from operation (this generates a drive removal event). If secondary slice services are not available the drive will not be removed. Errors returned in addition to the Warning level errors:</p> <ul style="list-style-type: none"> • NVRAM device mount point doesn't exist. • NVRAM device partition doesn't exist. • NVRAM device partition exists, but not mounted.
Critical	<p>An Error or Critical status has been detected by the hardware. The cluster master attempts to remove the slice drive from operation (this generates a drive removal event). If secondary slice services are not available the drive will not be removed.</p> <ul style="list-style-type: none"> • persistenceLost • armStatusSaveNArmed • csaveStatusError

Replace any failed hardware in the node. If this does not resolve the issue, contact NetApp Support for assistance.

- **powerSupplyError**

This cluster fault indicates one of the following conditions:

- A power supply is not present.
- A power supply has failed.
- A power supply input is missing or out of range.

To resolve this fault, verify that redundant power is supplied to all nodes. Contact NetApp Support for assistance.

- **provisionedSpaceTooFull**

The overall provisioned capacity of the cluster is too full.

To resolve this fault, add more provisioned space, or delete and purge volumes.

- **remoteRepAsyncDelayExceeded**

The configured asynchronous delay for replication has been exceeded. Check network connectivity between clusters.

- **remoteRepClusterFull**

The volumes have paused remote replication because the target storage cluster is too full.

To resolve this fault, free up some space on the target storage cluster.

- **remoteRepSnapshotClusterFull**

The volumes have paused remote replication of snapshots because the target storage cluster is too full.

To resolve this fault, free up some space on the target storage cluster.

- **remoteRepSnapshotsExceededLimit**

The volumes have paused remote replication of snapshots because the target storage cluster volume has exceeded its snapshot limit.

To resolve this fault, increase the snapshot limit on the target storage cluster.

- **scheduleActionError**

One or more of the scheduled activities ran, but failed.

The fault clears if the scheduled activity runs again and succeeds, if the scheduled activity is deleted, or if the activity is paused and resumed.

- **sensorReadingFailed**

A sensor could not communicate with the Baseboard Management Controller (BMC).

Contact NetApp Support for assistance.

- **serviceNotRunning**

A required service is not running.

Contact NetApp Support for assistance.

- **sliceServiceTooFull**

A slice service has too little provisioned capacity assigned to it.

To resolve this fault, add more provisioned capacity.

- **sliceServiceUnhealthy**

The system has detected that a slice service is unhealthy and is automatically decommissioning it.

- Severity = Warning: No action is taken. This warning period will expire in 6 minutes.

- Severity = Error: The system is automatically decommissioning data and re-replicating its data to other healthy drives.

Check for network connectivity issues and hardware errors. There will be other faults if specific hardware components have failed. The fault will clear when the slice service is accessible or when the service has been decommissioned.

- **sshEnabled**

The SSH service is enabled on one or more nodes in the storage cluster.

To resolve this fault, disable the SSH service on the appropriate node or nodes or contact NetApp Support for assistance.

- **sslCertificateExpiration**

The SSL certificate associated with this node is nearing expiration or has expired. This fault uses the following severities based on urgency:

Severity	Description
Warning	Certificate expires within 30 days.
Error	Certificate expires within 7 days.
Critical	Certificate expires within 3 days or has already expired.

To resolve this fault, renew the SSL certificate. If needed, contact NetApp Support for assistance.

- **strandedCapacity**

A single node accounts for more than half of the storage cluster capacity.

In order to maintain data redundancy, the system reduces the capacity of the largest node so that some of its block capacity is stranded (not used).

To resolve this fault, add more drives to existing storage nodes or add storage nodes to the cluster.

- **tempSensor**

A temperature sensor is reporting higher than normal temperatures. This fault can be triggered in conjunction with powerSupplyError or fanSensor faults.

To resolve this fault, check for airflow obstructions near the storage cluster. If needed, contact NetApp Support for assistance.

- **upgrade**

An upgrade has been in progress for more than 24 hours.

To resolve this fault, resume the upgrade or contact NetApp Support for assistance.

- **unresponsiveService**

A service has become unresponsive.

Contact NetApp Support for assistance.

- **virtualNetworkConfig**

This cluster fault indicates one of the following conditions:

- An interface is not present.
- There is an incorrect namespace on an interface.
- There is an incorrect netmask.
- There is an incorrect IP address.
- An interface is not up and running.
- There is a superfluous interface on a node.

Contact NetApp Support for assistance.

- **volumesDegraded**

Secondary volumes have not finished replicating and synchronizing. The message is cleared when the synchronizing is complete.

- **volumesOffline**

One or more volumes in the storage cluster are offline. The **volumeDegraded** fault will also be present.

Contact NetApp Support for assistance.

Monitor event logs for troubleshooting

You can review event logs for operations performed on the selected cluster along with cluster faults that might occur. Most errors are resolved automatically by the system. Other faults might require manual intervention.

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. Select **Reporting > Event Log**.
3. To review details, select an event and click **Details**.
4. Review the event information that includes the following:
 - **Event Type**: The type of event being logged; for example, API events or clone events.
 - **Service ID**: The ID of the service that reported the event (if applicable). The value is zero if the fault is not associated with a service.
 - **Node** or **Drive ID**: The ID of the node or drive that reported the event (if applicable).

Event types

The system reports multiple types of events; each event is an operation that the system has completed. Events can be routine, normal events or events that require administrator attention. The Event Type column on the Event Log page indicates in which part of the system the event occurred.



The system does not log read-only API commands in the event log.

The following list describes the types of events that might appear in the event log.

- **apiEvent**: Events initiated by a user through an API or web UI that modify settings.
- **binAssignmentsEvent**: Events related to the assignment of data bins. Bins are essentially containers that hold data and are mapped across the cluster.
- **binSyncEvent**: System events related to a reassignment of data among block services.
- **bsCheckEvent**: System events related to block service checks.
- **bsKillEvent**: System events related to block service terminations.
- **bulkOpEvent**: Events related to operations performed on an entire volume, such as a backup, restore, snapshot, or clone.
- **cloneEvent**: Events related to volume cloning.
- **clusterMasterEvent**: Events appearing upon cluster initialization or upon configuration changes to the cluster, such as adding or removing nodes.
- **csumEvent**: Events related to invalid data checksums on the disk.
- **dataEvent**: Events related to reading and writing data.
- **dbEvent**: Events related to the global database maintained by ensemble nodes in the cluster.
- **driveEvent**: Events related to drive operations.
- **encryptionAtRestEvent**: Events related to the process of encryption on a cluster.
- **ensembleEvent**: Events related to increasing or decreasing the number of nodes in an ensemble.
- **fibreChannelEvent**: Events related to the configuration of and connections to the nodes.
- **gcEvent**: Events related to processes run every 60 minutes to reclaim storage on block drives. This process is also known as garbage collection.
- **ieEvent**: Internal system error.
- **installEvent**: Automatic software installation events. Software is being automatically installed on a pending node.
- **iSCSIEvent**: Events related to iSCSI issues in the system.
- **limitEvent**: Events related to the number of volumes or virtual volumes in an account or in the cluster nearing the maximum allowed.
- **maintenanceModeEvent**: Events related to the node maintenance mode, such as disabling the node.
- **networkEvent**: Events related to the status of virtual networking.
- **platformHardwareEvent**: Events related to issues detected on hardware devices.
- **remoteClusterEvent**: Events related to remote cluster pairing.
- **schedulerEvent**: Events related to scheduled snapshots.
- **serviceEvent**: Events related to system service status.

- **sliceEvent:** Events related to the Slice Server, such as removing a metadata drive or volume.

There are three types of slice reassignment events, which include information about the service where a volume is assigned:

- flipping: changing the primary service to a new primary service

```
sliceID oldPrimaryServiceID→newPrimaryServiceID
```

- moving: changing the secondary service to a new secondary service

```
sliceID {oldSecondaryServiceID(s)}→{newSecondaryServiceID(s)}
```

- pruning: removing a volume from a set of services

```
sliceID {oldSecondaryServiceID(s)}
```

- **snmpTrapEvent:** Events related to SNMP traps.
- **statEvent:** Events related to system statistics.
- **tsEvent:** Events related to the system transport service.
- **unexpectedException:** Events related to unexpected system exceptions.
- **ureEvent:** Events related to Unrecoverable Read Errors that occur while reading from the storage device.
- **vasaProviderEvent:** Events related to a VASA (vSphere APIs for Storage Awareness) Provider.

Find more information

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

Monitor volume performance

You can view performance information for all volumes in the selected cluster from Reporting tab of the plug-in extension point.

Steps

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. Select **Volume Performance**.
3. To change how often the data refreshes on the page, click **Refresh every list** and choose a value.

The default refresh interval is 10 seconds if the cluster has less than 1000 volumes; otherwise, the default is 60 seconds. If you choose a value of Never, automatic page refreshing is disabled.

Volume performance data

- **Name:** Name of the volume when it was created.
- **Account:** The name of the account assigned to the volume.
- **Access Groups:** The name of the volume access group or groups to which the volume belongs.
- **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 the max
- >100 = Client is using the burst
- **Total IOPS:** The total number of IOPS (read and write) currently being executed against the volume.
- **Read IOPS:** The total number of read IOPS currently being executed against the volume.
- **Write IOPS:** The total number of write IOPS currently being executed against the volume.
- **Total Throughput:** The total amount of throughput (read and write) currently being executed against the volume.
- **Read Throughput:** The total amount of read throughput currently being executed against the volume.
- **Write Throughput:** The total amount of write throughput currently being executed against the volume.
- **Total Latency (ms):** The average time, in microseconds, to complete read and write operations to a volume.
- **Read Latency (ms):** The average time, in microseconds, to complete read operations to the volume in the last 500 milliseconds.
- **Write Latency (ms):** The average time, in microseconds, to complete write operations to a volume in the last 500 milliseconds.
- **Queue Depth:** The number of outstanding read and write operations to the volume.
- **Average IO Size:** Average size in bytes of recent I/O to the volume in the last 500 milliseconds.

Find more information

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

Monitor iSCSI sessions to determine connection status

You can view information about iSCSI sessions that are connected to the selected cluster in the NetApp Element Plug-in for VMware vCenter Server.

Steps

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. Select **iSCSI Sessions**.

iSCSI session data

- **Node:** The node hosting the primary metadata partition for the volume.
- **Account:** The name of the account that owns the volume. If value is blank, a dash (-) will be displayed.
- **Volume:** The volume name identified on the node.
- **Volume ID:** ID of the volume associated with the Target IQN.
- **Initiator ID:** A system-generated ID for the initiator.
- **Initiator Alias:** An optional name for the initiator that makes finding the initiator easier in a long list.
- **Initiator IP:** The IP address of the endpoint that initiates the session.
- **Initiator IQN:** The IQN of the endpoint that initiates the session.
- **Target IP:** The IP address of the node hosting the volume.
- **Target IQN:** The IQN of the volume.
- **Created On:** Date the session was established.

Find more information

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

Monitor VM performance tiering with QoSSIOC events

You can view events related to QoSSIOC when a VM with a QoS-enabled datastore is reconfigured or issued a power or guest event.

You can view QoSSIOC events from the plug-in extension point in NetApp Element Plug-in for vCenter Server.

QoSSIOC events are displayed from locally added clusters. In a Linked Mode environment, log into the vSphere Web Client that has the cluster added locally to view QoSSIOC events for that cluster.



- 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 NetApp Element Plug-in for vCenter Server 4.10 and earlier to manage cluster resources from other vCenter Servers using [vCenter Linked Mode](#) is limited to local storage clusters only.

What you'll need

- At least one cluster must be added and running.
- The QoSSIOC service must be configured and verified running using the QoSSIOC Settings page for the plug-in.
- At least one datastore must have QoSSIOC automation enabled.

Steps

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

QoSSIOC event data

- **Date:** The date and time of the QoSSIOC event.
- **Datastore Name:** The user-defined datastore name.
- **Cluster IP:** The IP address of the cluster containing the datastore from which the event originated.
- **Volume ID:** The system-generated ID for the associated volume.
- **Min IOPs:** The current minimum IOPS QoS setting of the volume.
- **Max IOPs:** The current maximum IOPS QoS setting of the volume.
- **Burst IOPs:** The current maximum burst QoS setting of the volume.
- **Burst Time:** The length of time a burst is allowed.

Find more information

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

Protect data with the vCenter Plug-in

Protect data with the NetApp Element Plug-in for VMware vCenter Server

You can ensure that copies of your data are created and stored where you need them by using the NetApp Element Plug-in for VMware vCenter Server. To do this, you can create and manage volume and group snapshots, set up snapshot schedules, and create volume and cluster pair relationships for replication between remote clusters.

Options

- [Create and manage volume snapshots](#)
- [Create and manage group snapshots](#)
- [Create snapshot schedules](#)
- [Perform remote replication between clusters](#)

Find more information

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

Create and manage volume snapshots in vCenter Server

Creating a [volume snapshot](#) creates a point-in-time copy of a volume. The process takes only a small amount of system resources and space, which makes snapshot creation faster than cloning.

You can use snapshots to roll a volume back to the state it was in at the time the snapshot was created. However, because snapshots are simply replicas of volume metadata, you cannot mount or write to them.

Options

- [Create a volume snapshot](#)
- [View volume snapshot details](#)
- [Clone a volume from a snapshot](#)
- [Roll back a volume to a snapshot](#)
- [Back up a volume snapshot to an external object store](#)
- [Delete a volume snapshot](#)

Create a volume snapshot

You can create a snapshot of an active volume to preserve the volume image at any point in time.

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 that you intend to use is selected in the navigation bar.

2. Select the **Volumes** sub-tab.
3. From the **Active** view, select the check box for the volume to use for the snapshot.
4. Select **Actions**.
5. In the resulting menu, select **Create Snapshot**.
6. (Optional): In the Create Snapshot dialog box, enter a name for the snapshot.



Use descriptive naming best practices. This is especially important if multiple clusters or vCenter Servers are used in your environment. If you do not enter a name, the system creates a snapshot default name using the date and time that the snapshot was created.

7. (Optional) Select the **Include snapshot in replication when paired** check box to ensure that the snapshot is replicated when the parent volume is paired.
8. Select one of the following as the retention period for the snapshot:
 - **Keep forever**: Retains the snapshot on the system indefinitely.
 - **Set retention period**: Determine a length of time (days, hours, or minutes) for the system to retain the snapshot.



When you set a retention period, you select a period that begins at the current time. (Retention is not calculated from the snapshot creation time.)

9. To take a single, immediate snapshot, select **Take snapshot now**.
10. To schedule the snapshot to run at a future time, complete the following steps:
 - a. Select **Create snapshot schedule**.
 - b. Enter a schedule name.
 - c. Select a schedule type and configure the schedule details.
 - d. (Optional) Select the check box for **Recurrent Schedule** to repeat the scheduled snapshot periodically.
11. Select **OK**.

View volume snapshot details

You might want to verify that the snapshot was added.

Steps

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



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

2. Select the **Snapshots** sub-tab.
3. (Optional) Select one of the following filters:
 - **Individual**: Volume snapshots that are not members of a group snapshot.
 - **Members**: Volume snapshots that are members of a group snapshot.
 - **Inactive**: Volume snapshots that were created from volumes that have been deleted but not yet purged.
4. View the snapshot details.

Clone a volume from a snapshot

You can create a new volume from a snapshot of a volume. When you do this, the system uses the snapshot information to clone a new volume using the data contained on the volume at the time the snapshot was created. This process also stores information about other snapshots of the volume in the new created volume.

Steps

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



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

2. Select the **Snapshots** sub-tab.
3. Select one of two views:
 - **Individual**: Lists volume snapshots that are not members of a group snapshot.
 - **Members**: Lists volume snapshots that are members of a group snapshot.
4. Select the check box for the volume snapshot to clone as a volume.
5. Select **Actions**.
6. In the resulting menu, select **Clone Volume from Snapshot**.
7. Enter a volume name, the total size and select either GB or GiB for the new volume.
8. Select an access type for the volume:
 - **Read Only**: Only read operations are allowed.
 - **Read/Write**: Both read and write operations are allowed.
 - **Locked**: No read or write operations are allowed.
 - **Replication Target**: Designated as a target volume in a replicated volume pair.
9. Select a user account to associate with the new volume.
10. Select **OK**.
11. Validate the new volume:

- a. 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**.
- b. Select the **Volumes** sub-tab.
- c. From the **Active** view, confirm that the new volume is listed.



Refresh the page if needed.

Roll back a volume to a snapshot

You can roll back a volume to a snapshot at any time. This undoes any changes made to the volume since the snapshot was created.

Steps

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



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

2. Select the **Snapshots** sub-tab.
3. Select one of two views:
 - **Individual**: Lists volume snapshots that are not members of a group snapshot.
 - **Members**: Lists volume snapshots that are members of a group snapshot.
4. Select the check box for the volume snapshot to use for the volume rollback.
5. Select **Actions**.
6. In the resulting menu, select **Rollback Volume to Snapshot**.
7. (Optional) To save the current state of the volume before rolling back to the snapshot:
 - a. In the Rollback to Snapshot dialog box, select **Save volume's current state as a snapshot**.
 - b. Enter a name for the new snapshot.
8. Select **OK**.

Back up a volume snapshot to an external object store

You can use the integrated backup feature to back up a volume snapshot. You can back up snapshots from a cluster running NetApp Element software to an external object store or to another Element-based cluster.

When you back up a snapshot to an external object store, you must have a connection to the object store that allows read/write operations.

- [Back up a volume snapshot to an Amazon S3 object store](#)

- [Back up a volume snapshot to an OpenStack Swift object store](#)
- [Back up a volume snapshot to a cluster running Element software](#)

Back up a volume snapshot to an Amazon S3 object store

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

Steps

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



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

2. Select the **Snapshots** sub-tab.
3. Select the check box for the volume snapshot you want to back up.
4. Select **Actions**.
5. In the resulting menu, select **Backup to**.
6. In the dialog under **Back up volume to**, select **Amazon S3**.
7. 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.
8. Enter the details:
 - **Host name**: Enter a host name to use to access the object store.
 - **Access key ID**: Enter an access key ID for the account.
 - **Secret access key**: Enter the secret access key for the account.
 - **Amazon S3 Bucket**: Enter the S3 bucket in which to store the backup.
 - **Prefix**: (Optional) Enter a prefix for the backup name.
 - **Nametag**: (Optional) Enter a nametag to append to the prefix.
9. Select **OK**.

Back up a volume snapshot to an OpenStack Swift object store

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

Steps

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



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

2. Select the **Snapshots** sub-tab.
3. Select the check box for the volume snapshot you want to back up.
4. Select **Actions**.
5. In the resulting menu, select **Backup to**.
6. In the dialog under **Back up volume to**, select **OpenStack Swift**.
7. 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.
8. Enter the details:
 - **URL**: Enter a URL to use to access the object store.
 - **User name**: Enter user name for the account.
 - **Authentication key**: Enter the authentication key for the account.
 - **Container**: Enter the container in which to store the backup.
 - **Prefix**: (Optional) Enter a prefix for the backup volume name.
 - **Nametag**: (Optional) Enter a name tag to append to the prefix.
9. Select **OK**.

Back up a volume snapshot to a cluster running Element software

You can back up a volume snapshot that resides on a cluster running NetApp Element software to a remote Element cluster.

What you'll need

You must create a volume on the destination cluster of equal or greater size to the snapshot you are using for the backup.

About this task


When you back up or restore 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.

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 that you intend to use is selected in the navigation bar.

2. Select the **volumes** sub-tab.
 3. Select the check box for the destination volume.
 4. Select **Actions**.
 5. In the resulting menu, select **Restore from**.
 6. In the dialog under **Restore from**, select **NetApp Element**.
 7. 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.
 8. Select **Generate Key** to generate a bulk volume write key for the destination volume.
 9. Copy the bulk volume write key to your clipboard to apply to later steps on the source cluster.
 10. From the vCenter that contains the source cluster, open the **Protection** tab:
 - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Protection**.
 - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Protection**.
- 

If two or more clusters are added, ensure that the cluster you intend to use for the task is selected in the navigation bar.
11. Select the check box for the snapshot you are using for the backup.
 12. Select **Actions**.
 13. In the resulting menu, select **Backup to**.
 14. In the dialog box under **Back up volume to**, select **NetApp Element**.
 15. Select the same option as the destination cluster under **with the following data format**.
 16. Enter the details:
 - **Remote cluster MVIP**: Enter the management virtual IP address of the destination volume's cluster.
 - **Remote cluster user password**: Enter the remote cluster user name.
 - **Remote user password**: Enter the remote cluster password.
 - **Bulk volume write key**: Paste the key you generated on the destination cluster earlier.
 17. Select **OK**.

Delete a volume snapshot

You can delete a volume snapshot from a cluster running NetApp Element software using the plug-in extension point. When you delete a snapshot, the system immediately removes it.

About this task

You can delete snapshots that are being replicated from the source cluster. If a snapshot is syncing to the target cluster when you delete it, the sync replication completes and the snapshot is deleted from the source cluster. The snapshot is not deleted from the target cluster.

You can also delete snapshots that have been replicated to the target from the target cluster. The deleted snapshot is kept in a list of deleted snapshots on the target until the system detects that you have deleted the snapshot on the source cluster. After the target has detected that you have deleted the source snapshot, the

target stops replication of the snapshot.

Steps

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



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

2. From the **Snapshots** sub-tab, select one of the following views:
 - **Individual**: A list of volume snapshots that are not part of a group snapshot.
 - **Inactive**: A list of volume snapshots that were created from volumes that have been deleted but not yet purged.
3. Select the check box for the volume snapshot 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 group snapshots in vCenter Server

You can create a group snapshot of a related set of volumes to preserve a point-in-time copy of the metadata for each volume. You can use the group snapshot as a backup or rollback to restore the state of the group of volumes to a desired point in time.

Options

- [Create a group snapshot](#)
- [View group snapshot details](#)
- [Clone volumes from a group snapshot](#)
- [Roll back volumes to a group snapshot](#)
- [Delete a group snapshot](#)

Create a group snapshot

You can create a snapshot of a group of volumes immediately or create a schedule to automate future snapshots of the group of volumes. A single group snapshot can consistently snapshot up to 32 volumes at one time.

You can later change replication settings or the retention period for a group snapshot. The retention period you specify begins when you enter the new interval. When you set a retention period, you can select a period that

begins at the current time (retention is not calculated from the snapshot creation time). You can specify intervals in minutes, hours, and days.

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 that you intend to use is selected in the navigation bar.

2. Click the **Volumes** sub-tab.

3. From the **Active** view, select the check box for the volume to use for the snapshot.

4. Click **Actions**.

5. In the resulting menu, select **Create Group Snapshot**.

6. (Optional) In the Create Group Snapshot dialog box, enter a name for the snapshot.



Use descriptive naming best practices. This is especially important if multiple clusters or vCenter Servers are used in your environment. If you do not enter a name, the system creates a group snapshot default name using the date and time that the snapshot was created.

7. (Optional) Select the **Include snapshot in replication when paired** check box to ensure that the snapshot is replicated when the parent volume is paired.

8. Select one of the following as the retention period for the snapshot:

- **Keep forever:** Retains the snapshot on the system indefinitely.
- **Set retention period:** Determine a length of time (days, hours, or minutes) for the system to retain the snapshot.



When you set a retention period, you select a period that begins at the current time. (Retention is not calculated from the snapshot creation time.)

9. To take a single, immediate snapshot, select **Take group snapshot now**.

10. To schedule the snapshot to run at a future time, complete the following steps:

- a. Select **Create snapshot schedule**.
- b. Enter a schedule name.
- c. Select a schedule type and configure the schedule details.
- d. (Optional) Select the check box for **Recurrent Schedule** to repeat the scheduled snapshot periodically.

11. Click **OK**.

View group snapshot details

You might want to verify that the snapshot was added.

Steps

1. From the vCenter Plug-in, open the **Protection** tab:

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



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

2. Click the **Group Snapshots** sub-tab.

3. Verify the snapshot details:

- **Create date:** The date and time when the group snapshot was created.
- **Status:** Displays the status of the snapshot on the remote cluster running NetApp Element software:
 - **Preparing:** The snapshot is being prepared for use and is not yet writable.
 - **Done:** This snapshot has finished preparation and is now usable.
 - **Active:** The snapshot is the active branch.
- **Number of volumes:** Number of volumes in the group snapshot.

Clone volumes from a group snapshot

You can clone a group of volumes from a point-in-time group snapshot. After you create the volumes, you can use them like any other volume in the system.

Steps

1. From the vCenter Plug-in, open the **Protection** tab:

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



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

2. Click the **Group Snapshots** sub-tab.

3. Select the check box for the group snapshot to use for the volume clones.

4. Click **Actions**.

5. In the resulting menu, select **Clone Volumes from Group Snapshot**.

6. (Optional) Enter a new volume name prefix, which will be applied to all volumes created from the group snapshot.

7. (Optional) Select a different account to which the clone will belong. If you do not select an account, the system assigns the new volumes to the current volume account.

8. Select a different access method for the volumes in the clone. If you do not select a method, the system uses the current volume access:

- **Read Only:** Only read operations are allowed.
- **Read/Write:** All read and write operations are accepted.

- **Locked:** Only administrator access is allowed.
- **Replication Target:** Designated as a target volume in a replicated volume pair.

9. Click **OK**.



Volume size and current cluster load affect the time needed to complete a cloning operation.

Roll back volumes to a group snapshot

You can roll back a group of active volumes to a group snapshot. This restores all the associated volumes in a group snapshot to their state at the time the group snapshot was created. This procedure also restores volume sizes to the size recorded in the original snapshot. If the system has purged a volume, all snapshots of that volume were also deleted at the time of the purge; the system does not restore any deleted volume snapshots.

Steps

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



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

2. Click the **Group Snapshots** sub-tab.
3. Select the check box for the group snapshot to use for the volume rollback.
4. Click **Actions**.
5. In the resulting menu, select **Rollback Volumes to Group Snapshot**.
6. (Optional) To save the current state of the volumes before rolling back to the snapshot:
 - a. In the **Rollback to Snapshot** dialog box, select **Save volumes' current state as a group snapshot**.
 - b. Enter a name for the new snapshot.
7. Click **OK**.

Delete a group snapshot

You can delete a group snapshot from the system. When you delete the group snapshot, you can choose whether all snapshots associated with the group are deleted or retained as individual snapshots.

If you delete a volume or snapshot that is a member of a group snapshot, you can no longer roll back to the group snapshot. However, you can roll back each volume individually.

Steps

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



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

2. Select the check box for the group snapshot you want to delete.
3. Click **Actions**.
4. In the resulting menu, select **Delete**.
5. Select one of the following options:
 - **Delete group snapshot and members:** Deletes the group snapshot and all member snapshots.
 - **Retain members:** Deletes the group snapshot but keeps all member snapshots.
6. Confirm the action.

Find more information

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

Create snapshot schedules

You can schedule a snapshot of a volume to occur automatically at specified date and time intervals. You can schedule either single volume snapshots or group snapshots to run automatically.

When you create snapshot schedules, you can store the resulting snapshots on a remote NetApp Element storage system if the volume is being replicated.



Schedules are created using UTC+0 time. You may need to adjust the actual time a snapshot will run based on your time zone.

- [Create a snapshot schedule](#)
- [View snapshot schedule details](#)
- [Edit a snapshot schedule](#)
- [Copy a snapshot schedule](#)
- [Delete a snapshot schedule](#)

Create a snapshot schedule

You can schedule a snapshot of a volume or volumes to occur automatically at specified intervals.

When you configure a snapshot schedule, you can choose from time intervals based on days of the week or days of the month. You can also specify the days, hours, and minutes before the next snapshot occurs.

If you schedule a snapshot to run at a time period that is not divisible by 5 minutes, the snapshot will run at the next time period that is divisible by 5 minutes. For example, if you schedule a snapshot to run at 12:42:00 UTC, it will run at 12:45:00 UTC. You cannot schedule a snapshot to run at intervals of less than 5 minutes.

Steps

1. From the vCenter Plug-in, open the **Protection** tab:

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



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

2. Select the **Schedules** sub-tab.

3. Select **Create Schedule**.

4. In the **Volume IDs CSV** field, enter a single volume ID or a comma-separated list of volume IDs to include in the snapshot schedule operation.

5. Enter a schedule name.

6. Select a schedule type and configure the details.

7. (Optional) To repeat the schedule indefinitely, check **Recurring Schedule**.

8. (Optional) In the New Snapshot Name field, enter a name for the new snapshot.



If you do not enter a name, the system creates a default snapshot name using the date and time the snapshot was created.

9. (Optional) Check **Include snapshot in replication when paired** to ensure that the snapshot is replicated when the parent volume is paired.

10. Select one of the following as the retention period for the snapshot:

- **Keep forever**: Retains the snapshot on the system indefinitely.
- **Set retention period**: Determine a length of time (days, hours, or minutes) for the system to retain the snapshot.



When you set a retention period, you select a period that begins at the current time. (Retention is not calculated from the snapshot creation time.)

11. Select **OK**.

View snapshot schedule details

You might want to verify snapshot schedule details.

Steps

1. From the vCenter Plug-in, open the **Protection** tab:

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



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

2. Select the **Schedules** page.

3. Verify the schedule details.

Edit a snapshot schedule

You can modify existing snapshot schedules. After modification, the next time the schedule runs it uses the updated attributes. Any snapshots created by the original schedule remain on the storage system.

Steps

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



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 **Schedules** sub-tab.
3. Select the check box for the snapshot schedule you want to edit.
4. Click **Actions**.
5. In the resulting menu, select **Edit**.
6. In the **Volume IDs CSV** field, modify the single volume ID or comma-separated list of volume IDs currently included in the snapshot operation.
7. (Optional) To pause an active schedule or resume a paused schedule, select the **Manually Pause Schedule** check box.
8. (Optional) Enter a different name for the schedule in the **New Schedule Name** field.
9. (Optional) Change the current schedule type to one of the following:
 - a. **Days of Week**: Select one of more days of the week and a time of day to create a snapshot.
 - b. **Days of Month**: Select one of more days of the month and a time of day to create a snapshot.
 - c. **Time Interval**: Select an interval for the schedule to run based on number of days, hours and minutes between snapshots.
10. (Optional) Select **Recurrent Schedule** to repeat the snapshot schedule indefinitely.
11. (Optional) Enter or modify the name for the snapshots defined by the schedule in the **New Snapshot Name** field.



If you leave the field blank, the system uses the time and date of the snapshot's creation as the name.

12. (Optional) Select the **Include snapshots in replication when paired** check box to ensure that the snapshots are captured in replication when the parent volume is paired.
13. (Optional) Select one of the following as the retention period for the snapshot:
 - **Keep forever**: Retains the snapshot on the system indefinitely.
 - **Set retention period**: Determine a length of time (days, hours, or minutes) for the system to retain the snapshot.



When you set a retention period, you select a period that begins at the current time (retention is not calculated from the snapshot creation time).

14. Click **OK**.

Copy a snapshot schedule

You can make a copy of a snapshot schedule and assign it to new volumes or use it for other purposes.

Steps

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



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 **Schedules** sub-tab.
3. Select the check box for the snapshot schedule you want to copy.
4. Click **Actions**.
5. In the resulting menu, click **Copy**.
The Copy Schedule dialog box appears, populated with the current attributes of the schedule.
6. (Optional) Enter a name and update attributes for the copy of the schedule.
7. Click **OK**.

Delete a snapshot schedule

You can delete a snapshot schedule. After you delete the schedule, it does not run any future scheduled snapshots. Any snapshots that were created by the schedule remain on the storage system.

Steps

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



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 **Schedules** sub-tab.
3. Select the check box for the snapshot schedule you want to delete.
4. Click **Actions**.
5. In the resulting menu, click **Delete**.
6. Confirm the action.

Find more information

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

Perform remote replication between clusters

For clusters running NetApp Element software, real-time replication enables the quick creation of remote copies of volume data. You can pair a storage cluster with up to four other storage clusters.

You can replicate volume data synchronously or asynchronously from either cluster in a cluster pair for failover and failback scenarios. You must first pair two NetApp Element clusters and then pair volumes on each cluster to take advantage of real-time remote replication.

What you'll need

- Ensure that you have added at least one cluster to the plug-in.
- Ensure that all node IP addresses on both management and storage networks for paired clusters are routed to each other.
- Ensure that the MTU of all paired nodes are the same and be supported end-to-end between clusters.
- Ensure that the difference between NetApp Element software versions on the clusters is no greater than one major version. If the difference is greater, one of the clusters must be upgraded to perform data replication.



WAN Accelerator appliances have not been qualified by NetApp for use when replicating data. These appliances can interfere with compression and deduplication if deployed between two clusters that are replicating data. Be sure to fully qualify the effects of any WAN Accelerator appliance before you deploy it in a production environment.

Steps

1. [Pair clusters](#)
2. [Pair volumes](#)
3. [Validate volume replication](#)
4. [Delete a volume relationship after replication](#)
5. [Manage volume relationships](#)

Pair clusters

You must pair two clusters as a first step to using real-time replication functionality. After you pair and connect two clusters, you can configure active volumes on one cluster to be continuously replicated to a second cluster, providing continuous data protection (CDP).

You can pair a source and target cluster using the MVIP of the target cluster if there is Cluster Admin access to both clusters. If Cluster Admin access is only available on one cluster in a cluster pair, a pairing key can be used on the target cluster to complete the cluster pairing.

What you'll need

- You need Cluster Admin privileges to one or both clusters being paired.

- Ensure there is less than 2000 ms of round-trip latency between clusters.
- Ensure that the difference between NetApp Element software versions on the clusters is no greater than one major version.
- Ensure that all node IPs on paired clusters are routed to each other.



Cluster pairing requires full connectivity between nodes on the management network. Replication requires connectivity between the individual nodes on the storage cluster network.

You can pair one NetApp Element cluster with up to four other clusters for replicating volumes. You can also pair clusters within the cluster group with each other.

Choose one of the following methods:

- [Pair clusters using known credentials](#)
- [Pair clusters with a pairing key](#)

Pair clusters using known credentials

You can pair two clusters for real-time replication by using the MVIP of one cluster to establish a connection with the other cluster. Cluster Admin access on both clusters is required to use this method.

About this task

The Cluster Admin user name and password is used to authenticate cluster access before the clusters can be paired.

If the MVIP is not known, or access to the cluster is not available, you can pair the cluster by generating a pairing key and use the key to pair the two clusters. For instructions, see [Pair clusters with a pairing key](#).

Steps

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



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 **Cluster Pairs** sub-tab.
3. Select **Create Cluster Pairing**.
4. Select one of the following:
 - **Registered Cluster:** If the remote cluster of the pairing is controlled by the same instance of the Element vCenter plug-in, select this.
 - **Credentialed Cluster:** If the remote cluster has known credentials that are outside of the Element vCenter plug-in configuration, select this.
5. If you selected **Registered Cluster**, select a cluster from the list of available clusters and click **Pair**.
6. If you selected **Credentialed Cluster**, do the following:
 - a. Enter the remote cluster MVIP address.

- b. Enter a cluster administrator user name.
 - c. Enter a cluster administrator password.
 - d. Select **Start Pairing**.
7. After the task completes and you see the Cluster Pairs page, verify that the cluster pair is connected.
 8. (Optional) On the remote cluster, verify that the cluster pair is connected by using the Element UI or the plug-in extension points:
 - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Protection > Cluster Pairs**.
 - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Protection > Cluster Pairs**.

Pair clusters with a pairing key

If you have Cluster Admin access to a local cluster but not the remote cluster, you can pair the clusters using a pairing key. A pairing key is generated on a local cluster and then sent securely to a Cluster Admin at a remote site to establish a connection and complete the cluster pairing for real-time replication.

This procedure describes cluster pairing between two clusters using vCenter on the local and remote sites. For clusters not controlled by the vCenter Plug-in, you can alternatively [start or complete cluster pairing](#) using the Element web UI.

Steps

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



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 **Cluster Pairs** sub-tab.
3. Select **Create Cluster Pairing**.
4. Select **Inaccessible Cluster**.
5. Select **Generate Key**.



This action generates a text key for pairing and creates an unconfigured cluster pair on the local cluster. If you do not complete the procedure, you will need to manually delete the cluster pair.

6. Copy the cluster pairing key to your clipboard.
7. Select **Close**.
8. Make the pairing key accessible to the Cluster Admin at the remote cluster site.



The cluster pairing key contains a version of the MVIP, user name, password, and database information to permit volume connections for remote replication. This key should be treated in a secure manner and not stored in a way that would allow accidental or unsecured access to the user name or password.



Do not modify any of the characters in the pairing key. The key becomes invalid if it is modified.

9. From the vCenter that contains the remote cluster, [open the Protection tab](#).



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



You can alternatively complete the pairing using the Element UI.

10. Select the **Cluster Pairs** sub-tab.

11. Select **Complete Cluster Pairing**.



Wait for the loading spinner to disappear before proceeding to the next step. If an unexpected error occurs during the pairing process, check for and manually delete any unconfigured cluster pairs on the local and remote cluster and perform the pairing again.

12. Paste the pairing key from the local cluster in the **Cluster Pairing Key** field.

13. Select **Pair Cluster**.

14. After the task completes and you see the **Cluster Pair** page, verify that the cluster pair is connected.

15. To verify that the cluster pair is connected, on the remote cluster [open the Protection tab](#) or use the Element UI.

Validate the cluster pair connections

After the cluster pairing has completed, you might want to verify the cluster pair connection to ensure replication success.

Steps

1. On the local cluster, select **Data Protection > Cluster Pairs**.
2. Verify that the cluster pair is connected.
3. Navigate back to the local cluster and the **Cluster Pairs** window and verify that the cluster pair is connected.

Pair volumes

After you have established a connection between clusters in a cluster pair, you can pair a volume on one cluster with a volume on the other cluster in the pair.

You can pair the volume using one of the following methods:

- [Pair volumes using known credentials](#): Use known credentials for both clusters
- [Pair volumes using a pairing key](#): Use a pairing key if cluster credentials are available only on the source cluster.
- [Create target volumes and pair them with local volumes](#): If you know the credentials for both clusters, create a replication target volume on the remote cluster to pair with the source cluster.

After a volume pairing relationship is established, you must identify which volume is the replication target:

- [Assign a replication source and target to paired volumes](#)

What you'll need

- You should have established a connection between clusters in a cluster pair.
- You need to have Cluster admin privileges to one or both clusters being paired.

Pair volumes using known credentials

You can pair a local volume with another volume on a remote cluster. Use this method if there is Cluster Admin access to both clusters on which volumes are to be paired. This method uses the volume ID of the volume on the remote cluster to initiate a connection.

Before you begin

- You have Cluster Admin credentials for the remote cluster.
- Ensure that the clusters containing the volumes are paired.
- You know the remote Volume ID unless you intend to create a new volume during this process.
- If you intend for the local volume to be the source, ensure that the access mode of the volume is set to Read/Write.

Steps

1. From the vCenter that contains the local cluster, 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** sub-tab.
3. From the **Active** view, select the check box for the volume that you want to pair.
4. Select **Actions**.
5. Select **Volume Pairing**.
6. Select one of the following:
 - **Volume Creation:** To create a replication target volume on the remote cluster, select this. This method can be used only on remote clusters that are controlled by a Element vCenter plug-in.
 - **Volume Selection:** If the remote cluster for the target volume is controlled by a Element vCenter plug-in, select this.
 - **Volume ID:** If the remote cluster for the target volume has known credentials that are outside of the Element vCenter plug-in configuration, select this.
7. Select a Replication Mode:
 - **Real-time (Synchronous):** Writes are acknowledged to the client after they are committed on both of the source and target clusters.
 - **Real-time (Asynchronous):** Writes are acknowledged to the client after they are committed on the source cluster.
 - **Snapshots Only:** Only snapshots created on the source cluster are replicated. Active writes from the

source volume are not replicated.

8. If you selected **Volume Creation** as the pairing mode option, do the following:

a. Select a paired cluster from the drop-down list.



This action populates the available accounts on the cluster to be selected in the next step.

b. Select an account on the target cluster for the replication target volume.

c. Enter a replication target volume name.



Volume size cannot be adjusted during this process.

9. If you selected **Volume Selection** as the pairing mode option, do the following:

a. Select a paired cluster.



This action populates the available volumes on the cluster to be selected in the next step.

b. (Optional) Select the **Set remote volume to Replication Target** option if you want to set the remote volume as the target in the volume pairing. The local volume, if set to read/write, becomes the source in the pair.



If you assign an existing volume as the replication target, the data on that volume will be overwritten. As a best practice, you should use a new volume as the replication target.



You can also assign replication source and target later in the pairing process from **Volumes > Actions > Edit**. You must assign a source and target to complete the pairing.

c. Select a volume from the list of available volumes.

10. If you selected **Volume ID** as the pairing mode option, do the following:

a. Select a paired cluster from the drop-down list.

b. If the cluster is not registered with the plug-in, enter a cluster administrator user ID and a cluster administrator password.

c. Enter a volume ID.

d. Select the **Set remote volume to Replication Target** option if you want to set the remote volume as the target in the volume pairing. The local volume, if set to read/write, becomes the source in the pair.



If you assign an existing volume as the replication target, the data on that volume will be overwritten. As a best practice, you should use a new volume as the replication target.



You can also assign replication source and target later in the pairing process from **Volumes > Actions > Edit**. You must assign a source and target to complete the pairing.

11. Select **Pair**.



After you confirm the pairing, the two clusters begin the process of connecting the volumes. During the pairing process, you can see progress messages in the Volume Status column on the Volume Pairs page.



If you have not yet assigned a volume to be the replication target, the pairing configuration is not complete. The volume pair displays PausedMisconfigured until the volume pair source and target are assigned. You must assign a source and target to complete the volume pairing.

12. Select **Protection > Volume Pairs** on either cluster.

13. Verify the status of the volume pairing.

Pair volumes using a pairing key

You can pair a local volume with another volume on a remote cluster using a pairing key. Use this method if there is Cluster Admin access to only the source cluster. This method generates a pairing key that can be used on the remote cluster to complete the volume pair.

Before you begin

- Ensure that the clusters containing the volumes are paired.
- **Best Practices:** Set the source volume to Read/Write and the target volume to Replication Target. The target volume should contain no data and have the exact characteristics of the source volume, such as size, 512e setting, and QoS configuration. If you assign an existing volume as the replication target, the data on that volume will be overwritten. The target volume may be greater or equal in size to the source volume, but it cannot be smaller.

About this task

This procedure describes volume pairing between two volumes using vCenter on the local and remote sites. For volumes not controlled by the vCenter Plug-in, you can alternately start or complete volume pairing using the Element web UI.

For instructions on starting or completing volume pairing from the Element web UI, see [NetApp Element software documentation](#).



The volume pairing key contains an encrypted version of the volume information and may contain sensitive information. Share this key only in a secure manner.

Steps

1. From the vCenter that contains the local cluster, 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** sub-tab.
3. From the **Active** view, select the check box for the volume that you want to pair.
4. Select **Actions**.

5. Select **Volume Pairing**.
6. Select **Inaccessible Cluster**.
7. Select a Replication Mode:
 - **Real-time (Synchronous)**: Writes are acknowledged to the client after they are committed on both of the source and target clusters.
 - **Real-time (Asynchronous)**: Writes are acknowledged to the client after they are committed on the source cluster.
 - **Snapshots Only**: Only snapshots created on the source cluster are replicated. Active writes from the source volume are not replicated.
8. Select **Generate Key**.



This action generates a text key for pairing and creates an unconfigured volume pair on the local cluster. If you don't do this, you will need to manually delete the volume pair.

9. Copy the pairing key to your clipboard.
10. Select **Close**.
11. Make the pairing key accessible to the Cluster Admin at the remote cluster site.



The volume pairing key should be treated in a secure manner and not stored in a way that would allow accidental or unsecured access.



Do not modify any of the characters in the pairing key. The key becomes invalid if it is modified.

12. From the vCenter that contains the remote cluster, [open the Management tab](#).



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

13. Select the **Volumes** sub-tab.
14. From the **Active** view, select the check box for the volume you want to pair.
15. Select **Actions**.
16. Select **Volume Pairing**.
17. Select **Complete Cluster Pairing**.
18. Paste the pairing key from the other cluster into the **Pairing Key** box.
19. Select **Complete Pairing**.



After you confirm the pairing, the two clusters begin the process of connecting the volumes. During the pairing process, you can see progress messages in the Volume Status column of the Volume Pairs page. If an unexpected error occurs during the pairing process, check for and manually delete any unconfigured cluster pairs on the local and remote cluster and perform the pairing again.



If you have not yet assigned a volume to be the replication target, the pairing configuration is not complete. The volume pair displays "PausedMisconfigured" until the volume pair source and target are assigned. You must assign a source and target to complete the volume pairing.

20. Select **Protection > Volume Pairs** on either cluster.

21. Verify the status of the volume pairing.



Volumes that are paired using a pairing key appear after the pairing process has been completed at the remote location.

Create target volumes and pair them with local volumes

You can pair two or more local volumes with associated target volumes on a remote cluster. This process creates a replication target volume on the remote cluster for each local source volume you select. Use this method if there is Cluster Admin access to both clusters on which volumes are to be paired and remote cluster is controlled by the plug-in.

This method uses the volume ID of each volume on the remote cluster to initiate one or more connections.

Before you begin

- Ensure that you have Cluster Admin credentials for the remote cluster.
- Ensure that the clusters containing the volumes are paired using the plug-in.
- Ensure that the remote cluster is controlled by the plug-in.
- Ensure that the access mode of each local volume is set to Read/Write.

Steps

1. From the vCenter that contains the local cluster, 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** sub-tab.
3. From the **Active** view, select two or more volumes that you want to pair.
4. Select **Actions**.
5. Select **Volume Pairing**.
6. Select a **Replication Mode**:
 - **Real-time (Synchronous)**: Writes are acknowledged to the client after they are committed on both of the source and target clusters.
 - **Real-time (Asynchronous)**: Writes are acknowledged to the client after they are committed on the source cluster.
 - **Snapshots Only**: Only snapshots created on the source cluster are replicated. Active writes from the source volume are not replicated.

7. Select a paired cluster from the drop-down list.
8. Select an account on the target cluster for the replication target volume.
9. (Optional) Type a prefix or suffix for the new volume names on the target cluster.



A sample volume name with the modified name appears.

10. Select **Create Pairs**.



After you confirm the pairing, the two clusters begin the process of connecting the volumes. During the pairing process, you can see progress messages in the Volume Status column on the Volume Pairs page. After the process completes, new target volumes are created and connected on the remote cluster.

11. Select **Protection > Volume Pairs** on either cluster.
12. Verify the status of the volume pairing.

Assign a replication source and target to paired volumes

If you did not assign a volume to be the replication target during volume pairing, configuration is not complete. You can use this procedure to assign a source volume and its replication target volume. A replication source or target can be either volume in a volume pair.

You can also use this procedure to redirect data from a source volume to a remote target volume should the source volume become unavailable.

Before you begin

You have access to the clusters containing the source and target volumes.

About this task

This procedure describes assigning source and replication volumes between two clusters using vCenter on the local and remote sites. For volumes not controlled by the vCenter Plug-in, you can alternately [assign a source or replication volume](#) using the Element web UI.

A replication source volume has read/write account access. A replication target volume can only be accessed by the replication source as read/write.

Best Practices: The target volume should contain no data and have the exact characteristics of the source volume, such as size, 512e setting, and QoS configuration. The target volume may be greater or equal in size to the source volume, but it cannot be smaller.

Steps

1. Select the cluster that contains the paired volume that you want to use as the replication source from the plug-in extension point:
 - Beginning with Element vCenter plug-in 5.0 From the **NetApp Remote Plugin > Management**.
 - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management**.
2. From the extension point for your Element Plug-in for vCenter Server version, select the **Management** tab.
3. Select the **Volumes** sub-tab.
4. From the **Active** view, select the check box for the volume that you want to edit.
5. Select **Actions**.

6. Select **Edit**.
7. From the Access drop-down list, select **Read/Write**.



If you are reversing source and target assignment, this action will cause the volume pair to display **PausedMisconfigured** until a new replication target is assigned. Changing access pauses volume replication and causes the transmission of data to cease. Be sure that you have coordinated these changes at both sites.

8. Select **OK**.
9. Select the cluster containing the paired volume that you want to use as the replication target:
 - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Management > Management**.
 - Beginning with Element vCenter plug-in 5.0 From the **NetApp Remote Plugin > Management > Management**.
10. Select the **Volumes** sub-tab.
11. From the **Active** view, select the check box for the volume you want to edit.
12. Select **Actions**.
13. Select **Edit**.
14. In the **Access** drop-down list, select **Replication Target**.



If you assign an existing volume as the replication target, the data on that volume will be overwritten. As a best practice, you should use a new volume as the replication target.

15. Select **OK**.

Validate volume replication

After a volume is replicated, you should ensure that the source and target volumes are active. When in Active state, volumes are paired, data is being sent from the source to the target volume, and the data is in sync.

Steps

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



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 **Volume Pairs** sub-tab.
3. Verify that the volume status is Active.

Delete a volume relationship after replication

After replication completes and you no longer need the volume pairing relationship, you can delete the volume relationship.

See [Delete a volume pair](#).

Manage volume relationships

You can manage volume relationships in many ways, such as pausing replication, reversing volume pairing, changing the mode of replication, deleting a volume pair, or deleting a cluster pair.

- [Pause replication](#)
- [Change the mode of replication](#)
- [Delete a volume pair](#)
- [Delete a cluster pair](#)

Pause replication

You can edit volume pair properties to manually pause replication.

Steps

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



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 **Volume Pairs** sub-tab.
3. Select the check box for the volume pair you want to edit.
4. Select **Actions**.
5. Select **Edit**.
6. Manually pause or start the replication process.



Pausing or resuming volume replication manually will cause the transmission of data to cease or resume. Be sure that you have coordinated these changes at both sites.

7. Select **Save Changes**.

Change the mode of replication

You can edit volume pair properties to make changes to the replication mode of the volume pair relationship.

Steps

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



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 **Volume Pairs** sub-tab.
3. Select the check box for the volume pair you want to edit.
4. Select **Actions**.
5. Select **Edit**.
6. Select a new replication mode:



Changing the mode of replication causes the mode to change immediately. Be sure that you have coordinated these changes at both sites.

- **Real-time (Synchronous)**: Writes are acknowledged to the client after they are committed on both the source and target clusters.
- **Real-time (Asynchronous)**: Writes are acknowledged to the client after they are committed on the source cluster.
- **Snapshots Only**: Only snapshots created on the source cluster are replicated. Active writes from the source volume are not replicated.

7. Select **Save Changes**.

Delete a volume pair

You can delete a volume pair if you want to remove a pair association between two volumes.

About this task

This procedure describes deleting a volume pairing relationship between two volumes using vCenter on the local and remote sites.

For volumes not controlled by the vCenter Plug-in, you can alternatively [delete a volume pair end](#) using the Element web UI.

Steps

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



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 **Volume Pairs** sub-tab.
3. Select one or more volume pairs you want to delete.
4. Select **Actions**.
5. Select **Delete**.
6. Confirm the details of each volume pair.



For clusters that are not managed by the plug-in, this action deletes only the volume pair end on the local cluster. You need to manually delete the volume pair end from the remote cluster to fully remove the pairing relationship.

7. (Optional for clusters managed by plug-in) Select the check box for **Change Replication Target Access to** and select a new access mode for the replication target volume. This new access mode will be applied after the volume pairing relationship has been removed.
8. Select **Yes**.

Delete a cluster pair

You can delete a cluster pairing relationship between two clusters using vCenter on the local and remote sites. To completely remove a cluster pairing relationship, you must remove cluster pair ends from both the local and remote clusters.

You can use the vCenter Plug-in to delete a cluster pair end.

For clusters not controlled by the vCenter Plug-in, you can alternatively [delete a cluster pair end](#) using the Element web UI.

Steps

1. From the vCenter that contains the local cluster, open the **Protection** tab:
 - Beginning with Element vCenter plug-in 5.0, select **NetApp Element Remote Plugin > Management > Protection**.
 - For Element vCenter plug-in 4.10 and earlier, select **NetApp Element Management > Protection**.
2. Select the **Cluster Pairs** sub-tab.
3. Select the check box for the cluster pair you want to delete.
4. Select **Actions**.
5. Select **Delete**.
6. Confirm action.



This action deletes only the cluster pair end on the local cluster. You need to manually delete the cluster pair end from the remote cluster to fully remove the pairing relationship.

7. Repeat the steps from the remote cluster in the cluster pairing.

Volume pairing messages and warnings

You can view the information for volumes that have been paired or are in the process of being paired on the Volume Pairs page of the Protection tab from the plug-in extension point. Beginning with Element vCenter plug-in 5.0, select the Management tab from the NetApp Element Remote Plugin extension point. For Element vCenter plug-in 4.10 and earlier, select the NetApp Element Management extension point.

The system displays pairing and progress messages in the Volume Status column.

- [Volume pairing messages](#)
- [Volume pairing warnings](#)

Volume pairing messages

You can view messages during the initial pairing process on the Volume Pairs page of the Protection tab from the plug-in extension point. These messages are displayed in the Volume Status column and can display on both source and target ends of the pairing.

- **PausedDisconnected**: Source replication or sync RPCs timed out. Connection to the remote cluster has been lost. Check network connections to the cluster.
- **ResumingConnected***: The remote replication sync is now active. Beginning the sync process and waiting for data.
- **ResumingRRSync***: A single helix copy of the volume metadata is being made to the paired cluster.
- **ResumingLocalSync***: A double helix copy of the volume metadata is being made to the paired cluster.
- **ResumingDataTransfer***: Data transfer has been resumed.
- **Active**: Volumes are paired and data is being sent from the source to the target volume and the data is in sync.
- **Idle**: No replication activity is occurring.

*This process is driven by the target volume and might not display on the source volume.

Volume pairing warnings

You can view warning messages after you pair volumes on the Volume Pairs page of the Protection tab from the plug-in extension point. These messages are displayed in the Volume Status column and can display on both source and target ends of the pairing.

These messages can display on both source and target ends of the pairing unless otherwise indicated.

- **PausedClusterFull**: Because the target cluster is full, source replication and bulk data transfer cannot proceed. The message displays on the source end of the pair only.
- **PausedExceededMaxSnapshotCount**: The target volume already has the maximum number of snapshots and cannot replicate additional snapshots.
- **PausedManual**: Local volume has been manually paused. It must be unpaused before replication resumes.
- **PausedManualRemote**: Remote volume is in manual paused mode. Manual intervention required to unpause the remote volume before replication resumes.
- **PausedMisconfigured**: Waiting for an active source and target. Manual intervention required to resume replication.
- **PausedQoS**: Target QoS could not sustain incoming IO. Replication auto-resumes. The message displays on the source end of the pair only.
- **PausedSlowLink**: Slow link detected and stopped replication. Replication auto-resumes. The message displays on the source end of the pair only.
- **PausedVolumeSizeMismatch**: Target volume is smaller than the source volume.
- **PausedXCopy**: A SCSI XCOPY command is being issued to a source volume. The command must complete before replication can resume. The message displays on the source end of the pair only.
- **StoppedMisconfigured**: A permanent configuration error has been detected. The remote volume has been purged or unpaired. No corrective action is possible; a new pairing must be established.

Find more information

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

Configure and manage virtual volumes

You can enable VMware vSphere [Virtual Volumes \(VVols\)](#) functionality and set up a virtual volumes configuration on a NetApp Element storage cluster. The Element Plug-in for vCenter Server monitors performance and gives you options to manage virtual volumes, [storage containers](#), [protocol endpoints](#), and hosts from the plug-in extension point.

What you'll need

- You are using a NetApp Element 10 or later cluster that is connected to an ESXi 6.5 or later environment with VVols compatibility.
- You are using vCenter 6.5 or later.

Setup tasks

You must perform initial configuration steps to use virtual volumes (VVols) in the NetApp Element Plug-in for vCenter Server.

Steps

1. [Enable virtual volumes functionality on the NetApp Element cluster](#)
2. [Register the VASA provider with vCenter](#)
3. [Create a storage container and associated VVol datastore](#)

Management tasks

- [Monitor virtual volume resources](#)
- [Create a VVol datastore for a storage container](#)
- [Delete a storage container](#)

Enable virtual volumes functionality on the NetApp Element cluster

You must manually enable vSphere Virtual Volumes (VVols) functionality using the plug-in extension point. The Element system comes with VVols functionality disabled by default, and it is not automatically enabled as part of a new installation or upgrade. Enabling the VVols feature is a one-time configuration task.

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 a cluster from the list that you want to enable.
3. Select **Actions**.
4. In the resulting menu, select **Enable VVols**.



After VVols functionality is enabled, it cannot be disabled. Enabling vSphere Virtual Volumes functionality permanently changes NetApp Element software configuration. You should only enable VVols functionality if your cluster is connected to a VMware ESXi VVols-compatible environment. You can only disable the VVols feature and restore the default settings by returning the cluster to the factory image.

5. Select **Yes** to confirm the Virtual Volumes configuration change.



When VVols functionality is enabled, the Element cluster starts the VASA Provider, opens port 8444 for VASA traffic, and creates protocol endpoints that can be discovered by vCenter and all ESXi hosts.

6. Select **Actions** for the selected cluster.
7. In the resulting menu, select **Details**.
8. Copy the VASA Provider URL from the **VASA Provider URL** field. You will use this URL to register the VASA Provider in vCenter.
9. See [Register the VASA provider with vCenter](#) for the next steps.

Register the VASA provider with vCenter

You must register the NetApp Element VASA Provider with vCenter so that vCenter is aware of VVol functionality on the cluster. Registering the VASA provider with vCenter is a one-time configuration task.

What you'll need

- You have enabled VVols functionality for the cluster.

About this task

This procedure describes the steps available in version 6.7 of vSphere. Your vSphere user interface may differ slightly from what is described depending on the version of vSphere installed. For additional help, see VMware vCenter documentation.



Do not register a NetApp Element VASA provider to more than one vCenter instance. The NetApp Element VASA provider can only be registered to a single vCenter due to limitations with how vCenter handles SSL. A single vCenter can have multiple NetApp Element clusters, but a cluster cannot be shared between two instances of vCenter.



For Element software 12.5 and earlier, do not register more than one NetApp Element VASA provider to a single vCenter instance. Where a second NetApp Element VASA provider is added, this renders all VVOL datastores inaccessible.



VASA support for up to 10 vCenters is available as an upgrade patch if you have already registered a VASA provider with your vCenter. To install, follow the directions in the VASA39 manifest and download the .tar.gz file from the [NetApp Software Downloads](#) site. The NetApp Element VASA provider uses a NetApp certificate. With this patch, the certificate is used unmodified by vCenter to support multiple vCenters for VASA and VVols use. Do not modify the certificate. Custom SSL certificates are not supported by VASA.

Steps

1. From vSphere Client Home, select **Hosts and Clusters**.

2. Select a vCenter instance on which to register the NetApp Element VASA Provider.
3. Select **Configure > Storage Providers**.
4. From **Storage Providers**, select the add icon.
5. Enter the following information in the **New Storage Provider** dialog box:
 - VASA Provider name.
 - VASA Provider URL.



The VASA Provider URL is provided to you when you enable VVols in the vCenter Plug-in. You can also find the URL from cluster details (**NetApp Element Configuration > Clusters** or **NetApp Element Remote Plugin > Configuration > Clusters**) or from cluster settings in the Element UI (<https://<MVIP>/cluster>).

- Administrative account user name for the NetApp Element cluster.
 - Administrative account password for the NetApp Element cluster.
6. Select **OK** to add the VASA Provider.
 7. Approve the thumbprint of the SSL cert when prompted.
The NetApp Element VASA Provider should now be registered with a status of **Connected**.



Refresh the storage provider, if necessary, to show the current status of the provider after registering the provider for the first time. You can also verify that the provider is enabled in **NetApp Element Configuration > Clusters** or **NetApp Element Remote Plugin > Configuration > Clusters**. Select **Actions** for the cluster you are enabling and select **Details**.

8. See [Create a storage container and associated VVol datastore](#) for the next steps.

Create a storage container and associated VVol datastore

You can create storage containers from the VVols tab in the plug-in extension point. You must create at least one storage container to begin provisioning VVol-backed virtual machines.

Before you begin

- You have enabled VVols functionality for the cluster.
- You have registered the NetApp Element VASA Provider for virtual volumes with vCenter.

Steps

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



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 **Storage Containers** sub-tab.
3. Select **Create Storage Container**.

4. Enter storage container information in the **Create a New Storage Container** dialog box:

a. Enter a name for the storage container.



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

b. Configure initiator and target secrets for CHAP.



Leave the CHAP Settings fields blank to automatically generate secrets.

c. Enter a name for the datastore. The **Create a datastore** check box is selected by default.



A VVol datastore is required to use the storage container in vSphere.

d. Select one or more hosts for the datastore.



If you are using vCenter Linked Mode, only hosts available to the vCenter Server to which the cluster is assigned are available to select.

e. Select **OK**.

5. Verify that the new storage container appears in the list in the **Storage Containers** sub-tab. Because a NetApp Element account ID is created automatically and assigned to the storage container, it is not necessary to manually create an account.

6. Verify that the associated datastore has also been created on the selected host in vCenter.

Monitor virtual volume resources

You can review virtual volume component performance and settings from the plug-in extension point:

- [Monitoring VVols](#)
- [Monitoring storage containers](#)
- [Monitoring protocol endpoints](#)

Monitoring VVols

You can review general data for all active virtual volumes on the cluster or detailed data for each virtual volume. The plug-in tracks virtual volume efficiency, performance, events, and QoS as well as associated snapshots, VMs, and bindings.

What you'll need

- You have powered on VMs so virtual volume details are available to view.

Steps

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

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



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 **Virtual Volumes** tab, you can search for a specific virtual volume.
3. Select the check box for the virtual volume you want to review.
4. Select **Actions**.
5. In the resulting menu, select **Details**.

Monitoring storage containers

You can review general data for all active storage containers on the cluster or detailed data for each storage container. The plug-in tracks storage container efficiency, performance, and associated virtual volumes.

Steps

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



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 **Storage Containers** tab.
3. Select the check box for the storage container you want to review.
4. Select **Actions**.
5. In the resulting menu, select **Details**.

Monitoring protocol endpoints

You can review general data for all protocol endpoints on the cluster.

Steps

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



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 **Protocol Endpoints** tab.
3. Select the check box for the protocol endpoint you want to review.
4. Select **Actions**.
5. In the resulting menu, select **Details**.

Create a VVol datastore for a storage container

After you create a storage container, you must also create a virtual volume datastore that represents the storage container on the NetApp Element cluster in vCenter. This procedure can be used as an alternative to creating a datastore from the [Create Storage Container](#) wizard. You must create at least one VVol datastore to begin provisioning VVol-backed virtual machines.

What you'll need

- An existing storage container in the virtual environment.



You might need to rescan NetApp Element storage in vCenter to discover storage containers.

Steps

1. From the Navigator view in vCenter, right-click a storage cluster and select **Storage > Datastores > New Datastore**.
2. In the **New Datastore** dialog box, select **VVol** as the type of datastore to create.
3. Provide a name for the datastore in the **Datastore name** field.
4. Select the NetApp Element storage container from the Backing Storage Container list.



You do not need to manually create protocol endpoint (PE) LUNs. They are automatically mapped to the ESXi hosts when the datastore is created.

5. Select the hosts that require access to the datastore.
6. Select **Next**.
7. Review the configurations and select **Finish** to create the VVol datastore.

Delete a storage container

You can delete storage containers from the plug-in extension point.

What you'll need

- All volumes have been removed from the storage container.

Steps

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



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 **Storage Containers** tab.
3. Select the check box for the storage container you want to delete.
4. Select **Actions**.

5. In the resulting menu, select **Delete**.
6. Confirm the action.
7. Refresh the list of storage containers in the **Storage Containers** sub-tab to confirm that the storage container has been removed.

Find more information

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

Unregister the vCenter Plug-in

You can unregister the NetApp Element Plug-in for VMware vCenter Server from vCenter using one of these procedures.

What you'll need

- vCenter Administrator role privileges to unregister a plug-in.
- The IP address of the management node.
- URL and credentials for the vCenter from which you are unregistering the plug-in.

About this task

For vSphere 6.7 and earlier, unregistering the plug-in has the same effect as disabling it but does not remove all associated files and folders that are installed locally. To remove all plug-in files, see instructions on [removing the plugin](#).

For vSphere 7.0, all files are removed automatically after you unregister the plugin.

Steps

1. To unregister the plug-in, follow the procedure for your installed version:
 - For vCenter Plug-in 3.0 or later, unregister the plug-in using the vCenter Plug-in registration utility:
 - a. Enter the IP address for your management node in a browser, including the TCP port for registration: <https://<ManagementNodeIP>:9443>.
 - b. Navigate to **Unregister Plug-in**.
 - c. Enter the following:
 - i. The IP address or FQDN server name of the vCenter service on which you have registered your plug-in.
 - ii. The vCenter Administrator user name.
 - iii. The vCenter Administrator password.
 - d. Select **Unregister**.
 - For vCenter Plug-in 2.7 to 2.7.1:
 - Use the vCenter Managed Object Browser (MOB) interface in your browser to manually unregister:
 - a. Enter the MOB URL: <https://<vcenter>/mob>
 - b. Select **Content > Extension Manager > UnregisterExtension**.
 - c. Enter `com.solidfire`.
 - d. Select **Invoke Method**.
 - Unregister using PowerCLI:

```
Connect-VIServer -Server $vcenter -User  
administrator@vsphere.local -Password xxxXXXx -Force -ErrorAction  
Stop -SaveCredentials  
$em = Get-View ExtensionManager  
$em.ExtensionList | ft -property Key  
$em.UnregisterExtension("com.solidfire")  
$em.UpdateViewData()  
$em.ExtensionList | ft -property Key  
Disconnect-VIServer * -Confirm:$false
```

Find more information

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

Remove the vCenter Plug-in

For vCenter Plug-in 4.0 to 4.10 used with vSphere 6.7 or earlier, you must complete the following process to remove all files associated with the plug-in manually from vCenter Server. For vSphere 7.0 and later, it is not necessary to remove files after you unregister the plug-in.

What you'll need

- vCenter Plug-in 4.0 to 4.10
- vSphere 6.7 or earlier
- You have [unregistered](#) the existing plug-in and have SSH, RDP, or other appropriate connectivity to vCSA or vCenter Server.

Steps

1. Log in as an administrator to the server that is running vCenter Server and open a command prompt.
2. Stop vCenter Server services:

- Windows:

- (For Flash clients) Run the following command:

```
C:\Program Files\VMware\vCenter Server\vmmon>.vmmon-cli --stop  
vsphere-client
```

- (For HTML5 clients) Run the following commands:

```
C:\Program Files\VMware\vCenter Server\vmmon>.vmmon-cli --stop  
vsphere-client  
C:\Program Files\VMware\vCenter Server\vmmon>.vmmon-cli --stop  
vsphere-ui
```

- vCenter Server Appliance (vCSA)

- (For Flash clients) Run the following command:

```
service-control --stop vsphere-client
```

- (For HTML5 clients) Run the following commands:

```
service-control --stop vsphere-client  
service-control --stop vsphere-ui
```

3. Remove SolidFire folders and files from the following locations:

- (For Windows) Use Windows Explorer and search for SolidFire in C:\ProgramData\VMware and

C:\Program Files\VMware.



The ProgramData folder is hidden. You must enter the complete file path to access the folder.

- (For vCSA) Run the following command:

```
find / -name "*solidfire*" -exec rm -rf {} \;
```

4. Start vCenter Server services:

- Windows:

- (For Flash clients) Run the following command:

```
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --start  
vsphere-client
```

- (For HTML5 clients) Run the following commands:

```
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --start  
vsphere-client  
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --start  
vsphere-ui
```

- vCSA:

- (For Flash clients) Run the following command:

```
service-control --start vsphere-client
```

- (For HTML5 clients) Run the following commands:

```
service-control --start vsphere-client  
service-control --start vsphere-ui
```

Find more information

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

Troubleshoot the vCenter Plug-in

You need to be aware of some of the common issues with the NetApp Element Plug-in for VMware vCenter Server and the steps to resolve them.

- [Plug-in registration successful but icons do not appear in web client](#)
- [Errors after NetApp Element Plug-in for VMware vCenter Server 4.8 or later upgrade with VMware vCenter Server 6.7U1](#)
- [Error registering plug-in using Registration UI](#)
- [Error updating plug-in using Registration UI](#)
- [Error message that NetApp extension cannot be upgraded](#)
- [Removing plug-in completes successfully but icons remain](#)
- [Plug-in cannot be unregistered or removed after admin password change](#)
- [Plug-in management tasks fail or volumes are not accessible to ESXi host](#)
- [Failure occurs during vCenter Plug-in use on Firefox 59.0.2 browsers](#)
- [Delete datastore operation fails](#)
- [Cluster pair cannot connect using a pairing key](#)
- [Error message for QoSSIOC status](#)
- [QoSSIOC service shown as available but is unavailable](#)
- [QoSSIOC is enabled for datastore but unavailable](#)
- [vCenter plug-in deployment fails after upgrading to VMware vSphere 7.0 Update 3](#)

Plug-in registration successful but icons do not appear in web client

Description

Registration shows as successful, but the plug-in icons are not visible from the vSphere Web Client.

Corrective Action for NetApp Element vCenter plug-in 4.10 and earlier

- Log out of the vSphere Web Client and log in again. Closing and re-opening your browser may be required.
- Clear your browser cache.
- From vCenter, restart the vSphere Web Client Service from the Services menu within Windows Administrative Tools or reboot vCenter.
- Ensure that you have all required default administrative privileges associated with the vCenter Administrator role.
- Check that the plug-in ZIP file successfully downloaded to vCenter:
 1. Open `vsphere_client_virgo.log` in vCenter. vCenter log files for versions 6.5 and 6.7 are in the following locations:
 - Flash installations: `/var/log/vmware/vsphere-client/logs/vsphere_client_virgo.log`
 - HTML5 installations: `/var/log/vmware/vsphere-ui/logs/vsphere_client_virgo.log`

2. If a failure message indicates that the ZIP download failed, download the ZIP again.



You might need to correct an unreachable or bad URL. Update the plug-in registration or unregister and register the plug-in again with a corrected URL. Failure to download the ZIP can also occur if you specified an HTTP URL without changing the `allowHTTP` setting.

- Verify networking ports. Ensure the management node is reachable from vCenter bidirectionally on the required ports.
- Check the vCenter's MOB extension record ("[com.solidfire](#)".server) that contains the download location URL for the plug-in ZIP:
 1. Paste the URL into a browser.
 2. Verify that the plug-in ZIP can be downloaded.
 - If the plug-in ZIP can be downloaded, proceed to the next step.
 - If the plug-in ZIP cannot be downloaded, check for networking issues between vCenter Server and the management node.
 3. If the plug-in cannot be downloaded, compare the `serverThumbprint` in the MOB record with the certificate SHA-1 for the ZIP URL that is displayed in the browser:
 - a. If the registration record in the MOB has an incorrect or stale URL or SHA-1, unregister the plug-in and register the plug-in again.
 - b. If the problem persists and the ZIP is unreachable, inspect the ZIP URL to determine if there is an issue with the management node address used. In some cases, it might be necessary to customize a URL using the registration utility for the plug-in so that the ZIP file can be downloaded.

Errors after NetApp Element Plug-in for VMware vCenter Server 4.8 or later upgrade with VMware vCenter Server 6.7U1

Description

After you upgrade to Element vCenter plug-in 4.8 or later with VMware vCenter Server 6.7U1, you might encounter the following issues:

- The clusters are not listed in the **Clusters** section in the plug-in extension point.
- A server error appears in the **Clusters** and **QoSSIOC Settings** sections.

Corrective Action

Restore the cluster and QoSSIOC settings:

1. Log out of vCenter.
2. After logging out, wait three to five minutes and then log back in.
3. In your current vSphere Client view, select the refresh icon.
4. Disable cache and refresh the browser, for example, by using Ctrl+F5.
5. Check if the clusters and QoSSIOC settings are restored.

If the issue persists, you need to [re-add the clusters for Element Plug-in 5.0 or later](#) or [re-add the clusters for Element Plug-in 4.10 or earlier](#).

Error registering plug-in using Registration UI

Description

When using the registration utility, there is an error registering the plug-in against the vCenter server. A plug-in with the key `com.solidfire` is already installed.

Corrective Action

In the registration utility, use **Update Plug-in** instead of **Register Plug-in**.

Error updating plug-in using Registration UI

Description

When using the registration utility, there is an error updating the plug-in against the vCenter server. A plug-in with the key `com.solidfire` is not installed for the update.

Corrective Action

In the registration utility, use **Register Plug-in** instead of **Update Plug-in**.

Error message that NetApp extension cannot be upgraded

Message

```
org.springframework.transaction.CannotCreateTransactionException: Could not open JPA EntityManager for transaction; nested exception is javax.persistence.PersistenceException: org.hibernate.exception.GenericJDBCException: Could not open connection.
```

Description

During a Windows vCenter Server upgrade from version 6.0 to 6.5, you see a warning that the NetApp Extension cannot be upgraded or may not work with the new vCenter Server. After you complete the upgrade and log in to the vSphere Web Client, the error occurs when you select a vCenter Plug-in extension point. This error occurs because the directory that stores the runtime database has changed from version 6.0 to 6.5. The vCenter Plug-in is unable to create the needed files for runtime.

Corrective Action

1. Unregister the plug-in.
2. Remove plug-in files.
3. Reboot the vCenter.
4. Register the plug-in.
5. Log in to the vSphere Web Client.

Removing plug-in completes successfully but icons remain

Description

Removing vCenter Plug-in package files completed successfully, but plug-in icons are still visible in the vSphere Web Client.

Corrective Action

Log out of the vSphere Web Client and log in again. Closing and re-opening your browser might be required. If logging out of vSphere Web Client does not resolve the issue, it might be necessary to reboot the vCenter server web services. Additionally, other users might have existing sessions. All user sessions must be closed.

Plug-in cannot be unregistered or removed after admin password change

Description

After the admin password for the vCenter that was used to register the plug-in is changed, the vCenter Plug-in cannot be unregistered or removed.

Corrective Action

For plug-in 2.6, go to the vCenter Plug-in **Register/Unregister** page. Click the **Update** button to change the vCenter IP address, user ID, and password.

For plug-in 2.7 or later, update the vCenter Administrator password in mNode Settings in the plug-in.

For plug-in 4.4 or later, update the vCenter Administrator password in QoSSIIOC Settings in the plug-in.

Plug-in management tasks fail or volumes are not accessible to ESXi host

Description

Create, clone, and share datastore tasks fail or volumes are not accessible by the ESXi host.

Corrective Action

- Check that the software iSCSI HBA is present and enabled on the ESXi host for datastore operations.
- Check that the volume is not deleted or assigned to an incorrect volume access group.
- Check that the volume access group has the correct host IQN.
- Check that the associated account has the correct CHAP settings.
- Check that volume status is active, volume access is `readWrite`, and `512e` is set to true.

Failure occurs during vCenter Plug-in use on Firefox 59.0.2 browsers

Message

Name:HttpResponse Raw Message:Http failure response for <https://vc6/ui/solidfire-war-4.2.0-SNAPSHOT/rest/vsphere//servers>: 500 Internal Server Error
Return Message:Server error. Please try again or contact NetApp support

Description

This issue occurs in vSphere HTML5 web clients using Firefox. The vSphere Flash client is not affected.

Corrective Action

Use the full FQDN in the browser URL. VMware requires full forward and reverse resolution of IP, short name, and FQDN.

Delete datastore operation fails

Description

A delete datastore operation fails.

Corrective Action

Check that all VMs have been deleted from the datastore. You must delete VMs from a datastore before the datastore can be deleted.

Cluster pair cannot connect using a pairing key

Description

A connection error occurs during cluster pairing using a pairing key. The error message in the **Create Cluster Pairing** dialog box indicates that there is no route to host.

Corrective Action

Manually delete the unconfigured cluster pair the process created on the local cluster and perform the cluster pairing again.

Error message for QoSSIOC status

Description

QoSSIOC status for the plug-in displays a warning icon and error message.

Corrective Action

- **Unable to reach IP address:** The IP address is invalid or no responses are received. Verify that the address is correct and that the management node is online and available.
- **Unable to communicate:** The IP address can be reached but calls to the address fail. This might indicate that the QoSSIOC service is not running at the specified address or a firewall might be blocking traffic.
- **Unable to connect to the SIOC service:** Open `sioc.log` in `/opt/solidfire/sioc/data/logs/` on the management node (`/var/log` or `/var/log/solidfire/` on older management nodes) to verify that the SIOC service started successfully. SIOC service startup can take 50 seconds or more. If the service did not start successfully, try again.

QoSSIOC service shown as available but is unavailable

Description

QoSSIOC service settings displays as UP, but QoSSIOC is unavailable.

Corrective Action for Element vCenter plug-in 5.0 or later

From the **QoSSIOC Settings** tab in the NetApp Element Remote Plugin > Configuration tab, select the refresh button. Update the IP address or user authentication information as needed.

Corrective Action for Element vCenter plug-in 4.10 or earlier

From the **QoSSIOC Settings** tab in the NetApp Element Configuration extension point, select the refresh button. Update the IP address or user authentication information as needed.

QoSSIOC is enabled for datastore but unavailable

Description

QoSSIOC is enabled for a datastore, but QoSSIOC is unavailable.

Corrective Action

Check that the VMware SIOC is enabled on the datastore:

1. Open `sioc.log` in `/opt/solidfire/sioc/data/logs/` on the management node (`/var/log` or `/var/log/solidfire/` on older management nodes).
2. Search for this text:

```
SIOC is not enabled
```

3. See [this article](#) for the corrective action specific to your issue.

Earlier versions of NetApp Element Plug-in for VMware vCenter Server documentation

Documentation is also available for releases earlier than version 5.2 of the NetApp Element Plug-in for VMware vCenter Server.



This [documentation link](#) for Element vCenter plug-in 5.2 also includes versions 5.1, 5.0, 4.10, 4.9, 4.8, 4.7, and 4.6.

Version	Plug-in release notes	Management services release notes	User guide
5.1	PDF	2.23.64	Link
5.0	PDF	2.22.7	Link
4.10	PDF	2.21.61	Link
4.9	PDF	2.20.69	Link
4.8	PDF	2.19.48	Link
4.7	PDF	2.18.91	Link
4.6	PDF	2.17.56 KB	Link
4.5	PDF	2.14.60 KB	PDF
4.4	PDF	2.11.34 KB	PDF
4.3	PDF	2.0.725 KB	PDF NOTE: This publication describes updated management node upgrade procedures for Element software 11.3/NetApp HCI 1.6. PDF NOTE: This publication describes updated management node upgrade procedures for Element software 11.5/NetApp HCI 1.7 PDF NOTE: This publication describes updated management node upgrade procedures for Element software 11.7/NetApp HCI 1.7P1

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

<https://www.netapp.com/company/legal/copyright/>

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- [Notice for Management Services 2.24.40 \(NetApp Element Plug-in for VMware vCenter Server 5.2.12\)](#)
- [Notice for Management Services 2.23.64 \(NetApp Element Plug-in for VMware vCenter Server 5.1.12\)](#)
- [Notice for Management Services 2.22.7 \(NetApp Element Plug-in for VMware vCenter Server 5.0.37\)](#)
- [Notice for Management Services 2.21.61 \(NetApp Element Plug-in for VMware vCenter Server 4.10.12\)](#)
- [Notice for Management Services 2.20.69 \(NetApp Element Plug-in for VMware vCenter Server 4.9.14\)](#)
- [Notice for Management Services 2.19.48 \(NetApp Element Plug-in for VMware vCenter Server 4.8.34\)](#)
- [Notice for Management Services 2.18.91 \(NetApp Element Plug-in for VMware vCenter Server 4.7.10\)](#)
- [Notice for Management Services 2.17.56 \(NetApp Element Plug-in for VMware vCenter Server 4.6.32\)](#)
- [Notice for Management Services 2.17.52 \(NetApp Element Plug-in for VMware vCenter Server 4.6.29\)](#)
- [Notice for Management Services 2.16 \(NetApp Element Plug-in for VMware vCenter Server 4.6.29\)](#)
- [Notice for Management Services 2.14 \(NetApp Element Plug-in for VMware vCenter Server 4.5.42\)](#)
- [Notice for Management Services 2.13 \(NetApp Element Plug-in for VMware vCenter Server 4.5.42\)](#)
- [Notice for Management Services 2.11 \(NetApp Element Plug-in for VMware vCenter Server 4.4.72\)](#)

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.