Dell PowerStore

Virtualization Infrastructure Guide

Version 4.1

February 2025
Rev. A13

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Preface

As part of an improvement effort, revisions of the software and hardware are periodically released. Some functions that are described in this document are not supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features. Contact your service provider if a product does not function properly or does not function as described in this document.

NOTE: PowerStore X model customers: For the latest how-to technical manuals and guides for your model, download the *PowerStore 3.2.x Documentation Set* from the PowerStore Documentation page at dell.com/powerstoredocs.

Where to get help

Support, product, and licensing information can be obtained as follows:

- **Product information**—For product and feature documentation or release notes, go to the PowerStore Documentation page at dell.com/powerstoredocs.
- **Troubleshooting**—For information about products, software updates, licensing, and service go to Dell Support and locate the appropriate product support page.
- **Technical support**—For technical support and service requests, go to Dell Support and locate the **Service Requests** page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

1

Introduction

Topics:

Purpose

This document provides an overview of how virtualization is implemented on PowerStore clusters.

This document contains the following information:

- Hypervisor configuration for a PowerStore cluster
- How to manage virtualization components in PowerStore Manager
- How to add an external ESXi host to a PowerStore cluster in vCenter Server
- Best practices and limitations for using PowerStore with vCenter Server and vSphere

Audience

The information in this guide is primarily intended for:

- System administrators who are responsible for a wide range of technologies in their organization including basic storage management
- Storage administrators who manage the operations of storage infrastructure within their organization
- Virtualization administrators who deliver and maintain the virtual infrastructure for their organization

Users should have current practical experience with the following topics:

- Managing virtual machines and ESXi hypervisors with the VMware vSphere Client
- Accessing the ESXi Shell in order to use ESXCLI commands
- Using other VMware management interfaces such as PowerCLI

2

Overview of the PowerStore Virtualization Infrastructure

Topics:

PowerStore virtualization terminology

PowerStore clusters use a specific implementation of virtualization concepts that are based in a VMware vSphere framework.

PowerStore T and PowerStore Q clusters are integrated with the following VMware vSphere elements:

- vCenter Server
- Virtual machines (VMs)
- Virtual Volumes (vVols)
- VMFS datastores
- NFS datastores
- Protocol Endpoints
- VASA provider
- Storage containers
- Storage Policy Based Management

vCenter Server

A vCenter Server must be registered in PowerStore Manager to enable virtual machine (VM) discovery, monitoring, and snapshot management. When a vCenter Server is connected to a PowerStore cluster, PowerStore Manager can be used to monitor VM attributes, capacity, storage and compute performance, and virtual volumes.

On PowerStore T and PowerStore Q clusters, a connection to a vCenter Server is optional and can be set up during or after initial configuration.

Virtual machines

VMs that are stored on vVol datastores in a PowerStore cluster are automatically discovered and displayed in PowerStore Manager. The VMs displayed include VMs using external compute resources on ESXi hosts.

PowerStore clusters support NFS, VMFS, and vVol datastores. PowerStore clusters also support serving storage externally using Fibre Channel (FC), iSCSI, NVMe over Fibre Channel (NVMe/FC), and NVMe over TCP (NVMe/TCP) protocols. Support for the NVMe, FC, and iSCSI protocols enables VMs on external ESXi hosts to use the VMFS and vVols storage on PowerStore clusters.

NOTE: You must create unique host objects on PowerStore for vVols using the NVMe protocol. The PowerStore host object that is used for NVMe vVols cannot also be used for traditional datastores, volumes, or file systems using the NVMe protocol.

VMFS datastores

VMFS datastores are used as repositories for virtual machines that use block-based storage. VMFS is a special high-performance file system format that is optimized for storing virtual machines. You can store multiple virtual machines on the

same VMFS datastore. Each virtual machine is encapsulated in a set of files and occupies a single directory. In addition to virtual machines, VMFS datastores store other files such as virtual machine templates and ISO images.

NFS datastores

NFS datastores are used as repositories for virtual machines that use file-based storage. NFS datastores use the same structure as a 64-bit PowerStore file system. An NFS-enabled NAS server must have an associated file system and NFS export in order to be used for NFS datastores. ESXi hosts can access this designated NFS export on the NAS server and mount the datastore for file storage. File services including file system shrink and extend, replication, and snapshots are supported for VMware NFS datastores. You can store multiple virtual machines on the same NFS datastore. NFS datastores are managed on the **File Systems** page in PowerStore Manager. See the *PowerStore Configuring NFS Guide* for more information about creating and managing NFS datastores.

Virtual Volumes

Virtual Volumes (vVols) are an object type that corresponds to VM disks and snapshots. vVols are supported on a PowerStore cluster using the VASA protocol.

vVols are stored in storage containers that are known as vVols datastores. vVols datastores allow vVols to be mapped directly to a PowerStore cluster. A VM can consist of multiple vVols depending on its configuration and status. The different types of vVol objects are Data vVol, Config vVol, Memory vVol, and Swap vVol.

For more information, see Virtual Volumes overview.

Protocol Endpoints

Protocol Endpoints (PEs) are used as I/O access points from ESXi hosts to a PowerStore cluster. These endpoints establish a data path on-demand for virtual machines and their respective vVol datastores.

For more information, see Protocol Endpoints and vVols.

VASA provider

The vSphere APIs for Storage Awareness (VASA) provider is a software component that enables vSphere to determine the capabilities of a storage system. VASA enables the basic information about the storage system and storage resources on a PowerStore cluster to be made available to the vCenter Server. This information includes storage policies, properties, and health status.

A PowerStore cluster includes a native VASA Provider. The VASA Provider can be optionally registered in vSphere during the initial configuration of a PowerStore T or PowerStore Q cluster.

For more information about VASA provider registration and certificates, see the *PowerStore Security Configuration Guide*.

Storage containers

A storage container is used to present vVol storage from a PowerStore cluster to vSphere. vSphere mounts the storage container as a vVol datastore and makes it available for VM storage. When a PowerStore cluster is used to provide VM storage, user VMs should be provisioned on the vVol datastores. The default storage container is mounted automatically on the nodes of the cluster.

For more information, see Storage containers overview.

Storage Policy Based Management

vVols use Storage Policy Based Management (SPBM) to ensure that VMs have the appropriate storage capabilities through their entire life cycle. Storage QoS policies can be created in vCenter after the storage provider is registered.

NOTE: The name of the storage type to use when creating storage QoS policies for a PowerStore cluster is `DELLEMC.POWERSTORE.VVOL`.

These policies are used to determine the storage capabilities when a VM is provisioned. For information about creating a VM storage policy, see the VMware vSphere documentation.

Virtual Volumes overview

Virtual Volumes (vVols) are storage objects that are provisioned automatically on a storage container and store VM data.

vVol provisioning

Different management actions generate different vVols that are associated with a VM.

Table 1. Types of vVols

vVol	Description
Data vVol	A data virtual volume corresponds directly to each virtual disk .vmdk file.
Config vVol	A configuration virtual volume represents a small directory that contains metadata files for a virtual machine.
Memory vVol	A memory virtual volume that holds the contents of virtual machine memory for a snapshot.
Swap vVol	A swap virtual volume is created when a VM is first powered on and holds copies of VM memory pages that cannot be retained in memory.

On the PowerStore cluster, each vVol provisioned in vCenter Server is visible as a vVol in PowerStore Manager. For more information, see Monitoring and managing vVols.

Protocol Endpoints and vVols

A Protocol Endpoint is an internal object in storage systems and appliances that is required for working with vVols.

A PowerStore cluster can manage vVols without a Protocol Endpoint, but the ESXi host cannot access the vVols. To gain access, ESXi hosts communicate with vVols through a Protocol Endpoint. The Protocol Endpoint serves as a logical I/O proxy that enables the ESXi host to establish data paths to vVols and their associated VMs.

PowerStore clusters automatically create and provision Protocol Endpoints when adding an ESXi host.

Storage containers overview

Storage containers on PowerStore appliances act as a logical grouping of vVols that enable vVols to map directly to the cluster.

A storage container spans all appliances in a cluster and uses storage from each. On PowerStore appliances, vVols reside in storage containers, which enable vVols to map directly to an appliance within the PowerStore cluster. The specific appliance that a given vVol resides on is not visible to vSphere, and a vVol can migrate between appliances without disrupting vSphere operations. With storage containers, VMs or VMDKs can be managed independently.

For information about managing storage containers in PowerStore Manager, see Monitoring and managing storage containers.

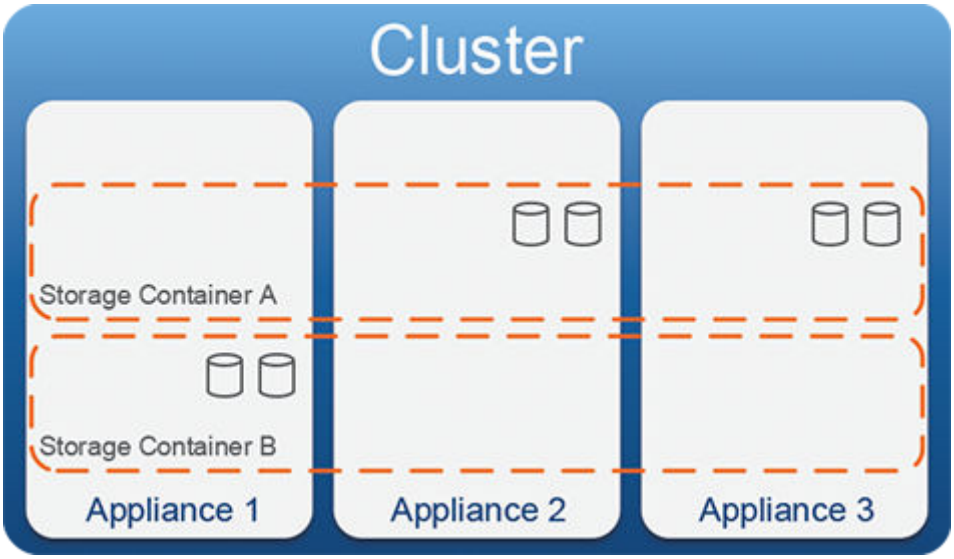

Figure 1. Storage containers spanning appliances in a PowerStore cluster

Multitenancy

PowerStore appliances support multiple storage containers on a cluster to support multitenancy requirements. Multiple storage containers can be created allowing the separation of VMs and associated vVols from one tenant to another.

Storage containers for ESXi hosts

About this task

To use storage containers with an external ESXi host:

Steps

1. Connect an external ESXi host to your PowerStore cluster.
2. Create an ESXi host in PowerStore Manager.
3. Use PowerStore Manager to create a storage container.
   For more information, see Create a storage container.
4. Use the vSphere Client or CLI to mount the storage container on the external ESXi host.
   For more information, see VMware vSphere product documentation.
5. Create a vVol datastore from the storage container.
6. Create VMs on the vVol datastore.

Virtualization architecture and configuration

In PowerStore T and PowerStore Q model clusters, a connection to a vCenter Server is optional and can be set up either during initial system configuration, or later in PowerStore Manager. Using vVol-based VMs on a PowerStore cluster requires registering the PowerStore VASA provider in vCenter.

NOTE: A vCenter Server connection with a registered VASA provider is not required to manage VMFS-based VMs, but it is still recommended.

If the VASA provider is not registered during initial system configuration, it can be registered in one of the following ways:

- The VASA provider can be registered when a connection to vCenter Server is configured in PowerStore Manager.
- The VASA provider can also be registered directly from vCenter, but additional steps are required.

NOTE: If a VASA provider is registered directly from vCenter, but a vCenter Server connection is not configured, PowerStore Manager cannot manage vVol-based VMs. Therefore, registering the VASA provider during the configuration of a vCenter Server connection in PowerStore Manager is recommended.

The PowerStore Resource Balancer manages the placement of vVols and keeps vVols for the same VM on the same appliance in a cluster. You can also migrate a vVol-based VM from one appliance to another from the **Virtual Machines** page of PowerStore Manager.

3

Configuring vCenter connections and VASA certificates

Topics:

Configure a vCenter server connection and register the VASA provider

Configuring a vCenter server connection can be completed either during or after the Initial Configuration wizard.

Prerequisites

- Using a vCenter user with the Administrator role and privileges is recommended when configuring a vCenter Server connection in PowerStore Manager.
- Alternatively, you can use a vCenter user with the minimum privileges set to **Storage Views** > **Configure service** and **Storage views** > **View**.

NOTE: PowerStore Manager only displays data for vCenter objects that vCenter user role used to configure the vCenter connection can access.

About this task

A PowerStore cluster can serve storage to multiple instances of vSphere.

- If using a self-signed VASA certificate on PowerStoreOS 3.5 or later, you can register multiple vCenter servers in PowerStore Manager. See Manually register multiple vCenter servers using the self-signed certificate for more information.
- If using a self-signed VASA certificate on a PowerStoreOS version earlier than 3.5, only one vCenter server can be registered in PowerStore Manager.
- If using a VMCA root certificate, only one vCenter server can be registered in PowerStore Manager.
- If using a third-party VASA certificate (PowerStoreOS 3.5 and later), you can register multiple vCenter servers with PowerStore if they all use the same root VASA CA certificate. For more information about registering multiple vCenter servers with PowerStore with a third-party certificate, see Manually register the VASA provider in vCenter.

NOTE: During the Initial Configuration wizard, you can opt to retain the PowerStore self-signed VASA certificate when configuring the vCenter server connection by enabling the **Retain VASA Certificate** option. Otherwise, the vCenter VMCA certificate or third-party VASA certificate is used. After initial configuration, VASA certificate settings can be modified under **Settings** > **Security** > **VASA Certificate** in PowerStore Manager.

Steps

1. Select **Compute** > **vCenter Server Connection** in PowerStore Manager.
2. Click **Connect**. The vCenter server configuration slide-out panel displays.
   a. Under **vCenter Server Configuration**, complete the following fields:
      - **vCenter Server IP Address/Host Name**
      - **vCenter Username**
      - **vCenter Password**
   b. Under **vCenter Server Configuration**, select the **Verify SSL server certificate** checkbox to enable PowerStore to validate the vCenter Server certificate upon registration (recommended).

c. Under **VASA Registration**, complete the following fields:
   - **PowerStore VM Administrator User** for PowerStore for VASA provider registration
   - **Password** of the PowerStore VM Administrator User

NOTE: The default PowerStore admin user role has VM Administrator privileges. If you do not have a user account with VM Administrator role privileges, add a **VM Administrator** user in PowerStore Manager.

3. Click **Connect**.
4. If you selected **Verify SSL server certificate**, additional information for the vCenter SSL certificate is displayed. Review the certificate information, then click **Confirm**.

NOTE: The machine SSL certificate appears in vCenter as `__Machine_Cert`. For more information about vCenter certificates, see the VMware documentation. For more information about viewing and verifying certificates, see the *PowerStore Security Configuration Guide*.

Next steps

- To update the stored IP address or credentials for vCenter Server on a PowerStore cluster, click **Update Configuration**.

  NOTE: You cannot change the vCenter server that a PowerStore cluster is connected to by updating the IP address. To change the vCenter server, see Change a vCenter Server connection.

- To disconnect the vCenter Server from a PowerStore cluster and unregister the VASA provider, click **Disconnect**.

  NOTE: You can no longer use the PowerStore cluster to manage VMs after the vCenter Server is disconnected.

Manually register the VASA provider in vCenter Server

If you want to register multiple vCenter servers with PowerStore, you must manually register the VASA provider in vCenter. If you are unable to register the VASA provider successfully in PowerStore Manager, you can also use this method.

About this task

Perform the following steps to manually register PowerStore as the VASA provider in vCenter.

Steps

1. Use vSphere to connect to the vCenter server and select the vCenter server object in the inventory.
2. Select the **Configure** tab and then select **Storage Providers**.
3. Click the **Add** icon.
4. Enter the connection information.
   - **Name** — Name for the storage provider, such as `PowerStore VASA provider`.
   - **URL** — VASA provider URL. The URL must be in the format: **`https://<IP address>:8443/version.xml`**, where *<IP address>* is the management IP address of the PowerStore cluster.
   - **User name** — Username of a PowerStore VM Administrator user account.
     - For local users, use **`local/<user name>`**.
     - For LDAP users, use ***`<domain>/<user name>`***.

     NOTE: If a VM Administrator user account does not exist on the PowerStore cluster, use PowerStore Manager to add a user account and select **VM Administrator** as the user role. If you use the default PowerStore admin user, a VM Administrator user account is not required because the PowerStore admin user already has VM Administrator role privileges.

   - **Password**—Password for the specified user account.
5. If you are registering multiple vCenter servers with PowerStore using a third-party certificate, clear the **Use storage provider certificate** checkbox.
6. Click **OK**.

Manually register multiple vCenter servers using the self-signed certificate

Beginning with PowerStoreOS 3.5, you can manually register multiple vCenter servers with PowerStore using the PowerStore self-signed certificate.

Prerequisites

NOTE: You cannot register multiple vCenter servers using a VMCA root certificate. Not enabling **Retrain VASA certificate** will result in the self-signed certificate to be overwritten with the VMCA root certificate.

Steps

1. In PowerStore Manager, go to **Settings** and, under **Security**, select **VASA Certificate**.
2. Set **Retain VASA Certificate** to **Enabled** to ensure the vCenter uses the PowerStore self-signed certificate.

   NOTE: If you do not enable the retain option, the VMCA root certificate eventually overwrites the self-signed certificate and registration of multiple vCenter servers fails.

3. In vCenter, manually add PowerStore as the VASA storage provider following the procedure in Manually register the VASA provider in vCenter Server.
4. Repeat this process for any additional vCenter servers that use the same PowerStore self-signed CA.

Next steps

Optionally, verify that the PowerStore self-signed certificate information displays for each vCenter server in the vCenter **Storage Providers** page.

Change a vCenter Server connection

Prerequisites

Ensure that you have the IP address or FQDN, username, and password for the vCenter Server.

About this task

Update the vCenter Server, vCenter admin credentials, or refresh the connection after you update the vCenter Server certificate in vCenter.

NOTE: To switch from a third-party certificate to a self-signed certificate, you must first disconnect the vCenter. See Switch from a third-party to a self-signed certificate for further instructions.

NOTE: Beginning with PowerStore 4.0 on systems with the **Verify SSL server certificate** checkbox enabled, changing the hostname of the vCenter server may impact the connection between PowerStore and the vCenter. The change in hostname may modify the machine SSL certificate and the VMCA root certificate. The certificates then become untrusted by PowerStore. See Restore a vCenter and VASA Provider connection for more details.

Steps

1. Under **Compute**, select **vCenter Server Connection**.
2. Select **Update configuration**.
3. Modify the vCenter Server IP or FQDN, vCenter username, and vCenter password.
4. Select the **Verify SSL server certificate** checkbox to enable PowerStore to validate the vCenter certificate (recommended).

   The first time that you select the checkbox, enter the vCenter password.

   NOTE: If the vCenter has an FQDN, it is recommended to use the vCenter FQDN instead of the IP address for the connection to PowerStore.

5. Click **Update** to save the changes.

6. If you enabled **Verify SSL server certificate** for the first time for the connected vCenter Server, additional information for the vCenter SSL certificate is displayed. Review the certificate information, then click **Confirm**.

   NOTE: The machine SSL certificate appears in vCenter as `__Machine_Cert`. For more information about vCenter certificates, see the VMware documentation. For more information about viewing and verifying certificates, see the *PowerStore Security Configuration Guide*.

Restore a vCenter and VASA Provider connection

Prerequisites

Beginning with PowerStore 4.0 on systems with the **Verify SSL server certificate** checkbox enabled, changing the hostname of the vCenter server may impact the connection between PowerStore and the vCenter. The change in hostname may modify the machine SSL certificate and the VMCA root certificate. The certificates then become untrusted by PowerStore.

This result can occur when:

- The hostname is changed from an IP address to an FQDN.
- The hostname is changed from an FQDN to an IP address.
- The hostname is changed from an IP address to a new IP address.

Also, resetting the VMCA root certificate in vSphere may impact the connection between PowerStore and the vCenter.

About this task

To restore the connection to vCenter and bring the VASA provider back online:

Steps

1. In PowerStore Manager, update the connection to vCenter as outlined in Change a vCenter Server connection. After updating the vCenter connection, the **vCenter Status** should appear as **Configured, Connected**.
2. If the **VASA Registration Status** still appears as **Offline** or **Unavailable** in PowerStore Manager, manually unregister and re-register the VASA provider in vCenter. See Manually register the VASA provider in vCenter Server.

VASA certificate

PowerStore operating system versions 3.5 and later support the import and use of a user provided, third-party Certificate Authority (CA) signed certificate. This CA signed certificate is used to replace the self-signed certificate that PowerStore VASA uses.

As part of this feature, you can do the following through either the PowerStore Manager, REST API, or CLI:

- Generate a Certificate Signing Request (CSR).
- Import a CA signed certificate.
- Select to retain the imported CA signed certificate so that it does not get overwritten by the vCenter server.

For more information about VASA, see the *PowerStore Security Configuration Guide*. For information about configuring a vCenter server connection to PowerStore, see the related PowerStore Online Help or the *PowerStore Virtualization Infrastructure Guide*.

Generate a Certificate Signing Request

Prerequisites

Before you generate a Certificate Signing Request (CSR), ensure that you have obtained the following information for the request:

- Common Name
- IP address
- DNS Name (optional)
- Organization
- Organization Unit

- Locality
- State
- Country
- Key Length

About this task

Generating a CSR is applicable to a Mutual Authentication Certificate, which is used in two-way authentication between PowerStore and the VASA server. To generate a CSR using the PowerStore Manager, do the following:

Steps

1. Select **Settings** and under **Security** select **VASA Certificate**.
   The **VASA Certificate** page appears.
2. Select **Generate CSR**.
   The **Generate CSR** slide out appears.
3. Type in the information that is used to generate the CSR.
4. Click **Generate**.
   The **Generate CSR** slide out changes to show the next steps that must be taken along with the certificate text.
5. Click **Copy to clipboard** to copy the certificate text to your clipboard.
6. Click **Close**.
7. The certificate authority (CA) must sign the certificate so that it can be imported as a Mutual Authentication Certificate.

Import a third party Certificate Authority signed server certificate for VASA Provider

Prerequisites

Before importing a third party Certificate Authority (CA) signed server certificate, ensure the following:

- A Certificate Signing Request (CSR) file was generated, downloaded and sent to the third party CA server for signing.
- The CA has signed the certificate so that it can be imported as a Mutual Authentication Certificate.
- Your vCenter trusts the CA of the certificate being imported, otherwise VASA functionality will be unavailable.
- You know the location of the certificate file or have the certificate text available to copy and paste for import.

About this task

To import a certificate using the PowerStore Manager, do the following:

Steps

1. Click **Settings** and, under **Security**, select **VASA Certificate**.
   The **VASA Certificate** page appears.
2. To prevent the VASA server certificate from being overwritten by the vCenter, ensure the Enable/Disable toggle is set to **Enabled**.
3. Select **Import**.
   The **Import Server Certificate** slide out appears.
4. Do one of the following:
   - Select **Select Certificate File**, then locate and select the file to import.
   - Select **Paste Certificate Text**, then copy and paste the certificate text in the text box.
5. Select **Import**.
   The certificate detail information should appear in the **VASA Certificate** page. Also, the VASA entry appearing on the **Certificate** page (**Settings** > **Security** > **Certificate**) should be identified by the **Service** as **VASA_HTTP** and **Scope** as **vasa**.

Switch from a self-signed to a VASA third-party CA certificate

About this task

Starting in PowerStoreOS 3.5, you can use a third-party VASA certificate instead of the default PowerStore self-signed certificate. This option also allows you to register more than one vCenter with the PowerStore cluster using your third-party root CA.

NOTE: If you have existing vVols on PowerStore Manager managed by the vCenter, the vVols may temporarily go offline after you remove PowerStore as the VASA provider in vCenter, until it is re-registered.

Steps

1. In PowerStore Manager, generate and import the third-party certificate by following procedures Generate a Certificate Signing Request and Import a third party Certificate Authority signed server certificate for VASA Provider.
2. In PowerStore Manager, set **Retain VASA Certificate** to **Enabled** once the certificate is accepted on PowerStore.
3. In vCenter, import the third-party CA certificate.
4. In vCenter, remove PowerStore as a VASA provider.
5. In vCenter, manually add PowerStore as the VASA storage provider following the procedure in Manually register the VASA provider in vCenter Server.

Next steps

Optionally, go to **Settings** > **Security** > **Certificates** to verify the self-signed VASA certificate appears with a **Type** of *Client CACertificate* and **Issued By** information for VMware or the third-party CA.

Switch from a third-party to a self-signed certificate

About this task

If you had previously used a VASA third-party CA certificate, use this procedure to revert to a PowerStore self-signed VASA certificate.

Steps

1. In PowerStore Manager, disconnect the vCenter server.
2. In PowerStore Manager on the **VASA Certificate** settings page, ensure the **Retain VASA Certificate** is set to **Enabled**.
3. In vCenter, remove the third-party CA certificate.
4. In PowerStore Manager, reconfigure the vCenter connection and register PowerStore as a VASA provider.

Next steps

Optionally, go to **Settings** > **Security** > **Certificates** to verify the self-signed VASA certificate appears with a **Type** of *Server Certificate* and an issuing organization of *PowerStore*.

VASA certificate renewal for vCenter and VASA third-party signed certificates

PowerStore monitors the following types of third-party signed certificates for expiration that are related to vCenter and VASA:

- VASA server (self-signed and retained)
- VASA server (VMCA signed)
- VASA server (third-party signed)
- VASA server (VMCA common)
- VMCA CA client validation (VMCA trusted root)
- vCenter connection (server CA certificate)

To renew a VASA server type certificate, renew the VMCA signed VASA Server certificate on vCenter for VMCA. For either a third-party or VMCA common certificate, the certificate must be imported into PowerStore. For a self-signed certificate, re-register the vCenter from PowerStore.

To renew a VMCA CA client certificate, renew the certificate from the vCenter.

To renew a vCenter connection server CA certificate, renew the certificate from the vCenter and then update this renewed certificate in PowerStore.

For more information about certificates, renewal, and alerts, see the *PowerStore Security Configuration Guide*.

4

Virtualization configuration in PowerStore appliances

Topics:

Managing virtualization components

You can monitor and manage basic properties of VMs, vVols, and storage containers from the PowerStore Manager. Advanced management capabilities are available with the vSphere Client.

Working with virtual resources

The PowerStore Manager provides detailed monitoring capabilities for connected VMs.

PowerStore Manager operations

The Virtual Machines page in PowerStore Manager allows you to view capacity, performance, and alerts for a VM. You can also manage data protection policies for a VM and manage the associated virtual volumes on the PowerStore cluster.

VMs that are deployed on vVols are displayed in PowerStore Manager. However, VMs on legacy non-vVol datastores are not displayed in PowerStore Manager.

For detailed information about the VM operations that you can perform from the PowerStore Manager, see Monitoring and managing VMs.

vCenter Server operations

Any VM operations that cannot be performed from the PowerStore Manager must be completed from the vCenter Server. In the PowerStore Manager, select **Compute** > **vCenter Server Connection** > **Launch vSphere** to start the vSphere Client and log in to the vCenter Server. For additional guidance, see the product documentation for the version of vCenter Server you are using.

Monitoring and managing VMs

The **Compute** > **Virtual Machines** page in the PowerStore Manager displays essential information about all connected vVol-based VMs in a centralized location.

The main view shows essential details for each VM. The table can be filtered, sorted, refreshed to show changes, and exported to a spreadsheet. VMs that are provisioned on a connected ESXi host are added to the table automatically. You can select one or more VMs to add or remove them from the dashboard watchlist or assign or remove a protection policy.

To view more details about a VM, select the name of the VM . You can monitor and manage the VM properties available on the following cards:

- **Capacity**: This card displays interactive line charts with storage usage history for the VM. You can view data for the past two years, month, or 24 hours, and print or download the chart data as an image or CSV file.

- **Compute Performance**: This card displays interactive line charts with CPU usage, memory usage, and system uptime history for the VM. You can view data for the past year, week, 24 hours, or hour and download the chart data as an image or CSV file.
- **Storage Performance**: This card displays interactive line charts with latency, IOPS, bandwidth, and I/O operation size history for the VM. You can view data for the last two years, month, 24 hours, or 1 hour and download the chart data as an image or CSV file.
- **Alerts**: This card displays alerts for the VM. The table can be filtered, sorted, refreshed to show changes, and exported to a spreadsheet. To view more details, select the description of the alert you are interested in.
- **Protection**: This card displays snapshots for the VM. The table can be filtered, sorted, refreshed to show changes, and exported to a spreadsheet. To view more details, select the name of the snapshot that you are interested in. You can also assign or remove a protection policy for the VM from this card.
  - VM snapshots, whether manual or scheduled, create VMware–managed snapshots.
  - You can take snapshots from PowerStore Manager or vSphere.
  - Whether the snapshots are taken from PowerStore Manager or vSphere, snapshots of vVol-based VMs are offloaded to the native snapshot engine on the cluster.
- **Virtual Volumes**: This card displays the vVols associated with the VM. The table can be filtered, sorted, refreshed to show changes, and exported to a spreadsheet. To view more details, select the name of the vVol you are interested in.

Monitoring and managing vVols

You can use PowerStore Manager to view essential information about vVols through the storage container or VM to which they are connected.

- From the **Storage** > **Storage Containers** page, select the storage container name. On the details page for the storage container, select the **Virtual Volumes** card.
- If the PowerStore cluster is connected to a vCenter Server, you can view vVols in the context of their VMs. From the **Compute** > **Virtual Machines** page, select the name of the VM . On the details page for the VM, select the **Virtual Volumes** card.

The main view shows the name of each vVol, what type of vVol it is, the amount of logical used space, the amount of space that is provisioned, when it was created, its storage container, and its I/O priority. The table can be filtered, sorted, refreshed to show changes, and exported to a spreadsheet. You can select a single vVol for migration to another appliance. You can select multiple vVols to collect support materials or add or remove them from the dashboard watchlist.

To view more details about a vVol, select the name of vVol. You can monitor and manage the vVol properties available on the following cards:

- **Capacity**—This card displays current and historical usage details for the vVol. You can view data for the past two years, one month, or 24 hours, print the chart, and download the chart data as an image or CSV file.
- **Performance**—This card displays interactive line charts with latency, IOPS, bandwidth, and I/O operation size history for the vVol. You can view data for the past two years, one month, 24 hours, or one hour and download the chart data as an image or CSV file.
- **Protection**—This card displays snapshots and replication sessions for the vVol.

To view the properties of the vVol, select the pencil icon next to the vVol name.

NVMe host namespaces for vVols

NVMe controller design allows each host NQN to host ID pair to act as a distinct host entity. ESXi hosts leverage this design by separating NVMe host NQN and host ID pairs into vVol and non-vVol host namespaces. A namespace is a logical unit of NVMe storage that behaves like a LUN or volume. The ESXi host uses two different controllers to access vVols and traditional volumes. In vSphere, the host entity is the same host for both vVols and traditional volumes. However, on the storage system, the same ESXi host using NVMe for vVols and non-vVol datastores are recognized as two different hosts. Thus, two unique host entries must be created on the storage system for NVMe vVol and NVMe traditional volume access. This design applies to both NVMe/TCP vVols and NVMe/FC vVols.

Configuring a storage container for NVMe/FC vVols

Prerequisites

Support for NVMe/FC vVols on PowerStore requires:

- VMware ESXi version 8.0 Update 2 or later
- A PowerStore storage network configured for the NVMe protocol

  NOTE: After configuring a new storage network or modifying an existing storage network, rescan the VASA Provider in vSphere.

- A PowerStore host created with the *NVMe vVol* host **Initiator Type**. See NVMe host namespaces for vVols for more information.

About this task

Configure a storage container for vVols using NVMe/FC.

Steps

1. In PowerStore Manager, register the VASA Provider. See Configure a vCenter server connection and register the VASA provider.

   Alternatively, manually register PowerStore as the VASA Provider in vCenter. See Manually register the VASA provider in vCenter Server.
2. In vSphere on the ESXi host, add the NVMe over FC storage adapter.

   For more information about configuring the storage adapter, see the Dell Host Connectivity Guide for VMware ESXi Server.
3. In vSphere on the ESXi host, create the VMkernel adapter with NVMe over FC enabled, or enable NVMe over FC on an existing VMkernel adapter. Rescan the VASA provider and the NVMe storage adapter.
   After the rescan, the PowerStore NVMe controllers should be visible in vSphere.
4. In PowerStore Manager, add the ESXi host NVMe/FC vVol initiator.
   a. Under **Compute**, select **Hosts Information** > **Add Host**.
   b. On the **Host Details** page, enter a name for the host and select **ESXi** as the operating system.
   c. On the **Initiator Type** page, select **NVMe vVol**.
   d. On the **Host Initiators** page, select the host initiator from the autodiscovered initiators list based on the unique NVMe vVol NQN or Host-ID. The **Initiator Type** column displays *NVMe vVol*, and the NQN string contains the value *vvol*.

      NOTE: ESXi hosts use a unique Host NQN and Host ID for NVMe vVols, separate from the ESXi host NVMe NQN. Because of the unique NVMe vVol IDs, separate host entries in PowerStore Manager must be created for NVMe vVols and traditional volumes using NVMe.

      - To validate the NVMe vVol-specific NQN for the host initiator in vSphere 8.0 Update 2, run the vSphere PowerCLI `esxcli storage vvol nvme info get` command.
      - To validate the NVMe vVol-specific NQN for the host initiator in vSphere 8.0 Update 1:
        - Enable SSH on the ESXi host.
        - Log in as root to the local VMware CLI.
        - Run the `localcli --plugin-dir /usr/lib/vmware/esxcli/int storage internal vvol vasanvmecontext get` command.
5. In PowerStore Manager, create a storage container with the NVMe storage protocol. See Create a storage container.
6. In vSphere, mount the new storage container to the ESXi host. Select the host, create a vVol datastore, and select the PowerStore NVMe/FC storage container.

Results

NOTE: For VMware ESXi 8.0 versions earlier than 8.0u1, NVMe/FC vVols may appear offline. See *Knowledgebase article 000227605* for details.

Configuring a storage container for NVMe/TCP vVols

Prerequisites

Support for NVMe/TCP vVols on PowerStore requires:

- VMware ESXi version 8.0 Update 2 or later
- PowerStoreOS version 3.6.x or later

- PowerStore storage network configured for the NVMe protocol

  NOTE: After configuring a new storage network or modifying an existing storage network, rescan the VASA Provider in vSphere.

- A PowerStore host created with the *NVMe vVol* host **Initiator Type**. See NVMe host namespaces for vVols for more information.

For the latest information about ESXi version compatibility and special considerations, see KB article 000216664. For information about the latest qualified versions of ESXi with PowerStore, see the *PowerStore Simple Support Matrix*, which can be downloaded from dell.com/powerstoredocs.

Limitations:

- Storage networks using Centralized Discovery Controllers (CDC) are not supported for PowerStore vVols.
- Using an ESXi host that is configured with both an NVMe adapter for FC and an NVMe adapter for TCP for NVMe vVols on a single PowerStore appliance is not supported.
- Automatic space reclaim is not supported for NVMe vVols. Although PowerStore vVols are thin, vSphere does not present them as thin to the guest operating systems.

About this task

Configure a storage container for vVols using NVMe/TCP.

See the VMware documentation for your ESXi version for detailed vSphere instructions.

Steps

1. In PowerStore Manager, register the VASA Provider. See Configure a vCenter server connection and register the VASA provider.

   Alternatively, manually register PowerStore as the VASA Provider in vCenter. See Manually register the VASA provider in vCenter Server.
2. In vSphere on the ESXi host, add the NVMe over TCP storage adapter.

   For more information about configuring the storage adapter, see the Dell Host Connectivity Guide for VMware ESXi Server.
3. In vSphere on the ESXi host, create the VMkernel adapter with NVMe over TCP enabled, or enable NVMe over TCP on an existing VMkernel adapter. Rescan the VASA provider and the NVMe storage adapter.
   After the rescan, the PowerStore NVMe controllers should be visible in vSphere.
4. In PowerStore Manager, add the ESXi host NVMe/TCP vVol initiator.
   a. Under **Compute**, select **Hosts Information** > **Add Host**.
   b. On the **Host Details** page, enter a name for the host and select **ESXi** as the operating system.
   c. On the **Initiator Type** page, select **NVMe vVol**.
   d. On the **Host Initiators** page, select the host initiator from the autodiscovered initiators list based on the unique NVMe vVol NQN or Host-ID. The **Initiator Type** column displays *NVMe vVol* and the NQN string contains the value *vvol*.

      NOTE: ESXi hosts use a unique Host NQN and Host ID for NVMe vVols, separate from the ESXi host NVMe NQN. Because of the unique NVMe vVol IDs, separate host entries in PowerStore Manager must be created for NVMe vVols and traditional volumes using NVMe.

      - To validate the NVMe vVol-specific NQN for the host initiator in vSphere 8.0 Update 2, run the vSphere PowerCLI `esxcli storage vvol nvme info get` command.
      - To validate the NVMe vVol-specific NQN for the host initiator in vSphere 8.0 Update 1:
        - Enable SSH on the ESXi host.
        - Log in as root to the local VMware CLI.
        - Run the `localcli --plugin-dir /usr/lib/vmware/esxcli/int storage internal vvol vasanvmecontext get` command.
5. In PowerStore Manager, create a storage container with the NVMe storage protocol. See Create a storage container.
6. In vSphere, mount the new storage container to the ESXi host. Select the host, create a vVol datastore, and select the PowerStore NVMe/TCP storage container.

Monitoring and managing storage containers

The **Storage** > **Storage Containers** page in the PowerStore Manager displays essential information about all storage containers in a centralized location.

The main view shows the name of each storage container, any current alerts, and capacity details. The table can be filtered, sorted, refreshed to show changes, and exported to a spreadsheet. You can perform the following actions on a storage container:

- Create a storage container.
- Change the name of a storage container. If the PowerStore cluster is connected to a vCenter Server, the name of the storage container is updated in vCenter to match the name in the PowerStore Manager.
- Limit space usage by a storage container.
- Delete a storage container.

  NOTE: You cannot delete a storage container when there are VMs on the associated storage containers in vCenter.

- Monitor current and historical space usage.

To view current and historical usage details for a storage container, select the name of the storage container. You can view data for the past two years, one month, or 24 hours, print the chart, and download the chart data as an image or CSV file. The PowerStore Manager raises an alert when usage of a storage container reaches or exceeds 85% of its available space.

Create a storage container

About this task

Use PowerStore Manager to create storage container on a PowerStore cluster.

Steps

1. Under **Storage**, select **Storage Containers**.
2. Click **Create**.
3. Enter a name for the storage container.
4. Optionally, select the **Enable storage container capacity quota** checkbox to specify a capacity quota for the storage container.
5. If applicable, set a **Container Quota** size.
6. Select the storage protocol.
   - Select SCSI for hosts that will access vVols on the storage container using an iSCSI or FC transport layer.
   - Select NVMe for hosts that will access vVols on the storage container using a TCP or FC transport layer.
7. Click **Create**.

Change storage container properties

About this task

You can change certain properties of a storage container, including the connection protocol type.

Steps

1. Under **Storage**, select **Storage Containers**.
2. Select an existing storage container, then select the edit icon to edit the storage container properties.
3. Rename the storage container, enable or disable the storage container capacity quota, modify the container quota or High water mark values, or change the storage protocol.

   NOTE: You can only modify the storage protocol if there are no bound vVols and the storage container is not mounted on any ESXi hosts.

4. Click **Apply**.

Limit space usage by a storage container

About this task

To limit the amount of space a storage container consumes, set a quota on that storage container. The quota represents the total maximum size of the data that can be written to the vVols in the storage container. Space that snapshots and thin clones consume does not count towards the quota.

Steps

1. Under **Storage**, select **Storage Containers**.
2. Select the storage container for which you want to set a quota and select **Modify**.
3. Select the **Enable storage container capacity quota** checkbox to enable a quota and specify the limit that you want, then select **Apply**.

Results

When the space that the storage container is using reaches or exceeds the high watermark for the quota, the system generates a notification. If the space used falls below the high watermark for the quota, the notification clears automatically. By default, the high watermark for the quota is 85%, but you can change this value.

To remove the quota on a storage container, clear the **Enable storage container capacity quota** checkbox on the **Properties** panel for that storage container.

Monitoring ESXi hosts

When a PowerStore cluster is connected to a vCenter Server, the cluster becomes aware of ESXi hosts and associates PowerStore hosts with ESXi hosts.

This functionality allows the PowerStore Manager to:

- Associate a host registered in the PowerStore Manager to its corresponding name in vCenter
- Display the ESXi host name on which vVol-based VM is running.

Manage Local Users

Steps

1. Select the **Settings** icon, and then select **Users** in the **Security** section.
2. If not already selected, select **Local**.
3. Do any of the following:
   - Add a user. When you add a user, you select the role of the user.
   - View or change the role of a user.
   - Delete a user.

     NOTE: The built-in Administrator account cannot be deleted.

   - Change the password of a user.
   - Lock or unlock a user.

     NOTE: Logged-in users with either an Administrator or Security Administrator role cannot lock their own account.

Using an external ESXi host with a PowerStore cluster

If you have another ESXi host that is connected to a vCenter Server in your environment, you can grant the host access to your PowerStore cluster.

- ESXi host configuration guidelines – For information about configuring an external ESXi host on a PowerStore cluster, see the E-Lab *Host Connectivity Guide for VMware ESXi Server* on eLab Navigator.

- Recommended vCenter Server settings – Use the appropriate size vCenter Server Appliance to hold the expected number of objects. The options are Tiny, Small, Medium, Large, and X-Large.

For information about the resources that are required and number of objects that are supported at each size level, see the VMware vCenter documentation.

Additional VMware software and configuration

VMware integration

You can use many VMware products with PowerStore the same way you would in your existing VMware environment. The following products are supported in this release:

- VMware vRealize Orchestrator (vRO)
- Dell Virtual Storage Integrator (VSI) for VMware vSphere Client
- VMware Storage Replication Adapters (SRA)
- VMware Site Recovery Manager (SRM)

For more information, see VMware documentation about working with Dell plugins.

5

Replicating datastores

You can replicate vVol datastores using the native PowerStore Manager functionality and Site Recovery Manager (SRM) 8.4 and later.

For more detailed information for replicating datastores, see the *PowerStore Protecting Your Data Guide*.

For more detailed information about replicating vVols using SRM, see the *PowerStore: VMware Site Recovery Manager Best Practices* white paper.

Topics:

Virtual volumes replication

PowerStore integrates with VMware Site Recovery Manager (SRM) to support asynchronous replication of virtual volume.

Virtual machine remote protection is configured using vSphere Storage Policy-Based Management (SPBM). For recovery from failure, failover of virtual machines is configured using VMware SRM.

VMware SRM is a VMware disaster recovery solution that automates recovery or migration of virtual machines between a protected site and a recovery site.

Snapshot and Replication rules that are created in PowerStore are exposed to vSphere and can be added to protection policies. vSphere provides a storage policy to PowerStore during vVol creation.

A replication group that includes virtual volumes that should be replicated together, is the replication and failover unit that is configured in vSphere.

Both Read-Only and Read/Write snapshots can be generated for vVols. Synchronization, manual, or according to the set schedule is applied only to Read-Only snapshots.

To view the details of a virtual volume replication session:

1. Select **Protection** > **Replication**.
2. Click the replication session status to view it details.

The graphic in the replication session details window indicates that vSphere manages the replication session.

From the replication session details window you can do the following:

- View the replication session details.
- Rename the replication group.
- Pause and resume the replication session.
- Synchronize the replication session.

6

Best practices and limitations

Topics:

Creating VM clones

The best practices for creating clones of vVol-based VMs on a PowerStore cluster depend on application and cluster type. The best practices also depend on how you plan to distribute VM clones.

Distributing VM clones across a multi-appliance cluster (linked or instant clones)

When linked or instant clones are created from a base VM, the PowerStore resource balancer selects an appliance on which to create the VM and it places the config vVol on that appliance. However, the data vVol for the linked clone is created on the same appliance as the base VM.

This issue can lead to following inefficiencies:

- Storage - The base VM and its VM clones only use storage on a single appliance.
- I/O load - The compute for VM clones might be distributed among multiple appliances, however all I/O is directed to the single appliance hosting the storage. This issue increases the I/O load and network traffic on the appliance.
- Increased fault domains - The config vVols and data vVols for VM clones are on multiple fault domains.

The best practices solution is to create a base VM on each appliance in the cluster. When creating a clone from a base VM, select the appliance with the fewest clones of the base VM.

NOTE: Distributing VM clones among appliances is typically performed when there are many clones of a base VM, such as 100 clones. If there are only a few VM clones, placing all the VM clones on a single appliance, and using the other appliances for other workloads may be sufficient.

For instructions on distributing VM clones across a multi-appliance PowerStore cluster, see Distribute VM clones across an existing PowerStore cluster.

Distributing VM clones to a new appliance in a cluster (linked or instant clones)

When an appliance is added to an existing PowerStore cluster, VM clones are stored on the same appliance as the base VM.

This issue can lead to following inefficiencies:

- Storage - The base VM and its clone only use storage on a single appliance.
- I/O load - The compute for VM clones might be distributed among multiple appliances, however all I/O is directed to the single appliance hosting the storage. This issue increases the I/O load and network traffic on the appliance.

The best practices solution is to manually migrate some of the VM clones to the new appliance in the cluster.

NOTE: Migrating vVols for linked VM clones transforms them into full clones, which can lead to increased storage utilization. However, the PowerStore cluster can compensate for this issue by using storage deduplication.

For instructions on migrating VM clones to a new appliance in a PowerStore cluster, see Distribute VM clones to a new appliance in a PowerStore cluster.

Distribute VM clones across an existing PowerStore cluster

To create VM clones on a PowerStore T model or PowerStore Q cluster with multiple appliances, create a base VM on each appliance, migrate the vVols for each base VM to the appropriate appliance, then create VM clones from the base VMs.

Steps

1. Use vSphere to create a base VM on each appliance in the cluster.

   Use a name for the base VM that reflects the appliance on which the base VM is located. For example, use the name `BaseVM-Appliance1` for appliance one and use the name `BaseVM-Appliance2` for appliance two.

   NOTE: If a base VM was not created on the appropriate appliance, use PowerStore Manager to migrate the vVols for the base VM to the correct appliance. For instructions, see Migrate vVols to another appliance (advanced).

2. Use vSphere to create VM clones from the base VMs.

   Remember to evenly distribute the VM clones across the appliances in the cluster to avoid possible cluster inefficiencies.

Distribute VM clones to a new appliance in a PowerStore cluster

When an appliance is added to an existing PowerStore cluster, VM clones are stored on the same appliances as the base VMs.

The best practices solution is to migrate some of the VM clones to the new appliance in the cluster using PowerStore Manager. For instructions on migrating vVols for VM clones, see Migrate vVols to another appliance (advanced).

NOTE: Migrating vVols for linked clones transforms them into full clones, which can lead to increased storage utilization. However, the PowerStore cluster can compensate for this issue by using storage deduplication.

Migrate vVol-based VMs to another appliance

Use this feature to migrate vVol VMs to another appliance in the cluster without any disruption to host I/O.

About this task

When you migrate a vVol-based VM, all associated fast clones and snapshots also migrate with the storage resource. During the migration, additional work space is allocated on the source appliance to facilitate data movement. The amount of space that is needed depends on the number of storage objects and amount of data being migrated. This work space is released and freed up after the migration is complete.

NOTE: Only vVol-based VMs can be migrated. Migrating VMFS-based VMs is not supported.

Steps

1. Under **Compute**, select **Virtual Machines**.
2. Select the vVol-based VM to migrate, then select **More Actions** > **Migrate**.
   The **Migrate** slide-out panel is displayed. The system will run checks to ensure the VM is applicable for migration.

   NOTE: If the VM is protected, the entire VM replication group will be migrated.
3. Select the **Destination Appliance** for the VM migration.
4. Select **Start Migration Immediately** to migrate now, or **Defer Migration** to perform the migration at a later time.
   When selecting **Defer Migration**, the migrations session is created, but not started. It can be started at a later time from the **Migration** page.

Migrate vVols to another appliance (advanced)

Only use this feature to migrate individual vVols to another appliance in the cluster when it is not possible to migrate the entire vVol-based VM.

About this task

NOTE: As a best practice, migrate the entire vVol-based VM using the procedure provided in Migrate vVol-based VMs to another appliance. Migrating the entire vVol-based VM guarantees colocation of all of the vVols that make up the VM for optimal performance. Migrating an individual vVol should only be done by advanced administrators in limited cases, such as when the vVol has certain capacity and IO requirements that necessitate placement of the vVol on a specific appliance.

When you migrate a vVol, all associated fast clones and snapshots also migrate with the storage resource. During the migration, additional work space is allocated on the source appliance to facilitate data movement. The amount of space that is needed depends on the number of storage objects and amount of data being migrated. This work space is released and freed up after the migration is complete.

Steps

1. Under **Storage**, select **Storage Containers**.
2. Select the storage container that contains the vVol that you want to migrate and select the **Virtual Volumes** card.
3. To display vSphere host names and the appliances on which vVols are located, select **Show/Hide Table Columns**, then select **vSphere Host Name** and **Appliance** to display those columns in the **Virtual Volumes** card.
4. Select the vVol to migrate and select **Migrate**.
   The **Migrate** slide-out panel is displayed.
5. Select an appliance that best meets the requirements for the vVol that you are migrating.
6. Select **Next**.
   A migration session with a status of Pending is created in the background.
7. Select **Finish**.
   The migration session is displayed on the **Migration Actions** page, and then the **Required Action for Migration** slide-out panel is displayed.
8. Select **Start Migration** and click **Migrate Now**.
   Depending on the amount of data that is being migrated, it may take several minutes, hours, or days to complete the migration. It may also have an impact on the overall system performance.

Using vVols across multiple vCenter Servers

If you are not using a third-party VASA CA certificate to register multiple vCenter servers with PowerStore, there are other options available. See KB article 000186239: *Using vVols across multiple vCenters: How to register the PowerStore VASA provider across multiple vCenters* for more information.

Using multiextent for VMFS datastores

VMware vSphere allows VMFS datastores to be expanded across multiple storage volumes (LUNs) by using the VMFS extents (multiextent) feature. Typically there is a one-to-one mapping between a VMFS datastore and a volume, but with multiextent, a single VMFS datastore may be partitioned across multiple storage volumes.

The distribution of the data by vSphere across these volumes may be unpredictable. As a best practice, you should build VMFS datastores that use multiextent on volumes that are in the same volume group. This produces crash-consistent snapshots and provides better data protection.