Work with virtual volumes

Element Software

NetApp
June 11, 2021

Table of Contents

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.

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 NetAppElement 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.