Dell PowerStore

Configuring Volumes

4.1

February 2025
Rev. A05

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

Additional Resources **5**

Chapter 1: Volumes **6**
- Volumes in PowerStore appliances 6
  - Volume and volume group topology 7
  - Volume Capacity 8
- Thin provisioning 9
- Create a volume 9
  - Volumes and applications 10
- Map volumes to a host or host group 11
- Change volume properties 11
- Delete a volume 12
- Recycle Bin for volumes 13
  - Setting the Recycle Bin retention time for deleted objects 13
  - Recover a deleted volume 14
- Assign a protection policy 14
- Change a protection policy for a volume 14
- Unassign a protection policy from a volume 14
- View snapshots column 15

Chapter 2: Volume groups overview **16**
- Volume groups in PowerStore appliances 16
  - Volume Group Capacity 17
- Create a volume group 17
- Add existing volumes to a volume group 18
- Add new volumes to a volume group 18
- Map volumes in a volume group to a host 19
- Remove a volume from a volume group 20
- Recycle Bin for volume groups 20
  - Recover or permanently delete a volume group 21

Chapter 3: Hosts and host group configurations **22**
- Add a host 22
- Add a host group 23
- Map volumes to a host or a host group 23
- Show a list of initiators 24
- Configure CHAP authentication 24

Chapter 4: Data mobility for volumes and volume groups **25**
- Migrate storage resources to another appliance 25
- Migrate vVols to another appliance (advanced) 26
- Migrate vVol-based VMs to another appliance 26

Chapter 5: Thin clones **28**

Thin clone terminology and hierarchy..... 28
Create a thin clone of a volume.....31
Create a thin clone of a volume group.....31

Chapter 6: Quality of Service (QoS) policies..... 32
Quality of Service (QoS) limits..... 33
Create a Quality of Service (QoS) policy and I/O limit rules.....34
Select a different QoS policy.....34
Delete a QoS policy.....34
Modify a QoS policy.....35

Chapter 7: Performance policies.....36
Change a performance policy for a volume..... 36

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

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, NVMe-over-Fibre Channel, and NVMe-over-TCP 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 or host group
- Change volume properties
- Delete a volume
- Recycle Bin for volumes
- Assign a protection policy
- Change a protection policy for a volume
- Unassign a protection policy from a volume
- View snapshots column

Volumes in PowerStore appliances

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

- Create a volume.
  - Associate a specific application with a volume.

    NOTE: In PowerStore 2.1, this step is required when creating a volume. You can change the category of application and specific application at any time later.

  - Optionally, you can associate the volume with a volume group and with a host or host group.
- Modify volume properties.
- Delete a volume after unmapping the volume from any hosts; recover a volume from the recycle bin if wanted.
- Expand the volume size.
- Modify the performance policy of a volume.
- Assign, unassign, and modify the QoS policy of a volume.
- Migrate a volume to a different appliance.
- Add a volume to or delete a volume from the dashboard watchlist.
- Map or unmap a volume to a host.
- Assign or unassign a protection policy.
- Restore content from a snapshot.
- Gather support materials.
- Create a thin clone of a volume.
- Refresh content from a related volume.
- Enable a Metro configuration for a volume.

To monitor the capacity, performance, alerts, protection status, and host mapping of a volume, click the name of the volume you want to view. In addition, the **Virtual Machine** tab displays all virtual machines that are associated with the volume.

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, although you can select the appliance from the drop-down list. If the Resource Balancer is choosing a default appliance, it does not choose a volume that has been mapped to a specific host or host group. In such cases, the volume is created only on an appliance that sees this host or 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.

Volume and volume group topology

PowerStore enables you to see a graphical display of your block storage topology. This topology displays volumes, volume groups, clones, snapshots, and snapshot containers, enabling you to see the specific relationships among the storage objects in your environment.

The topology is initially shown in a tree-like layout. You can expand and collapse each object to view details about the object and its relationship to other objects in the storage environment. These changes are saved to user preferences and can be reverted to the default display by clicking **Reset**.

As new objects are added, you can click the **Refresh Topology** button, represented by the curved arrow icon, to see the updated topology.

Using the **View Topology** function, you can perform the following actions:

- Collapse or expand the view of the topology.
- Display the members of a volume group.
- Change the topology by dragging objects to the place you choose.
- Search for storage objects by name.
- Display information about volumes, volume groups, and clones:
  - Details: Shows the type, family ID, storage protocol used, and so on
  - Capacity: Shows the amount of space that is provisioned locally, the amount of space provisioned for the family, and so on
  - Mapped hosts: Shows all hosts to which the storage object is mapped
- Display information about the snapshots and snapshot containers that are associated with each storage object.

NOTE: Scheduled snapshots do not appear in the topology view unless they are used to create clones.

View volume topology

PowerStore Manager enables you to see an expandable and collapsible diagram of your environment to understand the logical relationships between objects.

Steps

1. Go to **Storage** > **Volumes**.
2. On the **Volumes** page, click the **More Actions** drop-down menu and select **View Topology**.
3. (Optional) Click a specific object to see more information about it in the **Details** panel.

NOTE: If you have a large hierarchy of storage objects, you can use the **Name Search** field to look for a specific object by name. The search field is case-insensitive.

Volume Capacity

You can view capacity metrics for individual volumes from **Storage** > **Volumes** > **[volume]** > **Capacity**.

Collection frequency and retention periods

Capacity metrics are collected at 5 minute intervals and rolled up to 1 hour and 1 day aggregates. The data is retained as follows:

- 5 minute data is retained for 1 day.
- 1 hour data is retained for 30 days
- 24 hour data is retained for 2 years.

Usage

The **Usage** area displays the current capacity and data efficiency metrics for the volume.

NOTE: PowerStore Manager displays all capacities in base 2 by default. Hovering over the Percentage Used, Free, and Provisioned values at the top of Capacity tab displays a tooltip that shows the values in both base 2 and base 10. For more information, see Dell Knowledge Base Article 000188491: PowerStore: How PowerStore physical capacity is calculated.

Table 1. Current volume capacity metrics

Metric	Description
Used	Amount of data that is written to the volume. The doughnut chart displays the Used metric as a percentage of the total provisioned capacity. **NOTE:** This metric does not include space saving from data sharing within the volume family or data reduction.
Free	Amount of data can be written to the volume.
Thin Savings	The ratio of logical space provisioned for the volume family to logical space used by the volume family. This value shows the space savings that are achieved by using thin provisioning.
Snap Savings	The ratio is calculated by dividing the capacity that would have been required for fully provisioned copies of a volume or clone by the actual capacity that is used by the snapshots and clones of the primary volume or clone. This calculation shows the efficiency that is gained by using snapshots and clones. It does not include data reduction savings.
Snapshot/Thin Clone Space	Amount of data that is written to snapshots and clones of this volume.
Volume Family Unique Data	Physical space that is used by the volume family after deduplication and data sharing savings are applied. This metric is useful for determining the amount of space that is freed if the primary volume and any clones are deleted.

Historical Usage

The **Historical Usage** area displays the capacity metrics for the selected time period.

Table 2. Historical volume capacity metrics

Metric	Description
Provisioned	Total amount of data can be written to a volume as it was created.
Used	Amount of data that is written to the volume.

The **Historical Usage** chart shows the date and time along the x-axis against the usage along the y-axis. To interact with this chart:

- Select the time period.
- Hover over a data point in the chart to display the metric value at that point-in-time.
- Zoom in on a time period by moving the ends of the line chart. Click **Reset zoom** to reset the chart.

- Print or download the data from the chart by selecting an option on the chart menu. This is located on the top-right corner of the chart.

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, NVMe/FC, and NVMe/TCP), and initiator to use.

NOTE: If you plan to use volumes in a volume group, it is recommended that you create the volume group first. Then you can add volumes to the group.

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 and then want to add existing volumes to a volume group, you must first migrate them to the same appliance.

If you want to enable Metro protection for a volume, you must first create the volume and then enable that volume for a Metro cluster. Metro clusters provide enhanced availability and disaster avoidance, resource balancing across data centers, and storage migration.

Steps

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

   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.

- **Category:** Select a category from the drop-down menu for the type of application that you want to associate with the volume. You can select **Boot Volume**, **Business Applications**, **Relational Databases**, and so on.

  NOTE: Selecting a Category for the application is required in PowerStore Manager 2.1 and later. This field cannot be left blank.

  Creating a boot volume allows you to create a volume that you want to attach directly to a host without having to create another set of initiators. You can see a list of boot volumes that are attached to a host by going to **Compute** > **Host Information** and selecting a host from the list.

  NOTE: If you selected **Boot Volume** and the host initiator type is iSCSI, you must manually specify the LUN ID.

  You can select **Other** if the categories in the drop-down menu do not match the type of application that you are using. After you select **Other**, type the application name in the **Application** field.
- **Application:** Select the application from the drop-down menu.

  NOTE: Selecting an application is required in PowerStore Manager 2.1. This field cannot be left blank.

  If you do not see the application that you want in the drop-down menu, you can type it into the **Application** field. You can manually enter the name of an application whether you choose one of the selections under **Category** or select **Other**, from the drop-down menu. The maximum number of characters is 32.
- **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 that 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.
- **QoS Policy** (optional): Select a QoS policy to set maximum limits on IOPS or bandwidth, or both, on 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 or host groups that can access the volume. The radio buttons to select the protocol only appear if the storage protocol has not been set.

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

  When you connect the volume to the hosts or host groups, you can specify a Logical Unit Number. The Logical Unit Number panel appears only if you select SCSI for the host. If a Logical Unit Number is not specified, the system assigns one by default. You can add hosts or host groups after creating the volume.

Volumes and applications

You can specify how a volume is used by associating an application with it when you create the volume. You can also modify existing volumes to specify an application for them.

When you create a volume, you must specify the **Category** and the **Application** that is associated with that volume.

You can click the column icon to display the Application column on the **Storage** page in PowerStore Manager. This column shows which application, if any, that a volume is associated with.

NOTE: You can bypass the **Category** and **Application** requirements by creating the volume using REST API. You can also modify a volume through REST API. For more information, see PowerStore REST API Reference Guide.

If the **Category** drop-down menu does not include the type of application that you want to associate with the volume, you can select **Other**. Selecting **Other** prompts a blank field to appear under Application; you can type the name of the application there. The maximum number of characters is 32.

NOTE: Volumes created in PowerStore before PowerStoreOS version 5.2 do not have application types that are associated with them. You can add application types to these pre-5.2 volumes or leave them as is.

Volume groups

You can see the application type that is associated with each volume in the **Volumes** list, **Volume Groups** list, and the **Host** list.

Nondisruptive upgrades

Volumes created in PowerStore before PowerStoreOS version 5.2 do not have application types that are associated with them. You can add application types to these pre-5.2 volumes or leave them as is.

Clones

Clones inherit the **Category** and the **Application** types of their source volumes.

Snapshots

Snapshots do not inherit the **Category** and the **Application** types of their source volumes.

Map volumes to a host or host group

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 either **SCSI (Supports iSCSI or FC transport layer)** or **NVMe (Supports NVMe FC transport layer)** as the protocol that you want to use to map the volume or volumes.
4. Select any hosts or host groups that you want the volume to be mapped to.
5. 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

You can delete a volume, volumes, or volume group, an operation that places them in the Recycle Bin. You can also delete these objects permanently rather than moving them to the Recycle Bin.

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 you 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 does not have a secure snapshot that is associated with it.

  Volumes that have secure snapshots cannot be deleted.

- The volume is not involved in a migration.

Steps

1. Under **Storage**, select **Volumes**.
2. Click the check box next to the volume that you want to delete.

   You can delete multiple volumes by checking all the volumes that you want to delete.
3. Under **More Actions**, select **Delete**.
4. In the **Delete Volume** window, Select **Delete**

   You can click the **Skip Recycle Bin and permanently delete** check box to permanently delete the volume. Otherwise, the volume is sent to the Recycle Bin. Deleted volumes remain in the Recycle Bin for a default period of 7 days, after which the volumes are permanently deleted.

NOTE: You can manually change the retention period for the Recycle Bin.

Recycle Bin for volumes

PowerStore Manager includes a Recycle Bin allows you to recover intentionally or accidentally deleted volumes. No storage is reclaimed until the object is deleted permanently from the system.

You can set a system-wide retention period for deleted objects. After that period, the objects are permanently deleted. When deleting an object, you can either delete that object and have it placed in the Recycle Bin, or delete it permanently.

NOTE: The Recycle Bin works only for block storage. It does not support file-based volumes and vVols.

If you put a volume or volume group in the Recycle Bin as opposed to permanently deleting the object, those objects must meet the following conditions:

- The volume has no protection policies that are associated with it.
- The volume has no secure snapshots.
- The volume has no mappings.
- The volume is in a healthy state.
- Fast metrics have been disabled, if applicable.

Retention period

The default retention period for deleted objects is 7 days. You can adjust the retention period manually.

Snapshots and clones

When you delete a volume, all associated local snapshots and clones are also deleted.

NOTE: If the volume has remote snapshots, deleting the volume does not affect those remote snapshots.

When you recover a volume, all associated local snapshots and clones are also recovered.

Setting the Recycle Bin retention time for deleted objects

You can customize the number of days that volumes and volume groups are kept in the Recycle Bin. You change this setting at the cluster level.

About this task

When the chosen retention time expires, volumes and volume groups in the Recycle Bin are permanently deleted and cannot be recovered.

Steps

1. In the PowerStore Manager **Dashboard**, click **Settings**.
2. Select **Recycle Bin** in the **Cluster** section.
3. Enter the number of days in the **Expiration Duration** field.

   NOTE: Deleted objects retain their original expiration time even if you change the global retention time. For example, you delete a volume and allow it to be placed in the Recycle Bin with an **Expiration Duration** of 7 days. That volume is deleted after 7 days, even if you change the global **Expiration Duration** policy to 30 days.

Recover a deleted volume

You can recover a delete volume or volumes from the Recycle Bin before those objects are permanently deleted.

Steps

1. Under **Storage**, select **Recycle Bin**.
2. Select the **Volumes** tab.
3. Click the checkbox next to the name of the volume or volumes that you want to restore and click **Recover**.
   You can also click **Expire Now** to permanently delete any volumes that you do not want to keep.

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 policy that is assigned to the volume group protects that volume and cannot be changed at the volume level.

About this task

You can assign a protection policy to multiple volumes at the same time.

Steps

1. Under **Storage**, select **Volumes**.
2. Click the check box next to the relevant volume or volumes.
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

Unassigning a protection policy from a volume removes local protection, remote protection, or both from that volume.

About this task

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

- Scheduled snapshots and replication that is based on the policy rules stop.
- Existing snapshots remain and are retained in the system.

  Snapshot retention is based on the snapshot rule settings that are applied at the time of creation.

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

You can unassign a protection policy from multiple volumes simultaneously.

Steps

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

View snapshots column

PowerStore Manager enables you to see snapshots that have been taken of a storage object and a table view of these snapshots. This quick access to snapshots helps you to restore an object to its previous state.

About this task

The Snapshots column is not visible by default in PowerStore Manager. The column can be made visible for block storage, file storage, and virtual machines. You can find the Snapshots column on the following pages:

- **Storage** > **Volumes**
- **Storage** > **Volume Groups**
- **Storage** > **File Systems**
- **Compute** > **Virtual Machines**

Steps

1. Click the **Show/Hide Table Columns** icon on the right.
2. Scroll down and click the Snapshots checkbox.
   The number of snapshots is displayed for that storage object as a clickable element.
3. (Optional) Click the number in the snapshots column to go to the **Snapshots** page for that storage object.

2

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
- Recycle Bin for volume groups

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.
- Assign, unassign, or modify a QoS policy.
- Create a thin clone of the volume group.
- Refresh content from a related volume group.
- Gather support materials for a volume group.
- Add existing volumes to a volume group.
- Add new volumes to a volume group.
- Map or unmap a host or host 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.

Volume Group Capacity

You can view the capacity metrics for a volume group from the **Storage** > **volume groups** > **[volume group]** > **Capacity** card.

Collection frequency and retention periods

Capacity metrics for volume groups are collected every 5 minutes, and rolled up to 1-hour and 24-hour aggregates.

- 5-minute data is retained for 1 day.
- 1-hour data is retained for 30 days.
- 24-hour data is retained for 2 years.

Usage

The **Usage** area displays the current capacity metrics for the volume group.

NOTE: PowerStore Manager displays all capacities in base 2 by default. Hover over the Percentage Used, Free, and Provisioned values at the top of Capacity tab to display a tooltip that shows the values in both base 2 and base 10. For more information, see Dell Knowledge Base Article 000188491: PowerStore: How PowerStore physical capacity is calculated.

Table 3. Current volume group capacity metrics

Metric	Description
Used	Amount of data that is written to the volumes in the volume group. The doughnut chart displays the Used metric as a percentage of the total provisioned capacity.
Free	Amount of data that can be written to the volume group.

Historical Usage

The **Historical Usage** area displays the capacity metrics for the selected time period.

Table 4. Historical volume group capacity metrics

Metric	Description
Provisioned	Total amount of data that can be written to volumes in the volume group.
Used	Amount of data that is written to the volumes in the volume group.

The **Historical Usage** chart shows the date and time along the x-axis against the usage along the y-axis. To interact with this chart:

- Select the time period.
- Hover over a data point in the chart to display the metric value at that point-in-time.
- Zoom in on a time period by moving the ends of the line chart. Click **Reset zoom** to reset the chart.
- Print or download the data from the chart by selecting an option on the chart menu. This is located on the top-right corner of the chart.

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 QoS policy and a protection policy to apply to all volumes within the volume group.

   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**.

   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**.

   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 using 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.

   - **QoS Policy:** Select a QoS policy to set maximum limits on IOPS or bandwidth, or both, on the volume.
   - **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

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

About this task

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.

NOTE: You can only map volume groups that contain 50 or fewer member volumes. Use the **Members** tab on the volume group's page to map the volumes in batches of 50 or less.

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 must 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**.

Recycle Bin for volume groups

PowerStore Manager includes a Recycle Bin allows you to recover intentionally or accidentally deleted volume groups. No storage is reclaimed until the object is deleted permanently from the system.

You can set a system-wide retention period for deleted objects. After that period, the objects are permanently deleted. When deleting an object, you can either delete that object and have it placed in the Recycle Bin, or delete it permanently.

NOTE: The Recycle Bin works only for block storage. It does not support file-based volumes and vVols.

If you put a volume group in the Recycle Bin as opposed to permanently deleting the object, those objects must meet the following conditions:

- The volume group has no protection policies that are associated with it.
- The volume group members do not have secure snapshots.
- The volume group has no mappings.
- The members of the volume group must be in a healthy state.

Retention period

The default retention period for deleted items is 7 days. You can adjust the retention period manually.

Snapshots and clones

When you delete a volume group, all associated snapshots and clones are also deleted.

NOTE: If the volume group has remote snapshots, deleting that volume group does not affect those remote snapshots.

When you recover a volume group, all associated snapshots and clones are also recovered.

Recover or permanently delete a volume group

You can recover a delete volume group or groups from the Recycle Bin before those objects are permanently deleted.

Steps

1. Under **Storage**, select **Recycle Bin**.
2. Select the **Volume Groups** tab.
3. Select the volume group or groups that you want to recover and click **Recover**, or click **Expire Now** to permanently delete the objects .

3

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 Information** 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
- Show a list of initiators
- 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 nonqualified names (NQNs) for the initiators that 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 **Host Information**.
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 (FC), iSCSI, NVMe, or NVMe vVol.

   NOTE: You can use FC and iSCSI initiators with traditional datastores and vVols. You can use NVMe initiators only if you are working with traditional datastores. If you are working with vVols, you must select NVMe vVol as the initiator type.

   Review the prerequisites for the host connections.
5. On the **Host Initiators** page, select an initiator from the autodiscovered initiators list.
6. If the host operating system is ESXi, select the type of host connectivity on the **Host Connectivity** page.

   If you selected **Metro Connectivity**, select the Metro connectivity option for the ESXi host.

   NOTE: Metro connectivity is only available for ESXi hosts.
7. 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 **Host Information**.
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** > **Host Information**, 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**.

Show a list of initiators

You can display a list of all initiators and their protocol type as well as host and active session information.

About this task

The information that is displayed on the Initiators page includes the following:

- The initiator identifier
- The protocol that the initiator uses
- The associated host or hosts
- The number of active sessions on the initiator

You can also display the connected paths and see performance metrics for each initiator, including latency.

Steps

1. Go to **Compute** > **Host Information**.
2. On the **Host Information** page, click the **Initiators** tab.
3. (Optional) Click an individual initiator to see its connected path information and performance metrics.

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 **iSCSI 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**.

4

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 (advanced)
- Migrate vVol-based VMs 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 the amount of data being migrated. This work space is released and freed up after the migration is complete.

For more information about nondisruptively migrating storage resources, see KB 000105896.

NOTE: You can migrate volumes, volume groups, and vVols between appliances within a cluster. However, 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 is 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 logical size is different because the migration recommendation accounts for the migration space of the volume family, which may 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 by selecting the **Migrations** tab on the **Internal Migrations** page.

   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 (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.

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.

5

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 5. 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 used 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 5. 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:

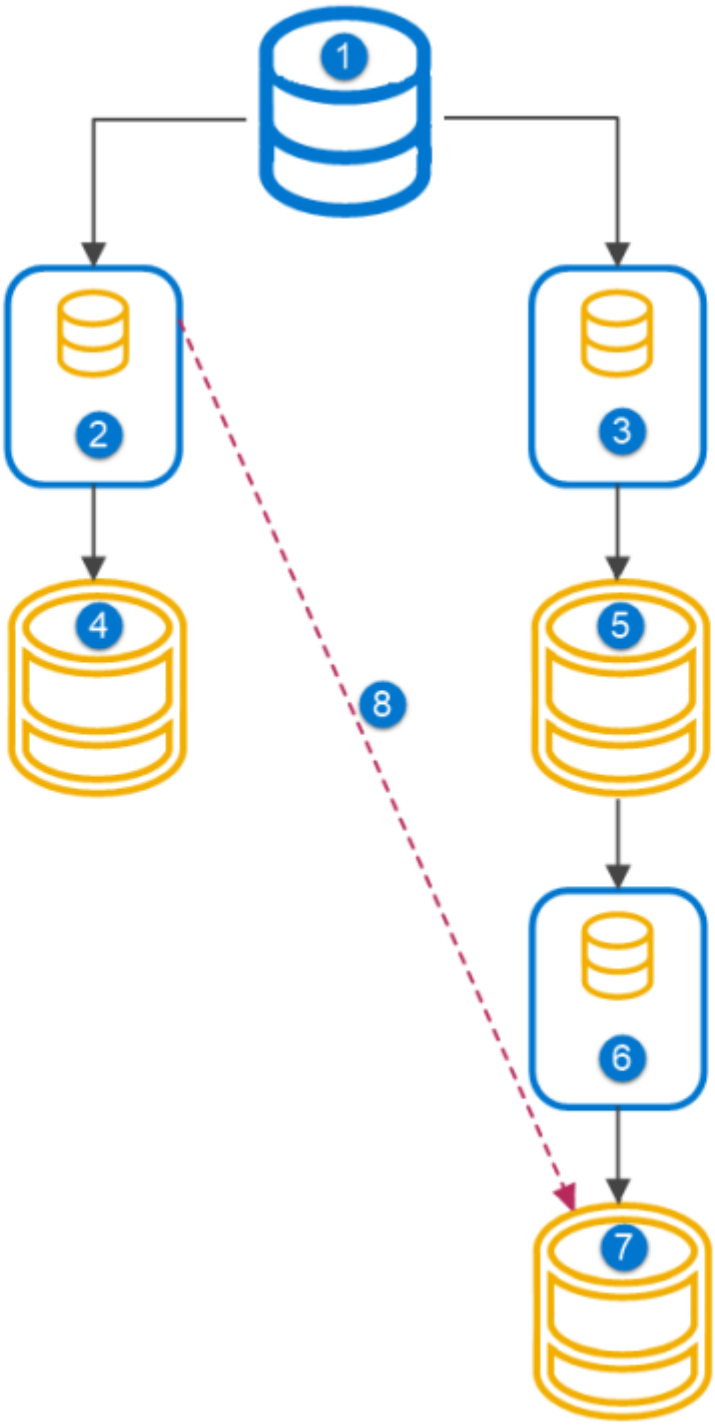

Figure 1. Thin clone hierarchy

1. Volume1
2. Snapshot 1
3. Snapshot 2
4. Thin Clone 1
5. Thin Clone 2

6. Snapshot 3
7. Thin Clone 3
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.
5. (Optional) Select the host or host group to which you want to map the thin clone.
6. Click **Clone**.

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.

6

Quality of Service (QoS) policies

You can apply QoS policies to set maximum limits on I/O for volumes and volume groups. These policies to ensure that critical applications get priority over other workloads and provide predictable performance for each application.

Maximum limits are enforced only from I/O that arrives from an external host. These limits are not enforced on internal synchronous or asynchronous replication or migration.

QoS policies are interoperable with existing performance policies.

You can apply QoS policies to the following:

- Volumes: Set an IOPS or bandwidth limit on a single volume.
- Volume groups: Set an IOPS or bandwidth limit to be shared with all volumes in a volume group. If a policy is assigned to a volume group, you cannot assign a policy to an individual volume.

NOTE: If you remove a volume from a volume group, that removed volume does not inherit a QoS policy that has been assigned to the group.

You can apply a QoS policy to a resource at any time. However, you can apply only one QoS policy to a volume or volume group.

NOTE: When you delete a volume from a volume group, that volume does not inherit the QoS policy that is assigned to the volume group.

QoS policies allow you to limit the following:

- Maximum IOPS: This value specifies the maximum number of I/O operations per second.
- Maximum bandwidth: This value specifies the maximum number of KB per second.

NOTE: You can set limits for the maximum IOPS or maximum bandwidth, or both. If both are selected, the system limits traffic according to which limit is reached first.

Supported limits

You can assign up to 100 QoS policies for each cluster.

Considerations

QoS is a performance-limiting feature. If an I/O rule for a resource has a limit that is too low, performance issues can result.

I/O limit rules

There are two types of limits that you can apply with I/O rules:

- Absolute limit: This limit is defined as the maximum number of IOPS a resource is allowed to complete regardless of its size.
- Density-based limit: This limit is based on the size of the resource and changes in proportion to the size of the provisioned resource.

NOTE: For density-based limits, the max IOPS and max bandwidth are based on the amount of provisioned GB that the resource has.

Burst

You can select a burst setting for a QoS policy. The Burst option allows traffic to exceed the maximum IOPS or bandwidth limit by a percentage of that limit for a few seconds. Valid percentage values are 1 to 100. A burst setting of 0 means that the feature is disabled.

To use the burst setting, you must accumulate burst credits. You accumulate burst credits when the resource operates below the I/O limit. The resource can keep exceeding the limit until all credits are used.

For example, assume you have a 10,000 IOPS limit and a 20% burst setting. The resource operates below its IOPS limit for a certain period, allowing you to accumulate 2,000 credits. If IOPS exceeds the 10,000 limit, the burst setting enables the resource to use those credits to allow increased traffic.

NOTE: A host can consume the available credits even if no burst value has been set.

When a volume or volume group is associated with a QoS policy that has a density-based I/O limit, the burst limits are updated if the volume is resized or the volume group has members that are added or removed.

NOTE: If a resource consistently tries to exceed a defined limit, the burst setting is not applied.

Migration

If a volume or volume group is migrated, any associated QoS policy is migrated along with that resource.

Metro volumes

If you assign a QoS policy to a metro volume, that policy is not automatically copied to the peer cluster. You can assign QoS policies independently to metro volumes on the source or destination.

If you want to assign a QoS policy to a metro volume, it is recommended that you apply the policy to the local and remote sides.

You can unassign a QoS policy at either end of a metro volume.

Topics:

- Quality of Service (QoS) limits
- Create a Quality of Service (QoS) policy and I/O limit rules
- Select a different QoS policy
- Delete a QoS policy
- Modify a QoS policy

Quality of Service (QoS) limits

With maximum limits, you specify what the maximum number of sustained IOPS or bandwidth is allowed over time. Maximum limits apply only to I/O from external hosts. These limits do not apply to internal asynchronous or synchronous replication operations or migration I/O.

Limits to number of policies

Each volume or volume group can be associated with only one QoS policy.

On a cluster level, there is a limit of 100 QoS policies for each cluster. However, there can be 1000 QoS associations for volumes and volume groups within a cluster.

If a QoS policy is assigned to a volume group, you cannot assign a different QoS policy to a volume within that group.

Create a Quality of Service (QoS) policy and I/O limit rules

You can create a QoS policy and I/O limit rules to apply to volumes and volume groups that have already been created.

Steps

1. Under **Storage**, click **QoS**.
2. On the **QoS Policies** page, click **Create**.
3. On the **Create a QoS Policy** slide-out panel, enter a name for the QoS policy and, optionally, a description of the policy.
4. Click **Create** to create an I/O limit rule.
5. On the **Create IO Limit Rule** slide-out panel, enter a name for the I/O limit rule.
6. Click the **Absolute Limit** radio button or the **Density-base Limit** radio button.
   - Click the **Absolute Limit** radio button if you want the maximum IOPS per GB or maximum bandwidth per GB to be a fixed value.
   - Click the **Density-based Limit** radio button if you want the limit to change in proportion to the capacity of the volume or volume group.
7. If you want to include a burst, enter a percentage in the **Burst** field.

   The burst setting is an option that allows traffic to exceed the maximum IOPS or bandwidth limit. When a burst is enabled, the traffic can exceed that limit by a designated percentage for a few seconds.
8. Click **Create**.

Select a different QoS policy

You can select a different QoS policy for the volume or volume group than the policy that was originally applied. You can also add a QoS policy to an existing volume or volume group.

Prerequisites

The QoS policy must exist.

Steps

1. Under **Storage**, select **Volumes**.
2. Check the box to select a volume from the list of volumes.
3. Click **More Actions** > **Change QoS Policy**.
4. In the **Change QoS Policy** slide-out panel, select the QoS policy that you want to apply to the volume from the drop-down menu.

   To remove a QoS policy from a volume, select **None**.
5. Click **Apply**.

Delete a QoS policy

You can delete a QoS policy that is no longer useful. A QoS policy can be deleted only if it is not assigned to a volume or volume group.

Steps

1. Under **Storage**, select **QoS**.
2. On the **QoS Policies** page, click the check box next to the QoS policy that you want to delete.
3. Click **More Actions** > **Delete**.
4. In the **Delete QoS Polices** dialog, click **Delete**.

Modify a QoS policy

You can modify a QoS policy to change its values and select a different I/O limit rule.

Steps

1. Under **Storage**, select **QoS**.
2. On the **QoS Policies** page, click the check box next to the QoS policy that you want to modify.
3. Click **Modify**.
4. In the **Modify QoS Policy** slide-out panel, select which policy attribute that you want to change; you can also add an I/O limit rule or select a different rule.
5. Click **Apply**.

7

Performance policies

A performance policy specifies I/O performance requirements for PowerStore storage resources.

PowerStore provides three predefined performance policies:

- High
- Medium (default)
- Low

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 storage resources

You can assign performance policies to volumes, volume groups, 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.

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.