Manage volumes and virtual volumes

Element Software

NetApp
June 10, 2024

Table of Contents

Manage volumes and virtual volumes

You can manage the data in a cluster running Element software from the Management tab in the Element UI. Available cluster management functions include creating and managing data volumes, volume access groups, initiators, and Quality of Service (QoS) policies.

- Work with volumes
- Work with virtual volumes
- Work with volume access groups and initiators

For more information

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

Work with volumes

The SolidFire system provisions storage using volumes. Volumes are block devices accessed over the network by iSCSI or Fibre Channel clients. From the Volumes page on the Management tab, you can create, modify, clone, and delete volumes on a node. You can also view statistics about volume bandwidth and I/O usage.

Find more information

- Manage Quality of Service policies
- Create a volume
- View individual volume performance details
- Edit active volumes
- Delete a volume
- Restore a deleted volume
- Purge a volume
- Clone a volume
- Assign LUNs to Fibre Channel volumes
- Apply a QoS policy to volumes
- Remove the QoS policy association of a volume

Manage Quality of Service policies

A Quality of Service (QoS) policy enables you to create and save a standardized quality of service setting that can be applied to many volumes. You can create, edit, and delete QoS policies from the QoS Policies page on the Management tab.

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

NetApp video: SolidFire Quality of Service Policies

See Performance and quality of service.

- Create a QoS policy
- Edit a QoS policy
- Delete a QoS policy

Create a QoS policy

You can create QoS policies and apply them when creating volumes.

1. Select **Management** > **QoS Policies**.
2. Click **Create QoS Policy**.
3. Enter the **Policy Name**.
4. Enter the**Min IOPS**, **Max IOPS**, and **Burst IOPS** values.
5. Click **Create QoS Policy**.

Edit a QoS policy

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

1. Select **Management** > **QoS Policies**.
2. Click the Actions icon for the QoS policy you want to edit.
3. In the resulting menu, select**Edit**.
4. In the **Edit QoS Policy** dialog box, modify the following properties as required:
    - Policy Name
    - Min IOPS
    - Max IOPS
    - Burst IOPS
5. Click **Save Changes**.

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 settings but become unassociated with a policy.

If you are trying instead to disassociate a volume from a QoS policy, you can change the QoS settings for that volume to custom.

1. Select **Management** > **QoS Policies**.
2. Click the Actions icon for the QoS policy you want to delete.

3. In the resulting menu, select **Delete**.
4. Confirm the action.

Find more information

- Remove the QoS policy association of a volume
- SolidFire and Element Software Documentation
- NetApp Element Plug-in for vCenter Server

Manage volumes

The SolidFire system provisions storage using volumes. Volumes are block devices accessed over the network by iSCSI or Fibre Channel clients.

From the Volumes page on the Management tab, you can create, modify, clone, and delete volumes on a node.

Create a volume

You can create a 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 specify QoS settings for a volume during creation.

1. Select **Management** > **Volumes**.
2. Click **Create Volume**.
3. In the **Create a New Volume** dialog box, enter the **Volume Name**.
4. Enter the total size of the volume.

   The default volume size selection is in GB. You can create volumes using sizes measured in GB or GiB:

   - 1GB = 1 000 000 000 bytes
   - 1GiB = 1 073 741 824 bytes
5. Select a **Block Size** for the volume.
6. Click the **Account** drop-down list and select the account that should have access to the volume.

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

   If there are more than 50 accounts, the list does not appear. Begin typing and the auto-complete function displays possible values for you to choose.
7. To set the **Quality of Service**, do one of the following:
   a. Under **Policy**, you can select an existing QoS policy, if available.
   b. Under **Custom Settings**, set customized minimum, maximum, and burst values for IOPS or use the default QoS values.

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

8. Click **Create Volume**.

View volume details

1. Select **Management** > **Volumes**.
2. Review the details.
   - **ID**: The system-generated ID for the volume.
   - **Name**: The name given to 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.
   - **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 allowed.
     - ReplicationTarget: Designated as a target volume in a replicated volume pair.
   - **Used**: The percentage of used space in the volume.
   - **Size**: The total size (in GB) of the volume.
   - **Snapshots**: The number of snapshots created for the volume.
   - **QoS Policy**: The name and link to the user-defined 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.
   - **Attributes**: Attributes that have been assigned to the volume as a key/value pair through an API method.
   - **512e**: Indication of whether 512e is enabled on a volume. Possible values:
     - Yes
     - No
   - **Created On**: The date and time that the volume was created.

View individual volume details

You can view performance statistics for individual volumes.

1. Select **Reporting** > **Volume Performance**.
2. In the volume list, click the Actions icon for a volume.
3. Click **View Details**.

   A tray appears at the bottom of the page containing general information about the volume.

4. To see more detailed information about the volume, click **See More Details**.

   The system displays detailed information as well as performance graphs for the volume.

Edit active volumes

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

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

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

Steps

1. Select **Management** > **Volumes**.
2. In the **Active** window, click the Actions icon for the volume you want to edit.
3. Click **Edit**.
4. **Optional:** Change the total size of the volume.

   - You can increase, but not decrease, the size of the volume. You can only resize one volume in a single resizing operation. Garbage collection operations and software upgrades do not interrupt the resizing operation.
   - If you are adjusting volume size for replication, 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.

   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
5. **Optional:** Select a different account access level of one of the following:
   - Read Only
   - Read/Write
   - Locked
   - Replication Target
6. **Optional:** Select the account that should have access to the volume.

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

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

7. **Optional:** To change the selection in **Quality of Service**, do one of the following:
   a. Under **Policy**, you can select an existing QoS policy, if available.
   b. Under **Custom Settings**, set customized minimum, maximum, and burst values for IOPS or use the default QoS values.

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

   When you change IOPS values, you should increment in tens or hundreds. Input values require valid whole numbers.

   Configure volumes with an extremely high burst value. This allows the system to process occasional large block sequential workloads more quickly, while still constraining the sustained IOPS for a volume.

8. Click **Save Changes**.

Delete a volume

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

The system does not immediately purge a deleted volume; the volume remains available for approximately eight hours. If you restore a volume before the system purges it, the volume comes back online and iSCSI connections are restored.

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

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

Steps

1. Select **Management** > **Volumes**.
2. To delete a single volume, perform the following steps:
   a. Click the Actions icon for the volume you want to delete.
   b. In the resulting menu, click **Delete**.
   c. Confirm the action.

   The system moves the volume to the **Deleted** area on the **Volumes** page.
3. To delete multiple volumes, perform the following steps:
   a. In the list of volumes, check the box next to any volumes you want to delete.
   b. Click **Bulk Actions**.
   c. In the resulting menu, click **Delete**.
   d. Confirm the action.

The system moves the volumes to the **Deleted** area on the **Volumes** page.

Restore a deleted volume

You can restore a volume in the 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.

1. Select **Management** > **Volumes**.
2. Click the **Deleted** tab to view the list of deleted volumes.
3. Click the Actions icon for the volume you want to restore.
4. In the resulting menu, click **Restore**.
5. Confirm the action.

   The volume is placed in the **Active** volumes list and iSCSI connections to the volume are restored.

Purge a volume

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

The system automatically purges deleted volumes eight hours after deletion. However, if you want to purge a volume before the scheduled time, you can do so.

1. Select **Management** > **Volumes**.
2. Click the **Deleted** button.
3. Perform the steps to purge a single volume or multiple volumes.

Option	Steps
Purge a single volume	a. Click the Actions icon for the volume you want to purge. b. Click **Purge**. c. Confirm the action.
Purge multiple volumes	a. Select the volumes you want to purge. b. Click **Bulk Actions**. c. In the resulting menu, select **Purge**. d. Confirm the action.

Clone a volume

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

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

Operating systems differ in how they treat cloned volumes. VMware 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 on mounting a VMFS datastore copy and managing duplicate VMFS datastores.

Before you truncate a cloned volume by cloning to a smaller size, ensure that you prepare the partitions so that they fit into the smaller volume.

Steps

1. Select **Management** > **Volumes**.
2. To clone a single volume, perform the following steps:
   a. In the list of volumes on the **Active** page, click the Actions icon for the volume you want to clone.
   b. In the resulting menu, click **Clone**.
   c. In the **Clone Volume** window, enter a volume name for the newly cloned volume.
   d. Select a size and measurement for the volume using the **Volume Size** spin box and list.

      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

   e. Select the type of access for the newly cloned volume.
   f. Select an account to associate with the newly cloned volume from the **Account** list.

      You can create an account during this step if you click the **Create Account** link, enter an account name, and click **Create**. The system automatically adds the account to the **Account** list after you create it.

3. To clone multiple volumes, perform the following steps:
   a. In the list of volumes on the **Active** page, check the box next to any volumes you want to clone.
   b. Click **Bulk Actions**.
   c. In the resulting menu, select **Clone**.
   d. In the **Clone Multiple Volumes** dialog box, enter a prefix for the cloned volumes in the **New Volume Name Prefix** field.
   e. Select an account to associate with the cloned volumes from the **Account** list.
   f. Select the type of access for the cloned volumes.
4. Click **Start Cloning**.

   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 might need to extend partitions or create new partitions in the free space to make use of it.

For more information

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

Assign LUNs to Fibre Channel volumes

You can change the LUN assignment for a Fibre Channel volume in a volume access group. You can also make Fibre Channel volume LUN assignments when you create a volume access group.

Assigning new Fibre Channel LUNs is an advanced function and could have unknown consequences on the connecting host. For example, the new LUN ID might not be automatically discovered on the host, and the host might require a rescan to discover the new LUN ID.

1. Select **Management** > **Access Groups**.
2. Click the Actions icon for the access group you want to edit.
3. In the resulting menu, select**Edit**.
4. Under **Assign LUN IDs** in the **Edit Volume Access Group** dialog box, click the arrow on the **LUN Assignments** list.
5. For each volume in the list that you want to assign a LUN to, enter a new value in the corresponding **LUN** field.
6. Click **Save Changes**.

Apply a QoS policy to volumes

You can bulk apply an existing QoS policy to one or more volumes.

The QoS policy you want to bulk apply must exist.

1. Select **Management** > **Volumes**.
2. In the list of volumes, check the box next to any volumes you want to apply the QoS policy to.
3. Click **Bulk Actions**.
4. In the resulting menu, click **Apply QoS Policy**.
5. Select the QoS policy from the drop-down list.
6. Click **Apply**.

Find more information

Quality of Service policies

Remove the QoS policy association of a volume

You can remove a QoS policy association from a volume by selecting custom QoS settings.

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

1. Select **Management** > **Volumes**.
2. Click the Actions icon for a volume that contains a QoS policy you want to modify.
3. Click **Edit**.
4. In the resulting menu under **Quality of Service**, click **Custom Settings**.
5. Modify **Min IOPS**, **Max IOPS**, and **Burst IOPS**, or keep the default settings.
6. Click **Save Changes**.

Find more information

Delete a QoS policy

Work with virtual volumes

You can view information and perform tasks for virtual volumes and their associated storage containers, protocol endpoints, bindings, and hosts using the Element UI.

The NetApp Element software storage system ships with the Virtual Volumes (VVols) feature disabled. You must perform a one-time task of manually enabling vSphere VVol functionality through the Element UI.

After you enable the VVol functionality, a VVols tab appears in the user interface that offers VVols-related monitoring and limited management options. Additionally, a storage-side software component known as the VASA Provider acts as a storage awareness service for vSphere. Most VVols commands, such as VVol creation, cloning, and editing, are initiated by a vCenter Server or ESXi host and translated by the VASA Provider to Element APIs for the Element software storage system. Commands to create, delete, and manage storage containers and delete virtual volumes can be initiated using the Element UI.

The majority of configurations necessary for using Virtual Volumes functionality with Element software storage systems are made in vSphere. See the *VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide* to register the VASA Provider in vCenter, create and manage VVol datastores, and manage storage based on policies.

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 multiple vCenters is available as an upgrade patch if you have already registered a VASA provider with your vCenter. To install, download the VASA39 .tar.gz file from the NetApp Software Downloads site and follow the directions in the manifest. 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

- Enable virtual volumes
- View virtual volume details
- Delete a virtual volume
- Create a storage container

- Edit a storage container
- Delete a storage container
- Protocol endpoints
- Bindings
- Host details

Enable virtual volumes

You must manually enable vSphere Virtual Volumes (VVols) functionality through the NetApp Element software. The Element software 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.

What you'll need

- The cluster must be running Element 9.0 or later.
- The cluster must be connected to an ESXi 6.0 or later environment that is compatible with VVols.
- If you are using Element 11.3 or later, the cluster must be connected to an ESXi 6.0 update 3 or later environment.

> Enabling vSphere Virtual Volumes functionality permanently changes the Element software configuration. You should only enable VVols functionality if your cluster is connected to a VMware ESXi VVols-compatible environment. You can disable the VVols feature and restore the default settings only by returning the cluster to the factory image, which deletes all data on the system.

Steps

1. Select **Clusters** > **Settings**.
2. Find the cluster-specific settings for Virtual Volumes.
3. Click **Enable Virtual Volumes**.
4. Click **Yes** to confirm the Virtual Volumes configuration change.

   The **VVols** tab appears in the Element UI.

   > When VVols functionality is enabled, the SolidFire 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.

5. Copy the VASA Provider URL from the Virtual Volumes (VVols) settings in **Clusters** > **Settings**. You will use this URL to register the VASA Provider in vCenter.
6. Create a storage container in **VVols** > **Storage Containers**.

   > You must create at least one storage container so that VMs can be provisioned to a VVol datastore.

7. Select **VVols** > **Protocol Endpoints**.
8. Verify that a protocol endpoint has been created for each node in the cluster.

Additional configuration tasks are required in vSphere. See the *VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide* to register the VASA Provider in vCenter, create and manage VVol datastores, and manage storage based on policies.

Find more information

VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide

View virtual volume details

You can review virtual volume information for all active virtual volumes on the cluster in the Element UI. You can also view performance activity for each virtual volume, including input, output, throughput, latency, queue depth, and volume information.

What you'll need

- You should have enabled VVols functionality in the Element UI for the cluster.
- You should have created an associated storage container.
- You should have configured your vSphere cluster to use Element software VVols functionality.
- You should have created at least one VM in vSphere.

Steps

1. Click **VVols** > **Virtual Volumes**.

   The information for all active virtual volumes is displayed.

2. Click the **Actions** icon for the virtual volume you want to review.
3. In the resulting menu, select **View Details**.

Details

The Virtual Volumes page of the VVols tab provides information about each active virtual volume on the cluster, such as volume ID, snapshot ID, parent virtual volume ID, and virtual volume ID.

- **Volume ID**: The ID of the underlying volume.
- **Snapshot ID**: The ID of the underlying volume snapshot. The value is 0 if the virtual volume does not represent a SolidFire snapshot.
- **Parent Virtual Volume ID**: The virtual volume ID of the parent virtual volume. If the ID is all zeros, the virtual volume is independent with no link to a parent.
- **Virtual Volume ID**: The UUID of the virtual volume.
- **Name**: The name assigned to the virtual volume.
- **Storage Container**: The storage container that owns the virtual volume.
- **Guest OS Type**: Operating system associated with the virtual volume.
- **Virtual Volume Type**: The virtual volume type: Config, Data, Memory, Swap, or Other.
- **Access**: The read-write permissions assigned to the virtual volume.
- **Size**: The size of the virtual volume in GB or GiB.

- **Snapshots**: The number of associated snapshots. Click the number to link to snapshot details.
- **Min IOPS**: The minimum IOPS QoS setting of the virtual volume.
- **Max IOPS**: The maximum IOPS QoS setting of the virtual volume.
- **Burst IOPS**: The maximum burst QoS setting of the virtual volume.
- **VMW_VmID**: Information in fields prefaced with "VMW_" are defined by VMware.
- **Create Time**: The time the virtual volume creation task was completed.

Individual virtual volume details

The Virtual Volumes page on the VVols tab provides the following virtual volume information when you select an individual virtual volume and view its details.

- **VMW_XXX**: Information in fields prefaced with "VMW_" are defined by VMware.
- **Parent Virtual Volume ID**: The virtual volume ID of the parent virtual volume. If the ID is all zeros, the virtual volume is independent with no link to a parent.
- **Virtual Volume ID**: The UUID of the virtual volume.
- **Virtual Volume Type**: The virtual volume type: Config, Data, Memory, Swap, or Other.
- **Volume ID**: The ID of the underlying volume.
- **Access**: The read-write permissions assigned to the virtual volume.
- **Account Name**: Name of the account containing the volume.
- **Access Groups**: Associated volume access groups.
- **Total Volume Size**: Total provisioned capacity in bytes.
- **Non-Zero Blocks**: Total number of 4KiB blocks with data after the last garbage collection operation has completed.
- **Zero Blocks**: Total number of 4KiB blocks without data after the last round of garbage collection operation has completed.
- **Snapshots**: The number of associated snapshots. Click the number to link to snapshot details.
- **Min IOPS**: The minimum IOPS QoS setting of the virtual volume.
- **Max IOPS**: The maximum IOPS QoS setting of the virtual volume.
- **Burst IOPS**: The maximum burst QoS setting of the virtual volume.
- **Enable 512**: Because virtual volumes always use 512-byte block size emulation, the value is always yes.
- **Volumes Paired**: Indicates if a volume is paired.
- **Create Time**: The time the virtual volume creation task was completed.
- **Blocks Size**: Size of the blocks on the volume.
- **Unaligned Writes**: For 512e volumes, the number of write operations that were not on a 4k sector boundary. High numbers of unaligned writes might indicate improper partition alignment.
- **Unaligned Reads**: For 512e volumes, the number of read operations that were not on a 4k sector boundary. High numbers of unaligned reads might indicate improper partition alignment.
- **scsiEUIDeviceID**: Globally unique SCSI device identifier for the volume in EUI-64 based 16-byte format.
- **scsiNAADeviceID**: Globally unique SCSI device identifier for the volume in NAA IEEE Registered Extended format.

- **Attributes**: List of name-value pairs in JSON object format.

Delete a virtual volume

Although virtual volumes should always be deleted from the VMware Management Layer, the functionality for you to delete virtual volumes is enabled from the Element UI. You should only delete a virtual volume from the Element UI when absolutely necessary, such as when vSphere fails to clean up virtual volumes on SolidFire storage.

1. Select **VVols** > **Virtual Volumes**.
2. Click the Actions icon for the virtual volume you want to delete.
3. In the resulting menu, select **Delete**.

> You should delete a virtual volume from the VMware Management Layer to ensure that the virtual volume is properly unbound before deletion. You should only delete a virtual volume from the Element UI when absolutely necessary, such as when vSphere fails to clean up virtual volumes on SolidFire storage. If you delete a virtual volume from the Element UI, the volume will be purged immediately.

4. Confirm the action.
5. Refresh the list of virtual volumes to confirm that the virtual volume has been removed.
6. **Optional**: Select **Reporting** > **Event Log** to confirm that the purge has been successful.

Manage storage containers

A storage container is a vSphere datastore representation created on a cluster running Element software.

Storage containers are created and tied to NetApp Element accounts. A storage container created on Element storage appears as a vSphere datastore in vCenter and ESXi. Storage containers do not allocate any space on Element storage. They are simply used to logically associate virtual volumes.

A maximum of four storage containers per cluster is supported. A minimum of one storage container is required to enable VVols functionality.

Create a storage container

You can create storage containers in the Element UI and discover them in vCenter. You must create at least one storage container to begin provisioning VVol-backed virtual machines.

Before you begin, enable VVols functionality in the Element UI for the cluster.

Steps

1. Select **VVols** > **Storage Containers**.
2. Click the **Create Storage Containers** button.
3. Enter storage container information in the **Create a New Storage Container** dialog box:
   a. Enter a name for the storage container.
   b. Configure initiator and target secrets for CHAP.

Leave the CHAP Settings fields blank to automatically generate secrets.

c. Click the **Create Storage Container** button.

4. 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.

View storage container details

On the Storage Containers page of the VVols tab, you can view information for all active storage containers on the cluster.

- **Account ID**: The ID of the Netapp Element account associated with the storage container.
- **Name**: The name of the storage container.
- **Status**: The status of the storage container. Possible values:
  - Active: The storage container is in use.
  - Locked: The storage container is locked.
- **PE Type**: The protocol endpoint type (SCSI is the only available protocol for Element software).
- **Storage Container ID**: The UUID of the virtual volume storage container.
- **Active Virtual Volumes**: The number of active virtual volumes associated with the storage container.

View individual storage container details

You can view the storage container information for an individual storage container by selecting it from the Storage Containers page on the VVols tab.

- **Account ID**: The ID of the NetApp Element account associated with the storage container.
- **Name**: The name of the storage container.
- **Status**: The status of the storage container. Possible values:
  - Active: The storage container is in use.
  - Locked: The storage container is locked.
- **Chap Initiator Secret**: The unique CHAP secret for the initiator.
- **Chap Target Secret**: The unique CHAP secret for the target.
- **Storage Container ID**: The UUID of the virtual volume storage container.
- **Protocol Endpoint Type**: Indicates the protocol endpoint type (SCSI is the only available protocol).

Edit a storage container

You can modify storage container CHAP authentication in the Element UI.

1. Select **VVols** > **Storage Containers**.
2. Click the **Actions** icon for the storage container you want to edit.
3. In the resulting menu, select **Edit**.

4. Under CHAP Settings, edit the Initiator Secret and Target Secret credentials used for authentication.

   If you do not change the CHAP Settings credentials, they remain the same. If you make the credentials fields blank, the system automatically generates new secrets.

5. Click **Save Changes**.

Delete a storage container

You can delete storage containers from the Element UI.

What you'll need

Ensure that all virtual machines have been removed from the VVol datastore.

Steps

1. Select **VVols** > **Storage Containers**.
2. Click the **Actions** icon for the storage container you want to delete.
3. In the resulting menu, select **Delete**.
4. Confirm the action.
5. Refresh the list of storage containers in the **Storage Containers** sub-tab to confirm that the storage container has been removed.

Protocol endpoints

Protocol endpoints are access points used by a host to address storage on a cluster running NetApp Element software. 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.

A cluster running Element software automatically creates one protocol endpoint per storage node in the cluster. For example, a six-node storage cluster has six protocol endpoints that are mapped to each ESXi host. Protocol endpoints are dynamically managed by Element software and are created, moved, or removed as needed without any intervention. Protocol endpoints are the target for multi-pathing and act as an I/O proxy for subsidiary LUNs. Each protocol endpoint consumes an available SCSI address, just like a standard iSCSI target. Protocol endpoints appear as a single-block (512-byte) storage device in the vSphere client, but this storage device is not available to be formatted or used as storage.

iSCSI is the only supported protocol. Fibre Channel protocol is not supported.

Protocol endpoints details

The Protocol Endpoints page on the VVols tab provides protocol endpoint information.

- **Primary Provider ID**

  The ID of the primary protocol endpoint provider.

- **Secondary Provider ID**

  The ID of the secondary protocol endpoint provider.

- **Protocol Endpoint ID**

  The UUID of the protocol endpoint.

- **Protocol Endpoint State**

  The status of the protocol endpoint. Possible values are as follows:

  - Active: The protocol endpoint is in use.
  - Start: The protocol endpoint is starting.
  - Failover: The protocol endpoint has failed over.
  - Reserved: The protocol endpoint is reserved.

- **Provider Type**

  The type of the protocol endpoint's provider. Possible values are as follows:

  - Primary
  - Secondary

- **SCSI NAA Device ID**

  The globally unique SCSI device identifier for the protocol endpoint in NAA IEEE Registered Extended Format.

Bindings

To perform I/O operations with a virtual volume, an ESXi host must first bind the virtual volume.

The SolidFire 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.

Bindings details

The Bindings page on the VVols tab provides binding information about each virtual volume.

The following information is displayed:

- **Host ID**

  The UUID for the ESXi host that hosts virtual volumes and is known to the cluster.

- **Protocol Endpoint ID**

  Protocol endpoint IDs that correspond to each node in the SolidFire cluster.

- **Protocol Endpoint in Band ID**

  The SCSI NAA device ID of the protocol endpoint.

- **Protocol Endpoint Type**

  The protocol endpoint type.

- **VVol Binding ID**

  The binding UUID of the virtual volume.

- **VVol ID**

  The universally unique identifier (UUID) of the virtual volume.

- **VVol Secondary ID**

  The secondary ID of the virtual volume that is a SCSI second level LUN ID.

Host details

The Hosts page on the VVols tab provides information about VMware ESXi hosts that host virtual volumes.

The following information is displayed:

- **Host ID**

  The UUID for the ESXi host that hosts virtual volumes and is known to the cluster.

- **Host Address**

  The IP address or DNS name for the ESXi host.

- **Bindings**

  Binding IDs for all virtual volumes bound by the ESXi host.

- **ESX Cluster ID**

  The vSphere host cluster ID or vCenter GUID.

- **Initiator IQNs**

  Initiator IQNs for the virtual volume host.

- **SolidFire Protocol Endpoint IDs**

  The protocol endpoints that are currently visible to the ESXi host.

Work with volume access groups and initiators

You can use iSCSI initiators or Fibre Channel initiators to access the volumes defined within volume access groups.

You can create access groups by mapping iSCSI initiator IQNs or Fibre Channel 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.

There are two types of CHAP authentication methods:

- Account-level CHAP authentication: You can assign CHAP authentication for the account.
- Initiator-level CHAP authentication: You can assign unique CHAP target and secrets for specific initiators without being bound to single CHAP across a single account. This Initiator-level CHAP authentication replaces account level credentials.

Optionally, with per-initiator CHAP, you can enforce initiator authorization and per-initiator CHAP authentication. These options can be defined on a per-initiator basis and an access group can contain a mix of initiators with different options.

Each WWPN that you add to an access group enables Fibre Channel network access to the volumes in the access group.

Volume access groups have the following limits:

- A maximum of 64 IQNs or WWPNs are allowed in an access group.
- An access group can be made up of a maximum of 2000 volumes.
- An IQN or WWPN can belong to only one access group.
- A single volume can belong to a maximum of four access groups.

Find more information

- Create a volume access group
- Add volumes to an access group
- Remove volumes from an access group
- Create an initiator
- Edit an initiator
- Add a single initiator to a volume access group
- Add multiple initiators to a volume access group
- Remove initiators from an access group
- Delete an access group
- Delete an initiator

Create a volume access group

You can create volume access groups by mapping initiators to a collection of volumes for secured access. You can then grant access to the volumes in the group with an account CHAP initiator secret and target secret.

If you use initiator-based CHAP, you can add CHAP credentials for a single initiator in a volume access group, providing more security. This enables you to apply this option for volume access groups that already exist.

Steps

1. Click **Management** > **Access Groups**.
2. Click **Create Access Group**.
3. Enter a name for the volume access group in the **Name** field.
4. Add an initiator to the volume access group in one of the following ways:

Option	Description
Adding a Fibre Channel initiator	a. Under Add Initiators, select an existing Fibre Channel initiator from the Unbound Fibre Channel Initiators list. b. Click **Add FC Initiator**.  You can create an initiator during this step if you click the **Create Initiator** link, enter an initiator name, and click **Create**. The system automatically adds the initiator to the Initiators list after you create it. A sample of the format is as follows: `5f:47:ac:c0:5c:74:d4:02`
Adding an iSCSI initiator	Under Add Initiators, select an existing initiator from the Initiators list. **Note:** You can create an initiator during this step if you click the **Create Initiator** link, enter an initiator name, and click **Create**. The system automatically adds the initiator to the Initiators list after you create it. A sample of the format is as follows: `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b`  You can find the initiator IQN for each volume by selecting **View Details** in the Actions menu for the volume on the **Management** > **Volumes** > **Active** list. When you modify an initiator, you can toggle the requiredCHAP attribute to True, which enables you to set the target initiator secret. For details, see API information about the ModifyInitiator API method. Manage storage with the Element API

5. **Optional:** Add more initiators as needed.
6. Under Add Volumes, select a volume from the **Volumes** list.

   The volume appears in the **Attached Volumes** list.
7. **Optional:** Add more volumes as needed.

8. Click **Create Access Group**.

Find more information

Add volumes to an access group

View individual access group details

You can view details for an individual access group, such as attached volumes and initiators, in a graphical format.

1. Click **Management** > **Access Groups**.
2. Click the Actions icon for an access group.
3. Click **View Details**.

Volume access group details

The Access Groups page on the Management tab provides information about volume access groups.

The following information is displayed:

- **ID**: The system-generated ID for the access group.
- **Name**: The name given to the access group when it was created.
- **Active Volumes**: The number of active volumes in the access group.
- **Compression**: The compression efficiency score for the access group.
- **Deduplication**: The deduplication efficiency score for the access group.
- **Thin Provisioning**: The thin provisioning efficiency score for the access group.
- **Overall Efficiency**: The overall efficiency score for the access group.
- **Initiators**: The number of initiators connected to the access group.

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 on the **Active** volumes page.

You can also use this procedure to add volumes to a Fibre Channel volume access group.

1. Click **Management** > **Access Groups**.
2. Click the Actions icon for the access group you want to add volumes to.
3. Click the **Edit** button.
4. Under Add Volumes, select a volume from the **Volumes** list.

   You can add more volumes by repeating this step.

5. Click **Save Changes**.

Remove volumes from an access group

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

Modifying CHAP settings in an account or removing initiators or volumes from an access group can cause initiators to lose access to volumes unexpectedly. To verify that volume access will not be lost unexpectedly, always logout iSCSI sessions that will be affected by an account or access group change, and verify that initiators can reconnect to volumes after any changes to initiator settings and cluster settings have been completed.

1. Click **Management** > **Access Groups**.
2. Click the Actions icon for the access group you want to remove volumes from.
3. Click **Edit**.
4. Under Add Volumes in the **Edit Volume Access Group** dialog box, click the arrow on the **Attached Volumes** list.
5. Select the volume you want to remove from the list and click the **x** icon to remove the volume from the list.

   You can remove more volumes by repeating this step.
6. Click **Save Changes**.

Create an initiator

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

You can also assign initator-based CHAP attributes by using an API call. To add a CHAP account name and credentials per initiator, you must use the `CreateInitiator` API call to remove and add CHAP access and attributes. Initiator access can be restricted to one or more VLANs by specifying one or more virtualNetworkIDs via the `CreateInitiators` and `ModifyInitiators` API calls. If no virtual networks are specified, the initiator can access all networks.

For details, see the API reference information. Manage storage with the Element API

Steps

1. Click **Management** > **Initiators**.
2. Click **Create Initiator**.
3. Perform the steps to create a single initiator or multiple initiators:

Option	Steps
Create a single initiator	a. Click **Create a Single Initiator**. b. Enter the IQN or WWPN for the initiator in the **IQN/WWPN** field. c. Enter a friendly name for the initiator in the **Alias** field. d. Click **Create Initiator**.

Option	Steps
Create multiple initiators	a. Click **Bulk Create Initiators**. b. Enter a list of IQNs or WWPNs in the text box. c. Click **Add Initiators**. d. Choose an initiator from the resulting list and click the corresponding Add icon in the **Alias** column to add an alias for the initiator. e. Click the check mark to confirm the new alias. f. Click **Create Initiators**.

Edit an initiator

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

To add a CHAP account name and credentials per initiator, you must use the `ModifyInitiator` API call to remove and add CHAP access and attributes.

See Manage storage with the Element API.

Steps

1. Click **Management** > **Initiators**.
2. Click the Actions icon for the initiator you want to edit.
3. Click **Edit**.
4. Enter a new alias for the initiator in the **Alias** field.
5. Click **Save Changes**.

Add a single initiator to a volume access group

You can add an initiator to an existing volume access group.

When you add an initiator to a volume access group, the initiator has access to all volumes in that volume access group.

You can find the initiator for each volume by clicking the Actions icon and then selecting **View Details** for the volume in the active volumes list.

If you use initiator-based CHAP, you can add CHAP credentials for a single initiator in a volume access group, providing more security. This enables you to apply this option for volume access groups that already exist.

Steps

1. Click **Management** > **Access Groups**.
2. Click the **Actions** icon for the access group you want to edit.
3. Click **Edit**.
4. To add a Fibre Channel initiator to the volume access group, perform the following steps:

a. Under Add Initiators, select an existing Fibre Channel initiator from the **Unbound Fibre Channel Initiators** list.

b. Click **Add FC Initiator**.

> You can create an initiator during this step if you click the **Create Initiator** link, enter an initiator name, and click **Create**. The system automatically adds the initiator to the **Initiators** list after you create it.

A sample of the format is as follows:

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

5. To add an iSCSI initiator to the volume access group, under Add Initiators, select an existing initiator from the **Initiators** list.

> You can create an initiator during this step if you click the **Create Initiator** link, enter an initiator name, and click **Create**. The system automatically adds the initiator to the **Initiators** list after you create it.

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

A sample of the format is as follows:

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

> You can find the initiator IQN for each volume from the **Management** > **Volumes** Active Volumes page by clicking the Actions icon and then selecting **View Details** for the volume.

6. Click **Save Changes**.

Add multiple initiators to a volume access group

You can add multiple initiators to an existing volume access group to allow access to volumes in the volume access group with or without requiring CHAP authentication..

When you add initiators to a volume access group, the initiators have access to all volumes in that volume access group.

> You can find the initiator for each volume by clicking the Actions icon and then **View Details** for the volume in the active volumes list.

You can add multiple initiators to an existing volume access group to enable access to volumes and assign unique CHAP credentials for each initiator within that volume access group. This enables you to apply this option for volume access groups that already exist.

You can assign initator-based CHAP attributes by using an API call. To add a CHAP account name and credentials per initiator, you must use the ModifyInitiator API call to remove and add CHAP access and

attributes.

For details, see Manage storage with the Element API.

Steps

1. Click **Management** > **Initiators**.
2. Select the initiators you want to add to an access group.
3. Click the **Bulk Actions** button.
4. Click **Add to Volume Access Group**.
5. In the Add to Volume Access Group dialog box, select an access group from the **Volume Access Group** list.
6. Click **Add**.

Remove initiators from an access group

When you remove an initiator from an access group, it can no longer access the volumes in that volume access group. Normal account access to the volume is not disrupted.

Modifying CHAP settings in an account or removing initiators or volumes from an access group can cause initiators to lose access to volumes unexpectedly. To verify that volume access will not be lost unexpectedly, always logout iSCSI sessions that will be affected by an account or access group change, and verify that initiators can reconnect to volumes after any changes to initiator settings and cluster settings have been completed.

Steps

1. Click **Management** > **Access Groups**.
2. Click the **Actions** icon for the access group you want to remove.
3. In the resulting menu, select **Edit**.
4. Under Add Initiators in the **Edit Volume Access Group** dialog box, click the arrow on the **Initiators** list.
5. Select the x icon for each initiator you want to remove from the access group.
6. Click **Save Changes**.

Delete an access group

You can delete an access group when it is no longer needed. You do not need to delete Initiator IDs and Volume IDs from the volume access group before deleting the group. After you delete the access group, group access to the volumes is discontinued.

1. Click **Management** > **Access Groups**.
2. Click the **Actions** icon for the access group you want to delete.
3. In the resulting menu, click **Delete**.
4. To also delete the initiators associated with this access group, select the **Delete initiators in this access group** check box.
5. Confirm the action.

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. Click **Management** > **Initiators**.
2. Perform the steps to delete a single initiator or multiple initiators:

Option	Steps
Delete single initiator	a. Click the **Actions** icon for the initiator you want to delete. b. Click **Delete**. c. Confirm the action.
Delete multiple initiators	a. Select the check boxes next to the initiators you want to delete. b. Click the **Bulk Actions** button. c. In the resulting menu, select **Delete**. d. Confirm the action.

Copyright information

Trademark information