


Dell EMC PowerStore

Configuring Volumes

2.x

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.

Additional Resources	4
Chapter 1: Volumes	5
Volumes in PowerStore appliances.....	5
Thin provisioning.....	6
Create a volume.....	6
Map volumes to a host.....	7
Change volume properties.....	7
Delete a volume.....	8
Assign a protection policy.....	8
Change a protection policy for a volume.....	9
Unassign a protection policy from a volume.....	9
Chapter 2: Volume groups overview	10
Volume groups in PowerStore appliances.....	10
Create a volume group.....	11
Add existing volumes to a volume group.....	11
Add new volumes to a volume group.....	12
Map Volumes in a Volume Group to a Host.....	12
Remove a volume from a volume group.....	13
Chapter 3: Hosts and host group configurations	14
Add a host.....	14
Add a host group.....	15
Map volumes to a host or a host group.....	15
Configure CHAP authentication.....	16
Chapter 4: Data mobility for volumes and volume groups	17
Migrate storage resources to another appliance.....	17
Migrate vVols to another appliance.....	18
Chapter 5: Thin clones	19
Thin clone terminology and hierarchy.....	19
Create a thin clone of a volume.....	22
Create a thin clone of a volume group.....	22
Chapter 6: Performance policies	23
Change a performance policy for a volume.....	23

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.

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 <https://www.dell.com/powerstoredocs>.

- **Troubleshooting**

For information about products, software updates, licensing, and service, go to <https://www.dell.com/support> and locate the appropriate product support page.

- **Technical support**

For technical support and service requests, go to <https://www.dell.com/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.

Volumes

A volume is a single unit that represents a specific amount of storage. Volume storage resources provide hosts with access to general-purpose, block-level storage through network-based iSCSI, Fibre Channel, and NVMe-over-Fibre Channel connections. With volume storage, you can manage partitions of block storage resources so that host systems can mount and use these resources. Each volume is associated with a name, a NAA (Network Addressing Authority) identifier and a NGUID (Namespace Globally Unique Identifier).

After a host connects to a volume, it can use the volume like a local storage drive. When a volume is created, the PowerStore Resource Balancer automatically determines on which appliance the volume is provisioned unless that volume has been mapped to a specific host/host group. In such cases, the volume is created only on an appliance that sees this host/host group. Since there is no redirection between appliances within a cluster, I/O is sent to one of the two nodes that contains storage for the volume.

Topics:

- [Volumes in PowerStore appliances](#)
- [Thin provisioning](#)
- [Create a volume](#)
- [Map volumes to a host](#)
- [Change volume properties](#)
- [Delete a volume](#)
- [Assign a protection policy](#)
- [Change a protection policy for a volume](#)
- [Unassign a protection policy from a volume](#)

Volumes in PowerStore appliances

You can perform the following operations from the **Volumes** page within the PowerStore Manager:

- Create a volume.
Optionally, you can associate the volume with a volume group and with a host/host group.
- View and change volume properties.
- Delete a volume (after unmapping the volume from any hosts).
- Expand the volume size.
- Modify the performance policy of a volume.
- Migrate a volume to a different appliance.
- Add a volume to or delete a volume from the dashboard watchlist.
- Map a volume to a host.
- Assign or unassign a protection policy.
- Restore content from a snapshot.
- Collect support materials.
- Create a thin clone of a volume.
- Refresh content from a related volume.

To monitor the capacity, performance, alerts, protection status, and connectivity of a volume, click the name of the volume you want to view.

The following list describes some important considerations when creating volumes:

- Your system creates volumes as thin volumes.
- When a volume is created, the Resource Balancer determines on which appliance the volume is provisioned unless that volume has been mapped to a specific host/host group. In such cases, the volume is created only on an appliance that sees this host/host group.
- Volumes can be between 1 MB and 256 TB in size.

- There is no redirection between appliances in a cluster, meaning that I/O is sent to one of the two nodes that contains storage for the volume.

Thin provisioning

Storage provisioning is the process of allocating available drive capacity to meet the capacity, performance, and availability requirements of hosts and applications. In PowerStore, volumes and file systems are thin provisioned to optimize the use of available storage.

Thin provisioning works as follows:

- When you create a volume or file system, the system allocates an initial quantity of storage to the storage resource. This provisioned size represents the maximum capacity to which the storage resource can grow without being increased. The system reserves only a portion of the requested size, called the initial allocation. The requested size of the storage resource is called the subscribed quantity.
- The system will only allocate physical space when data is written. A storage resource appears full when data written to the storage resource reaches the provisioned size of the storage resource. Since provisioned space is not physically allocated multiple storage resources could subscribe to the common storage capacity.

Thin provisioning allows multiple storage resources to subscribe to a common storage capacity. Therefore, it allows organizations to purchase less storage capacity up front, and increase available drive capacity on an on-demand basis, according to actual storage usage. While the system allocates only a portion of the physical capacity requested by each storage resource, it leaves the remaining storage available for other storage resources to use.

The system reports the capacity savings gained from thin provisioning using the Thin Savings metric, which is calculated for volume families and file systems. A volume family consists of a volume and its associated thin clones and snapshots.

Thin provisioning is always enabled.

Create a volume

Prerequisites

Obtain the following information:

- The storage size that you want to allocate for the volume.
- Performance and Protection policies to apply to the volume.
- Information about the host or hosts that can access the volume (if a host configuration does not exist).

This information includes the address of the host or WWN, operating system, storage protocol (iSCSI or NVMe), and initiator to use.

i **NOTE:** If you plan on using volumes in a volume group, it is recommended that you create the volume group first, and then add new volumes to it.

When you create volumes, they may get automatically placed in different appliances within the cluster. A volume group requires all member volumes to reside in the same appliance. If you then want to add existing volumes to a volume group, you must first migrate them to the same appliance.

Steps

1. Under **Storage**, select **Volumes**.
2. Click **Create**.

i **NOTE:** You can also create volumes when you create a volume group.

3. In the **Create Volumes** slide-out panel, enter the following volume information:
 - **Name (or Prefix):** When you create a single volume, this name is the name of the volume. When you create multiple volumes, this name is the base name to which a number is appended.
 - **Quantity:** You can add up to 100 volumes that have the same properties. The system appends the volume name with a number when creating multiple volumes.
 - **Size:** The size is the quantity of storage that is subscribed for the volume. After you create the volume, you can increase its size but not decrease it. PowerStore supports the creation of thin volumes up to 256 TB in size.

- **Placement:** You can place the volume in an appliance that is shown in the drop-down list, or allow the system to place the volume automatically.
- **Associated Volume Group** (optional) : Select which volume group you want to associate the volume with.
- **Volume Protection Policy** (optional): Select a protection policy that contains snapshot and replication rules applicable for the volume. You can add a protection policy after creating the volume.
- **Volume Performance Policy:** Set the performance profile on volumes to service IOPS when there is contention for resources at the system level. Limit I/O throughput and bandwidth to provide more predictable performance.

Select a Performance Policy consistent with the I/O priority (High, Medium, or Low).

- **Available Hosts/Host Groups** (optional): Select the storage protocol and then select the hosts/host groups that can access the volume.

NOTE: A volume can be attached to either a SCSI or NVME host. Volume migration and replication will use iSCSI for transport.

When you connect the volume to the hosts/host groups, you can specify a Logical Unit Number. If a Logical Unit Number is not specified, the system assigns one by default. You can add hosts/host groups after creating the volume.

Map volumes to a host

You can map and unmap volumes to a single host or multiple hosts.

About this task

The following restrictions apply:

- After a volume is mapped to a host, it shares the same storage protocol (SCSI or NVMe) as the host to which it is mapped.
- Mixed protocols are not supported.

Steps

1. From **Storage > Volumes**, check the box next to the volume or volumes that you want to map to a host.
2. Select **Provision > Map** to open the **Map Hosts** slide-out panel.
3. Select any hosts that you want the volume to be mapped to.
4. Click **Apply**.

Change volume properties

Steps

1. Under **Storage**, select **Volumes**.
2. Click the check box next to the volume name and then click **Modify**.

NOTE: You can also access the **Properties** panel by clicking the name of the volume to open the volume page and then clicking **Actions > Properties**

The **Properties** slide-out panel allows you to change the volume name and description, to increase the volume size and to change the performance policy. When you modify the size of the source volume, the size of the destination volume is also modified.

NOTE: If you want to rename a volume that is being replicated, you must pause the replication session if a session is running. You can then change the name on the source volume only. The volume name on the destination system updates when the replication session resumes.

To change the source volume name to a name that exists on the destination system, you must first rename the volume on that destination system.

Delete a volume

Prerequisites

Delete a volume only under the following conditions:

- The volume was used for testing purposes, and the tests have finished.
- The volume has been replicated to a different destination, and the source volume is no longer needed.
- You are trying to save space by deleting the volume and the data on that volume is no longer needed.

 **CAUTION: Volume deletion is an irreversible operation.**

About this task

Ensure that the following conditions are met before attempting to delete a volume:


- The volume is not a member of a volume group.

The deletion is blocked if the volume is a member of a volume group.

- The volume does not have an associated protection policy.


The deletion is blocked if the volume has an associated protection policy.

- The volume is not mapped to any hosts.

 **NOTE:** If hosts are mapped, volumes cannot be deleted. Remove host access before deleting any volumes. Plan host downtime where needed, or ensure the hosts no longer need the volume before deleting access. If you are migrating hosts from one volume to another, ensure that the hosts can access the new volume. After you verify that the hosts can access the new volume, delete them from the old volume.

- The volume does not have any associated snapshots that contain required backup data .

Deleting the volume also deletes the associated snapshots.

 **NOTE:** Following an attempt to delete the volume, the system displays a warning, but does not block the deletion operation.

- The volume is not involved in a migration.

Steps

1. Under **Storage**, select **Volumes**.
2. Click the check box next to the volume you want to change.
You can delete multiple volumes by checking all the volumes you want to delete.
3. Select **Delete**.

Assign a protection policy

A protection policy establishes snapshot and data replication rules for data protection. If the volume is a member of a volume group, the volume group policy assigned to the volume group protects that volume and cannot be changed at the volume level.

Steps

1. Under **Storage**, select **Volumes**.
2. Click the check box next to the relevant volume.
3. Select **Protect > Assign Protection Policy**.
4. On the **Assign Protection Policy** slide-out panel, select a policy and click **Apply**.

Change a protection policy for a volume

A protection policy establishes snapshot and data replication rules for data protection. You can change the protection policy assigned to a volume.

About this task

If the current policy assigned to the volume includes a replication rule, you can only change it to a policy with no replication rule (which will stop this volume's replication) or to a policy with a replication rule that uses the same remote system.

Steps

1. Under **Storage**, select **Volumes**.
2. Click the name of the volume you want to change.
3. On the **Volumes** page for that specific volume, click the **Protection** tab, and then click **Change**.
4. On the **Change Protection Policy** slide-out panel, select a policy.

Unassign a protection policy from a volume

A Unassigning a protection policy from a volume will remove local and/or remote protection from that volume.

About this task

Unassigning a protection policy from a volume results in the following:

- Scheduled snapshots and replication that are based on the policy rules stop.
- Existing snapshots remain and are retained in the system based on the snapshot rule settings that applied on time of creation.

If the volume is a member of a protected volume group, the protection policy cannot be unassigned at the volume level.

Steps

1. Under **Storage**, select **Volumes**.
2. Click the check box next to the relevant volume.
3. Select **Protect** > **Unassign Protection Policy**.

Volume groups overview

A volume group is a logical container for a group of volumes.

A volume group provides a single point of management for multiple storage resources that work together as a unit.

You can use volume groups to achieve the following:

1. A simpler and easier way to manage and monitor resources.
2. Maintaining consistency across multiple volumes.

For example, you can use volume groups to monitor metrics and manage data protection for development applications, user applications, and user storage resources. You can also use volume groups to separate the management of test environments from development environments.

Volume groups for a PowerStore appliance are dynamic and can be adjusted as your requirements change. You can add new members to a volume group or delete them from a volume group after it is created.

Topics:

- [Volume groups in PowerStore appliances](#)
- [Create a volume group](#)
- [Add existing volumes to a volume group](#)
- [Add new volumes to a volume group](#)
- [Map Volumes in a Volume Group to a Host](#)
- [Remove a volume from a volume group](#)

Volume groups in PowerStore appliances

A volume group in a PowerStore appliance consists of one or more volumes. A volume can only be a member of one volume group at a time.

To configure a volume group in a PowerStore appliance use the **Volume Groups** page in the PowerStore Manager. You can perform the following operations from this page:

- Create a volume group.
- Modify properties for the volume group, including whether write order consistency is enabled for the volumes in the volume group.
- Delete a volume group.
- Modify the performance policy of a volume group.
- Migrate a volume group to a different appliance.
- Add a volume group to or delete a volume group from the dashboard watchlist.
- Restore from a snapshot.
- Assign or unassign a protection policy.
- Create a thin clone of the volume group.
- Refresh content from a related volume group.

To monitor the capacity, performance, protection status, and members of a volume group, click the name of the volume group you want to view. For performance, you can view an aggregation of metrics across the volume group. For protection, you can perform snapshot operations, monitor and manage replication, and manage the protection policy.

 **NOTE:** Once you assign a protection policy to a volume group, it cannot be changed at the member level.

Create a volume group

Prerequisites

All members of a volume group must be hosted from a single appliance.

Steps

1. Under **Storage**, select **Volume Groups**.

2. Click **Create**.

3. On the **Create Volume Group** slide-out panel, enter the name of the volume group. Optionally enter a description and choose a protection policy to apply to all volumes within the volume group.

i **NOTE:** If you apply a protection policy to the volume group, you cannot override the protection for individual volumes within the group. If you anticipate that member volumes might require different protection policies, consider removing these volumes from the group or creating a separate group for them.

4. To ensure consistent protection across all members of the volume group, select **Apply write order consistency to all volumes in this volume group**.

This setting means that local and remote protection holds all writes on members of the volume group to provide a uniform point-in-time copy across all members. Making a volume group write-order-consistent ensures that the write order is preserved among members when volume group snapshots are taken or when the volume group is replicated.

5. Click **Create**.

Add existing volumes to a volume group

About this task

The volume that you are adding to the volume group must be on the same appliance as other members.

If a volume group does not have a protection policy and is not write-order-consistent, you can add a volume that has a protection policy to that volume group.

However, be aware of some restrictions that apply when adding existing volumes to volume groups:

- If the volume group has a protection policy, the volume that you are adding cannot have a protection policy already in place.
- If the volume group has a protection policy and is write-order-consistent, you cannot add a volume that has a protection policy to that volume group .
- If you add a volume to volume group that has existing snapshots, you cannot use those volume group snapshots for refresh or restore operations.
 - If you must restore or refresh the volume group from a snapshot that was taken before the new volume was added, you must remove the new volume.
 - Restore and refresh operations require that the volume group membership match the membership that existed when the snapshot was taken.

Steps

1. Under **Storage**, select **Volume Groups**.

2. Click the check box next to the volume group to which you want to add volumes.

3. Select **More Actions > Add Existing Volumes**.

i **NOTE:** You can also open the **Add Existing Volumes** slide-out panel via the **Members** tab of the volume group.

4. From the **Add Existing Volumes** slide-out panel, select the volumes to add to the group.

5. Click **Apply**.

i **NOTE:** When you add volumes to a volume group or change the size of the volume group during an asynchronous replication session, the changes do not immediately appear on the destination. You can either perform a manual synchronization or wait until the synchronization occurs based on the RPO.

Add new volumes to a volume group

Steps

1. Under **Storage**, select **Volume Groups**.
2. Click the check box next to the volume group to which you want to add volumes.
3. Select **More Actions > Add New Volumes**.
 - NOTE:** You can also open the **Create Volumes for Volume Group** slide-out panel via the **Members** tab of the volume group.
4. Enter the volume information in the **Create Volumes for Volume Group** slide-out panel:
 - **Name (or Prefix):** When you create a single volume, this name is the name of the volume. When you create multiple volumes, this name is the base name to which a number is appended.
 - **Quantity:** You can add up to 100 volumes that have the same properties. The system appends the volume name with a number when creating multiple volumes.
 - **Size:** The size is the quantity of storage that is subscribed for the volume. After you create the volume, you can increase its size but not decrease it. PowerStore supports the creation of thin volumes up to 256 TB in size.
 - **Volume Protection Policy** (optional): Select a protection policy that contains snapshot and replication rules applicable for the volume. You can add a protection policy after creating the volume.
 - NOTE:** You cannot assign a protection policy to a volume if it is added to a volume group with an assigned policy. You can assign a policy to a volume group with no assigned policy. In that case, the new volume will not be protected at the volume group level.
 - **Volume Performance Policy:** Limit I/O throughput and bandwidth to provide more predictable performance. You can select or create a Performance Policy consistent with the I/O priority (High, Medium, or Low).
 - **Available Hosts/ Host Groups** (optional): Select the hosts/host groups that can access the volume. When you connect the volume to a host/host group, you can specify a Logical Unit Number. If a Logical Unit Number is not specified, the system assigns one by default. You can add the host/host group after creating the volume.
 - NOTE:** When you add volumes to a volume group or change the size of the volume group during an asynchronous replication session, the changes do not immediately appear on the destination. You can either perform a manual synchronization or wait until the synchronization occurs based on the RPO.
5. Click **Create**.

Map Volumes in a Volume Group to a Host

About this task

You can map multiple volume that are members of a volume group to a host or host group.

- NOTE:** Mapping a host to a volume group is enabled for convenience. The mapping is performed for the individual volumes within the group and not to the volume group object itself.

The following restrictions apply:

- After a volume is mapped to a host, it shares the same storage protocol (SCSI or NVMe) as the host to which it is mapped.
- Mixed protocols are not supported.

Steps

1. From **Storage > Volume Groups**, check the box next to the volume group that you want to map to a host.
 - NOTE:** mapping can be done only for one volume group at a time.
2. Select **Provision > Map** to open the **Map Hosts** slide-out panel.
3. Select any hosts that you want the volume group to be mapped to.
4. Click **Apply**.

Remove a volume from a volume group

You can remove a volume from an existing volume group. Removing a volume from a volume group can affect future operations on that volume and volume group.

About this task

These affected operations can include refresh, restore, and deletion operations as well as applying and deleting protection policies.

Be aware of some conditions that apply when removing volumes from volume groups:

- The volume retains the protection policy of the volume group from which it is removed.
- You cannot delete the volume that you removed from the volume group until all the volume group snapshots that were taken when the volume was a part of the group are either expired or deleted.
- When you remove a volume from a volume group that has a protection policy with a replication rule, the volume retains that policy but is not compliant until the volume group is synchronized with the destination.
 - When the volume group is synchronized to the destination, the membership change is applied to the destination volume group.
- If you remove a volume from volume group that has existing snapshots, you cannot use those volume group snapshots for refresh or restore operations.
 - If you need to restore or refresh the volume group from a snapshot that was taken before the volume was removed, you must add the volume back to the volume group.
 - Restore and refresh operations require that the volume group membership match the membership that existed when the snapshot was taken.

Steps

1. Under **Storage**, select **Volume groups**.
2. On the **Volume Groups** page, click the name of the volume group from which you want to remove the volume.
3. Click the **Members** tab, and then click the check box for the name of the volume that you want to remove.
4. Click **More Actions > Remove**.

Hosts and host group configurations

Host configurations are logical connections through which hosts or applications can access storage resources. Before a host can access storage, you must define a configuration for the host and associate it with a storage resource.

You can pool individual hosts together into a host group. A host group is a collection of hosts that enables you to perform volume-related operations across all the hosts in the group. For example, when you provision volumes for a host group, the volumes become available to all member hosts. A host group uses an iSCSI or Fibre Channel connection. It cannot use both.

Under **Compute**, click **Hosts & Host Groups** to perform the following actions:

- Manage hosts and host groups.
- Review the storage resources that are mapped to individual hosts or host groups.
- Review the initiators that are associated with the existing host configurations.
- For host groups, you can also add more hosts.

You can configure host access to volumes, volume groups, and thin clones when you initially create them or, later, from the relevant Details page. Go to one of the following screens:

- If you are creating a storage resource, in the **Create** wizard, go to the **Host Mappings** screen.
- For existing storage resources, select the **Host Mappings** tab on the Details page of the relevant storage resource.

Host group considerations

The following rules apply to host groups:

- A host can belong to one host group only.
- If the host has mapped volumes, you cannot add a host to a host group.
- You cannot add a host to a host group that uses a different protocol.
- A volume can be mapped to multiple host groups.
- An initiator can only be associated with one host or host group.
- When you delete a host from a host group, the associated volumes get detached from the host, and the host becomes a stand-alone host.

Topics:

- [Add a host](#)
- [Add a host group](#)
- [Map volumes to a host or a host group](#)
- [Configure CHAP authentication](#)

Add a host

Prerequisites

Obtain the following information:

- A hostname that you can use as a lookup later.
- Type of host operating system.
- iSCSI initiator IQNs, FC initiator WWNs, and NVMe initiator NQNs for the initiators you want the host to use for accessing storage.

About this task

Before you can map a host to access storage on your cluster, you must define a configuration for it in PowerStore Manager.

Steps

1. Under **Compute**, select **Hosts & Host Groups**.
2. Click **Add Host**.
3. On the **Host Details** page, enter a name for the host and select the operating system.
4. On the **Initiator Type** page, select Fibre Channel, iSCSI, or NVMe.
Review the prerequisites for the host connections.
5. On the **Host Initiators** page, select an initiator from the autodiscovered initiators list.
6. On the **Summary** page, review the host connection details, and click **Add Host**.

Add a host group

Prerequisites

The following rules apply to host groups:

- A host can belong to one host group only.
- If the host has mapped volumes, you cannot add a host to a host group.
- You cannot add a host to a host group that uses a different protocol.
- A volume can belong to multiple host groups.
- A host group can be associated with one initiator.
- When you remove a host from a host group, the associated volumes get detached from the host, and the host becomes a stand-alone host.

Obtain the following information:

- A host group name that you can use as a lookup later.
- Name of the hosts you want to include in the host group.

Steps

1. Under **Compute**, select **Hosts & Host Groups**.
2. Click **Add Host Group**.
3. On the **Add Host Group** page:
 - Enter a name for the host group.
 - Select the protocol.
 - Select the hosts to add to the group.
4. Click **Create**.

Map volumes to a host or a host group

You can map volumes to a single host or to a host group.

About this task

The following restrictions apply:

- After a volume is mapped to a host, it shares the same storage protocol (SCSI or NVMe) as the host to which it is mapped.
- Mixed protocols are not supported.

Steps

1. From **Compute > Hosts & Host Groups**, check the box next to the host or host group to which you want to map volumes.
2. Select **Provision > Map** to open the **Map Volumes** slide-out panel.
3. Select one or more volumes that you want to be mapped to the host or host group.
4. Select whether to provide a Logical Unit Number or have one generated automatically.
5. Click **Apply**.

Configure CHAP authentication

Challenge Handshake Authentication Protocol (CHAP) authenticates iSCSI initiators (hosts) and targets (volumes and snapshots) to expose iSCSI storage while ensuring a secure, standard storage protocol.

About this task

Without CHAP authentication, any host that is connected to the same IP network as the system iSCSI ports can read from and write to the system. If your system is on a public network, it is strongly recommended that you use CHAP authentication.

NOTE: If you plan to use CHAP authentication, you must set up and enable CHAP authentication before preparing volumes to receive data. If you prepare drives to receive data before you set up and enable CHAP authentication, you could lose access to the volumes.

For more information about CHAP authentication, including the benefits that it provides and details about implementation types, see the context-sensitive help entry in PowerStore Manager.

For in-depth information about how this feature works, see the *PowerStore Security Configuration Guide*.

Steps

1. Select the **Settings** icon, and then select **CHAP** in the **Security** section.
2. Enable CHAP authentication.
Additional configuration details are displayed.
3. Select the type of CHAP implementation to use and click **Apply**.

Data mobility for volumes and volume groups

Start a migration session to move a volume or volume group to a different appliance.

Topics:

- [Migrate storage resources to another appliance](#)
- [Migrate vVols to another appliance](#)

Migrate storage resources to another appliance

Use this feature to move volumes, volume groups, or vVols to another appliance in the cluster without any disruption to host I/O.

About this task

Before removing or shutting down an appliance for service, migrate storage resources to another appliance. When you migrate a volume or volume group, all associated snapshots and thin clones 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: In this release, you can migrate volumes, volume groups, and vVols between appliances within a cluster. File-based storage resources are provisioned and managed only on the primary appliance of a cluster.

You can perform assisted migration or manual migration in PowerStore Manager:

- Assisted migration - In the background, the system periodically monitors storage resource utilization across the appliances. Migration recommendations are generated based on factors such as drive wear, appliance capacity, and health. If you accept a migration recommendation, a migration session gets automatically created.
 - NOTE:** The logical size for a volume that is displayed on the **Assisted Migration Recommendation** screen is different than the actual size of the volume. This issue occurs because the migration recommendation accounts for the migration space of the volume family, which may, if applicable, include clones and snapshots.
- Manual migration - You can choose the storage resources to migrate to another appliance in the cluster.

To manually migrate a volume or volume group to another appliance in your cluster:

NOTE: To manually migrate a vVol, see [Migrate Virtual Volumes to another appliance](#).

Steps


1. Under **Storage**, select **Volumes** or **Volume Groups**.
2. Select the storage resource that you want to migrate.
3. Under **More Actions**, select **Migrate**.
The **Migrate** slide-out panel is displayed.
4. Select an appliance that best meets the requirements for the storage resource that you are migrating.
5. Select **Next**.
A migration session with a status of Pending is created in the background.
6. Select **Finish**.
The migration session is displayed on the **Migration Actions** page, and then the **Required Action for Migration** slide-out panel is displayed.
 - NOTE:** If applicable, rescan the associated host adapters for the associated hosts to ensure that the storage is accessible when the migration is complete.
7. Select **Start Migration**.

If a **Rescan Host** dialog box displayed, select the **Yes, the associated hosts have been rescanned** check box and select **Start Migration** if you have rescanned the associated hosts. If you have not rescanned the associated hosts, rescan them before continuing the migration.

A **Data Migration** dialog box is displayed.

8. To start the migration, select **Migrate Now**.

You can monitor the migration session under **Migration > Internal Migrations**.

 **NOTE:** Depending on the amount of data getting migrated, it may take several minutes, hours, or days to complete the migration. It may also have an impact on the overall system performance.

Migrate vVols to another appliance

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

About this task

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 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.

Thin clones

A thin clone is a read-write copy of a volume, volume group, or snapshot that shares blocks with the parent resource. Data available on the source at the moment of the thin clone creation is immediately available to the thin clone. The thin clone references the source snapshot for this data. However, data resulting from changes to the thin clone after its creation is stored on the thin clone. Changes to the thin clone do not affect the source snapshot.

Advantages of using thin clones

Thin clones allow you to create and manage space-efficient copies of production environments, which is beneficial for the following types of activities:

- Development and test environments - Thin clones allow development and test personnel to work with real workloads and use all data services associated with production storage resources without interfering with production. They also allow development personnel to promote a test thin clone to production.
- Parallel processing - Parallel processing applications that span multiple servers can use multiple thin clones of a single production data set to achieve results more quickly.
- Online backup - You can use thin clones to maintain hot backup copies of production systems. If there is corruption in the production data set, you can immediately resume the read-write workload by using the thin clones.
- System deployment - You can use thin clones to build and deploy templates for identical or near-identical environments. For example, you can create a test template that is thin cloned as needed for predictable testing.

Thin clone restrictions

The following restrictions apply to thin clones:

- After you create a thin clone, the source volume, volume group, or snapshot can be deleted.
- If you move a thin clone, the volume family to which it belongs is also moved.

Topics:

- [Thin clone terminology and hierarchy](#)
- [Create a thin clone of a volume](#)
- [Create a thin clone of a volume group](#)

Thin clone terminology and hierarchy

The snapshots and thin clones for a volume, volume group, or storage container form a hierarchy. This document uses the following terms to describe this hierarchy:

Table 1. Thin clone terminology

Term	Definition
Source	A volume, volume group, or snapshot of a volume or volume group that is used as the source for thin clone create and refresh operations. The source can change when the clone is refreshed.
Base volume, base volume group, base storage container	The founding (production) volume, volume group, or storage container for derivative snapshots and thin clones.
Family	A volume, volume group, or base storage container and all its derivative thin clones and snapshots. This family includes snapshots and thin clones of the storage resource.
Parent	The original parent storage container, volume, volume group or thin clone for the snapshot. This resource does not change when a thin clone is refreshed to a different

Table 1. Thin clone terminology (continued)

Term	Definition
	source snapshot, because the new source snapshot must be in the same base volume, volume group, or storage container family.

For example, suppose the following hierarchy of snapshots and thin clones exists for Volume 1:

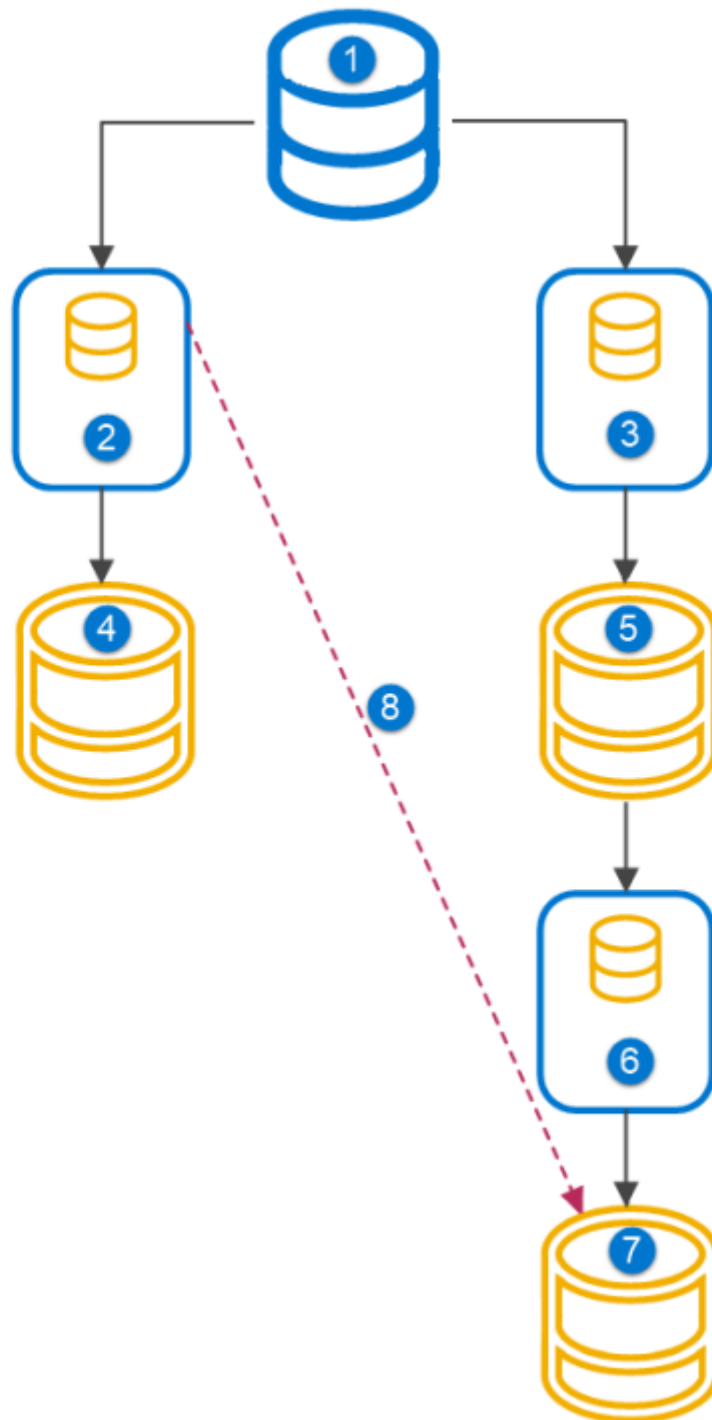


Figure 1. Thin clone hierarchy

- 1. Volume1
- 2. Snapshot 1
- 3. Snapshot 2
- 4. Thin Clone1
- 5. Thin Clone2

6. Snapshot 3
7. Thin Clone3
8. Refresh

The base volume family for Volume 1 includes all the snapshots and thin clones that are shown in the diagram.

For Thin Clone 2:

- The family is Volume 1.
- The parent is Snapshot 2.
- The source is Snapshot 2.

For Thin Clone 3:

- The family is Volume 1.
- The parent is Snapshot 3.
- The source is Snapshot 3.

Now, if Thin Clone 3 is refreshed from Snapshot 1:

- The family is still Volume 1.
- The original parent is Thin Clone 2
- The source has changed from Snapshot 3 to Snapshot 1.

If Thin Clone 2 is deleted after Thin Clone 3 is refreshed, the original parent resource shows as empty.

Create a thin clone of a volume

Steps

1. Under **Storage**, select **Volumes**.
2. Select the volume to thin clone.
3. Select **Repurpose** > **Create Thin Clone Using Volume**.
4. On the **Create Thin Clone** slide-out panel, specify the thin clone information.

Create a thin clone of a volume group

Steps

1. Under **Storage**, select **Volume Groups**.
2. Select the volume group to thin clone.
3. Select **Repurpose** > **Create Thin Clone**.
4. On the **Create Thin Clone** slide-out panel, specify the thin clone information.

Performance policies

A performance policy specifies I/O performance requirements for PowerStore storage resources. PowerStore provides three pre-defined performance policies:

- High
- Medium (default)
- Low

PowerStore has share-based QoS. Share-based QoS means when there is contention at system level, a volume with a high-performance policy services more IOPS than a volume with a medium-performance policy. Further, a volume with a medium-performance policy services more IOPS than one with a low-performance policy.

It is recommended that you associate the high-performance policy with critical applications only. Reserving a high-performance policy for critical applications ensures that those critical applications are not competing for I/O against less-critical applications.

Performance policies for PowerStore T model storage resources

You can assign performance policies to volumes and thin clones when you provision them or modify their configuration.

If you do not explicitly configure a performance policy for a resource, the resource is associated with a Medium performance policy.

Performance policies for PowerStore X model storage resources

The system assigns performance policies to VM volume groups and individual VMs based on their capability profiles in VMware vCenter. It correlates the following VMware performance-based capability profiles to performance policies:

VMware capability profile	PowerStore performance policy
High-Priority performance	High
Medium-Priority performance	Medium
Low-Priority performance	Low

Use vCenter to change the performance policy for VM volume groups and individual VMs.

Topics:

- [Change a performance policy for a volume](#)

Change a performance policy for a volume

Steps

1. Under **Storage**, select **Volumes**.
2. Click the check box next to the relevant volume.
3. Select **More Actions** > **Change Performance Policy**
4. Select the performance policy on the **Change Performance Policy** slide-out panel.