Dell PowerStore: Snapshots and Thin Clones

July 2022

H18156.5

White Paper

Abstract

This white paper provides an overview of the snapshot and thin clone features of Dell PowerStore, including information about the underlying structures and management methods.

Dell Technologies

Copyright

Contents

Executive summary

Overview

As data becomes increasingly important to organizations of all types, these organizations continually strive to find the safest and most effective ways to protect their data. While many methods of data protection exist, one of the simplest and most-effective methods involves using snapshots. Snapshots allow recovery of data by rolling back to an older point-in-time or copying select data from the snapshot. Snapshots continue to be an essential data-protection mechanism that is used across a wide variety of industries and use cases. Snapshots can preserve the most important mission-critical production data, sometimes with other data-protection technologies.

Dell PowerStore provides a simple but powerful approach to local data protection using snapshots. PowerStore uses the same snapshot technology across all the resources within the system, including volumes, volume groups, file systems, virtual machines, and thin clones. Snapshots use thin, redirect-on-write technology to ensure that system space is used optimally and reduces the management burden by never requiring administrators to designate protection space. Snapshots can be created manually through PowerStore Manager, PowerStore CLI, REST API, or automatically using protection policies. Protection policies can be created and assigned to quickly create local and remote protection on supported resources.

A thin clone is a read/write copy of a volume, volume group, NAS server, or file system. Thin clones use the same underlying pointer-based technology that snapshots use to create multiple copies of storage resources. Thin clones support many data services, which engineers and developers can leverage in their environments. When users create a thin clone, it acts as a regular resource and is listed with the other resources of the system. Like snapshots, users can create, manage, and destroy thin clones through PowerStore Manager, PowerStore CLI, and REST API.

Ansible Modules are available for PowerStore which allows data center and IT administrators to automate and orchestrate the configuration and management of PowerStore appliances. The Ansible modules have wide ranging capabilities including managing volumes, volume groups, hosts, host groups, snapshots, protection policies, and gather detailed information about the appliance. These different tasks can be performed by running simple playbooks written in yaml syntax.

Audience

This document is intended for IT administrators, storage architects, partners, and Dell Technologies employees. This audience also includes any individuals who may evaluate, acquire, manage, operate, or design a Dell networked storage environment using PowerStore systems.

Revisions

Date	Description
April 2020	Initial release: PowerStoreOS 1.0
May 2020	Minor updates
April 2021	Minor updates: PowerStoreOS 2.0
June 2021	Minor updates
November 2021	Template update
July 2022	Minor updates: PowerStoreOS 3.0

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Ryan Poulin

Contributors: Ethan Stokes

Note: For links to other documentation for this topic, see the PowerStore Info Hub.

Introduction

PowerStore overview

PowerStore achieves new levels of operational simplicity and agility. It uses a container-based microservices architecture, advanced storage technologies, and integrated machine learning to unlock the power of your data. PowerStore is a versatile platform with a performance-centric design that delivers multidimensional scale, always-on data reduction, and support for next-generation media.

PowerStore brings the simplicity of public cloud to on-premises infrastructure, streamlining operations with an integrated machine-learning engine and seamless automation. It also offers predictive analytics to easily monitor, analyze, and troubleshoot the environment. PowerStore is highly adaptable, providing the flexibility to host specialized workloads directly on the appliance and modernize infrastructure without disruption. It also offers investment protection through flexible payment solutions and data-in-place upgrades.

Snapshots overview

Snapshots are the local data protection solution within a PowerStore system. They provide a method of recovery for data that has been corrupted or accidentally deleted. Snapshots are read-only objects and cannot be modified. This immutable property allows snapshots to serve as ransomware protection in the event production data is compromised. Snapshots are pointer-based objects that provide point-in-time copies of data that is stored in volumes, volume groups, file systems, thin clones, or virtual machines. Snapshots can be created either manually or automatically within a PowerStore system and are considered write-order/crash-consistent. To create application-consistent snapshots, use Dell AppSync where supported. AppSync ensures all incoming I/O for a given application is quiesced and flushed before a snapshot is taken.

Note:

- As snapshots are not full copies of the original data, they should not be relied upon as a backup or as the disaster recovery solution.
- A write-order/crash-consistent snapshot is not considered application consistent since the snapshot may not be a full representation of the application dataset at that point-in-time.
- Typically, a host/client caches data with the intention to write it to the storage resource. Cached data is not available within the storage when a snapshot is taken without AppSync.
- Snapshots also consume overall system storage capacity to preserve the point-in-time. Ensure that the appliance has enough capacity to accommodate snapshots.

While the following sections outline the creation and management of snapshots in PowerStore Manager, snapshots can also be created and managed using the PowerStore CLI and REST API. Whether administrators take manual snapshots through PowerStore Manager, use the customizable snapshot rules, or create advanced data protection scripts, they can fully manage their storage environments using whichever method that they prefer. This ability leads to a powerful, flexible foundation for managing data protection regardless of the complexity of the use case or environment.

Redirect-on-write technology

PowerStore uses redirect-on-write technology for all writes entering the system. When a resource writes to a location which is shared with another resource or by a snapshot, the data is redirected to a new location and the resource pointers are updated to reference the new location. The following figure provides an example of redirect-on-write technology.

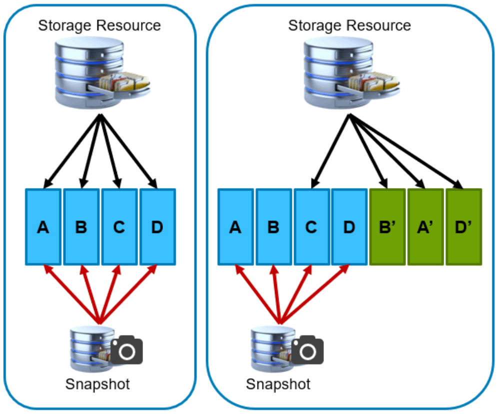


Figure 1. Redirect-on-write example

In this example, a storage resource contains four blocks of data: A, B, C, and D. A snapshot is taken of the storage resource to preserve this point-in-time, and points to blocks A, B, C, and D. When the host/client modifies blocks B, A, then D, the data is written to new locations on the system. The pointers for the storage resource are then updated to reflect the new locations for B', A', and D'. This example assumes that no data-reduction savings are achieved. For more information about data reduction within PowerStore, see the white paper *Dell PowerStore: Data Efficiencies* on the PowerStore Info Hub.

Terminology

The following table provides definitions for some of the terms that are used in this document.

Table 1. Terminology

Term	Definition
Appliance	Term used for solution containing a base enclosure and any attached expansion shelves. The size of an appliance could be only the base enclosure or the base enclosure plus expansion enclosures.
Cluster	Multiple appliances in a single grouping. Clusters can consist of one appliance or more.
File system	A storage resource that can be accessed through file sharing protocols such as SMB or NFS.
NAS server	A virtualized Network-Attached Storage server that uses the SMB, NFS, or FTP/SFTP protocols to catalog, organize, and transfer files within file system shares and exports. A NAS Server, the basis for multi-tenancy, must be created before you can create file-level storage resources. NAS servers are responsible for the configuration parameters on the set of file systems that it serves.
Network File System (NFS)	An access protocol that enables users to access files and folders on a network. NFS is typically used by Linux/UNIX hosts.
PowerStore T model	Container-based storage system that is running on purpose-built hardware. This storage system supports unified (block and file) workloads, or block-optimized workloads.
PowerStore X model	Container-based storage system that is running inside a virtual machine that is deployed on a VMware hypervisor. In addition to the block-optimized workloads that this storage system offers, it also allows users to deploy applications to be deployed directly on the array.
PowerStore Manager	The web-based user interface (UI) for storage management.
PowerStore Command Line Interface (PSTCLI)	An interface that allows a user to perform tasks on the storage system by typing commands instead of using the UI.
Representational State Transfer (REST) API	A set of resources (objects), operations, and attributes that provide interactive, scripted, and programmatic management control of the PowerStore cluster.
Server Message Block (SMB)	An access protocol that allows remote file data access from clients to hosts on a network. This is typically used in Microsoft Windows environments.
Snapshot	A point-in-time view of data stored on a storage resource. A user can recover files from a snapshot or restore a storage resource from a snapshot.
Storage resource	The top-level object a user can provision, associated with a specific quantity of storage. An example of a storage resource is a volume, volume group, or file system. All host access and data protection activities are performed at this level.
Thin clone	A read/write copy of a volume, volume group, file system, NAS server, or snapshot that shares blocks with the parent resource.
Volume	A block-level storage device that can be shared using a protocol such as iSCSI or Fibre Channel.
Volume group	A storage instance which contains one or more volumes within a storage system.

Snapshot operations

Introduction

The following operations are supported on snapshots for all storage resource types unless otherwise noted. These operations can be completed using PowerStore Manager, PowerStore CLI, or REST API. Usually, the snapshot operations below for volumes, volume groups, file systems, thin clones, and virtual machines are the same. Differences in behavior are explained.

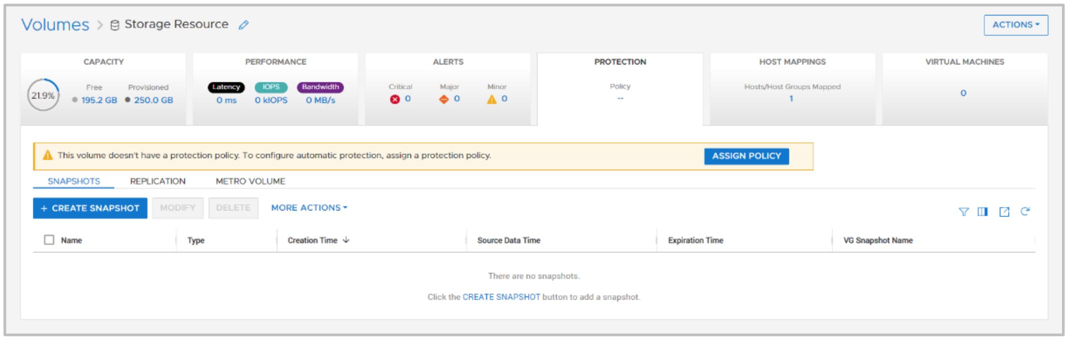
Create

When a snapshot is created, the snapshot contains the state of the storage resource and all files and data within it at that point-in-time. A snapshot is essentially a picture of the resource at that moment in time. After creation, the space that is consumed by the snapshot is virtually zero, since pointer-based technology is used and all data within the snapshot is shared with the parent resource. The amount of data that is uniquely owned by the snapshot increases over time as overwrites to the parent resource occur as previously shown in Figure 1. In that example, after changes to the parent storage resource were made, blocks A, B, and D are only owned by the snapshot.

Users may manually create snapshots of a storage resource at any time or have them created by the system on a user-defined schedule. To have snapshots created automatically, a user must create and assign a protection policy containing a snapshot rule to a resource. Protection policies and snapshot rules are further explained in Snapshot rules. The following outlines the process to manually create snapshots on the various resources within a PowerStore system.

To create a snapshot on a resource within PowerStore Manager, go to the properties window of the resource, click the **Protection** tab, click the **Snapshots** tab, and click **Create Snapshot**. Figure 2 shows an example of the location of the **Create Snapshot** button, which is used to create a manual snapshot. This process is the same for all storage resource types, whether the resource is a volume, volume group, file system, thin clone, or virtual machine within PowerStore. In this example, the properties window for a volume is displayed.

Note: For virtual machines, the Create Snapshot operation is only supported when all storage associated with a virtual machine is provided from a PowerStore Storage Container. When the **Datastore Type** column on the **Virtual Machines** page shows **vVol**, snapshots are supported. When **Mixed, VMFS,** or **NFS** is displayed, creating a snapshot on the virtual machine is not supported.



This volume doesn't have a protection policy. To configure automatic protection, assign a protection policy.

□ Name	Type	Creation Time ↓	Source Data Time	Expiration Time	VG Snapshot Name

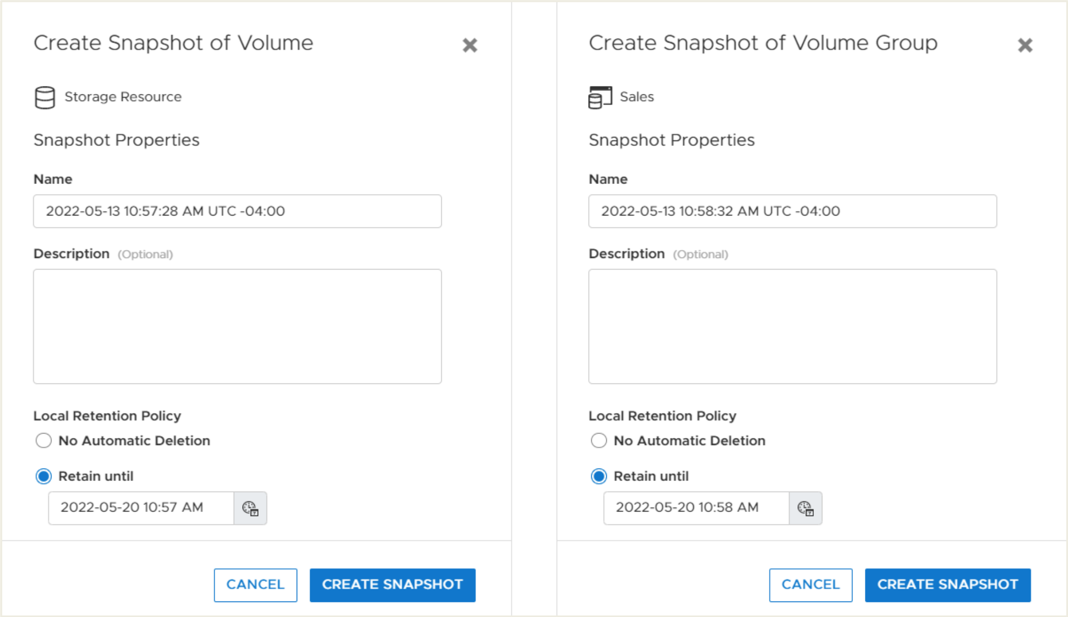
There are no snapshots.

Click the CREATE SNAPSHOT button to add a snapshot.

Figure 2. Volume properties page > Protection tab > Snapshots tab

When a user creates a snapshot manually, they must specify several attributes before creating the snapshot. These attributes include the **Name**, **Description** (optional), and the **Local Retention Policy**. The **Name** is the name that the snapshot is given, which is used when listing the snapshots on the resource. The **Description** is optional and can be used to provide more information about the snapshot, such as why it was taken or what it is used for. The **Local Retention Policy** determines if the snapshot should be automatically deleted in the future by the system. By default, the snapshot has a retention of seven days from the time the snapshot is created, but this can be customized by the user by providing a specific date and time for the snapshot to be deleted automatically by the system. The user can also choose **No Automatic Deletion** to retain the snapshot indefinitely.

Figure 3 shows an example of the Take Snapshot window for a volume and a volume group. These windows are identical regarding the information that requested from the user. Creating a snapshot of a thin clone of a volume and volume group is similar.



Create Snapshot of Volume

Storage Resource

Snapshot Properties

Name: 2022-05-13 10:57:28 AM UTC -04:00

Description (Optional)

Local Retention Policy

○ No Automatic Deletion

● Retain until 2022-05-20 10:57 AM

Create Snapshot of Volume Group

Sales

Snapshot Properties

Name: 2022-05-13 10:58:32 AM UTC -04:00

Description (Optional)

Local Retention Policy

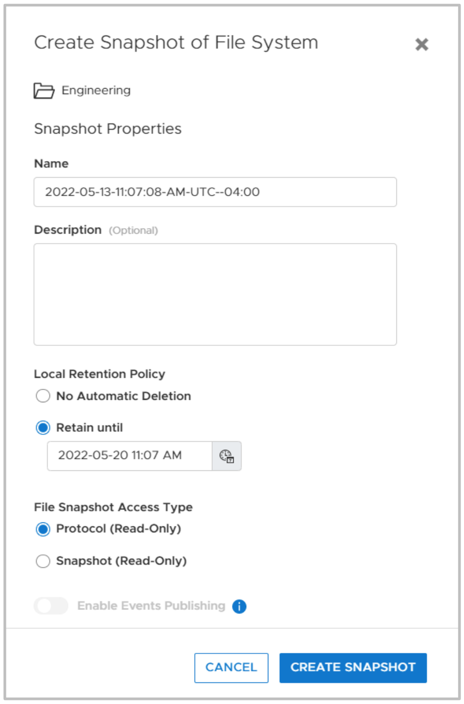
○ No Automatic Deletion

● Retain until 2022-05-20 10:58 AM

Figure 3. Take Snapshot window with volume and volume group example

When creating a snapshot of a file system, an additional option called **File Snapshot Access Type** is provided. The user has the option of choosing **Protocol (Read-Only)**, which is the default selection, or **Snapshot (Read-Only)**. The File System Access Type must be selected now, and it cannot be modified after creation.

An example of the **Take Snapshot** window is shown in Figure 4. System Access Type is discussed in detail in Snapshot access.



Create Snapshot of File System

Engineering

Snapshot Properties

Name

2022-05-13-11:07:08-AM-UTC--04:00

Description (Optional)

Local Retention Policy

○ No Automatic Deletion

● Retain until

2022-05-20 11:07 AM

File Snapshot Access Type

● Protocol (Read-Only)

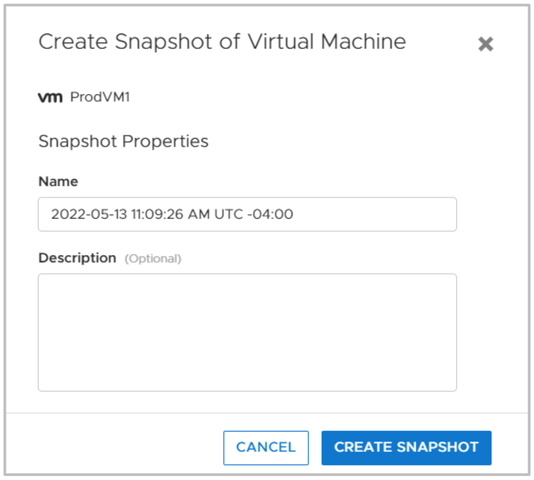
○ Snapshot (Read-Only)

Enable Events Publishing

Figure 4. Take Snapshot window with file system example

Virtual machine snapshots can either be taken within PowerStore Manager, or within VMware vCenter. When creating a snapshot within PowerStore Manager, the user may customize the **Name** and provide an optional **Description**. Once the snapshot is created, it is displayed within the properties window of the virtual machine in PowerStore Manager and the Manage Snapshots window within vCenter.

The following figure shows an example of the **Take Snapshot** window.



Create Snapshot of Virtual Machine

vm ProdVM1

Snapshot Properties

Name

2022-05-13 11:09:26 AM UTC -04:00

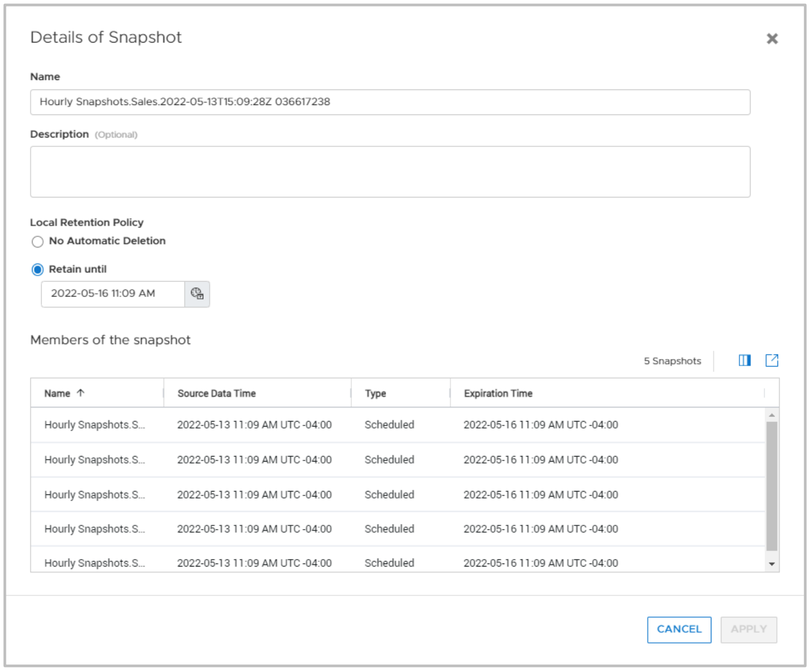
Description (Optional)

Figure 5. Take Snapshot window with virtual machine example

In PowerStoreOS 3.0 and later, users can see how many snapshots currently exist on a resource by viewing the Snapshots column. This column has been added to the volumes, volume groups, file systems, or virtual machine pages so that users can see how many snapshots exist on each resource. This column is hidden by default but can be added to the view using the Show/Hide Table Columns option.

Modify

The Modify option is used to update several attributes of an existing snapshot. This can be completed by going to the properties page of a resource within PowerStore Manager, selecting the **Protection** tab, selecting a snapshot, and clicking **Modify**. The specific attributes that can be edited are resource-dependent and are further detailed below. For virtual machine snapshots, edits can only be made from vCenter. For volumes, volume groups, and their thin clones, users can view and edit the details of a snapshot by selecting a specific snapshot on the **Protection** tab within the properties window of the parent resource and clicking **Modify**. This opens the **Details of Snapshot** page. An example of the **Details of Snapshot** page for a volume group snapshot is shown in Figure 6.The user can choose to update the snapshot **Name**, **Description**, and **Local Retention Policy**. For the **Local Retention Policy**, the user has the option of selecting **No Automatic Deletion** or setting a **Retain until** date and time. In certain situations, changing a snapshot to no automatic deletion may be required, preserving the snapshot until it is determined that it is no longer needed. For volumes and thin clones of volumes and volume groups, the same information can be changed.



Details of Snapshot

Name: Hourly Snapshots.Sales.2022-05-13T15:09:28Z 036617238

Description (Optional):

Local Retention Policy

○ No Automatic Deletion

● Retain until: 2022-05-16 11:09 AM

Members of the snapshot

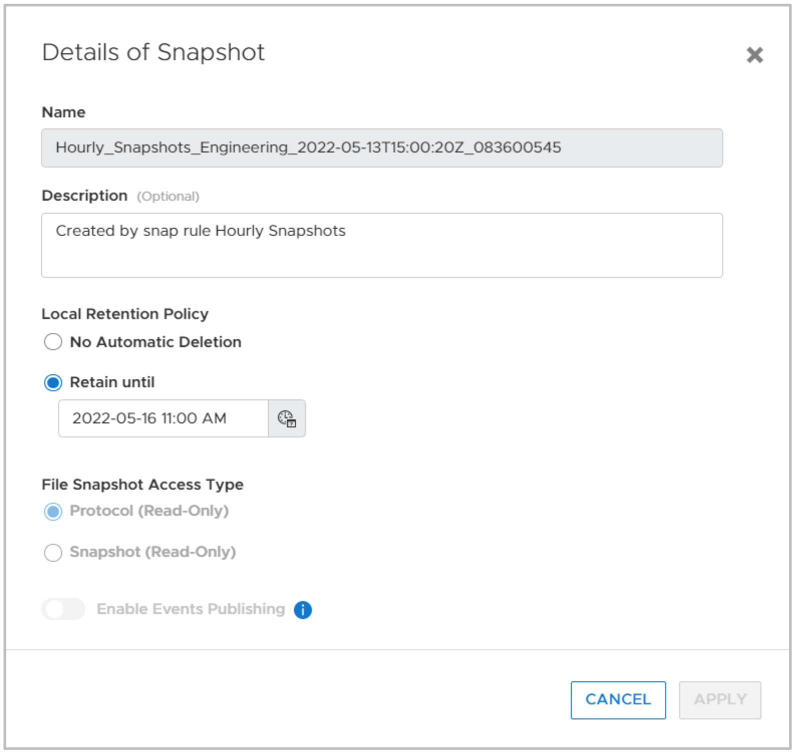
5 Snapshots

Name ↑	Source Data Time	Type	Expiration Time
Hourly Snapshots.S...	2022-05-13 11:09 AM UTC -04:00	Scheduled	2022-05-16 11:09 AM UTC -04:00
Hourly Snapshots.S...	2022-05-13 11:09 AM UTC -04:00	Scheduled	2022-05-16 11:09 AM UTC -04:00
Hourly Snapshots.S...	2022-05-13 11:09 AM UTC -04:00	Scheduled	2022-05-16 11:09 AM UTC -04:00
Hourly Snapshots.S...	2022-05-13 11:09 AM UTC -04:00	Scheduled	2022-05-16 11:09 AM UTC -04:00
Hourly Snapshots.S...	2022-05-13 11:09 AM UTC -04:00	Scheduled	2022-05-16 11:09 AM UTC -04:00

Figure 6. Details of Snapshot page for a volume group snapshot

For file systems, only the **Description** and **Local Retention Policy** can be modified. Like other resources, this can occur at any point-in-time.

Figure 7 shows that the **Name** and **File Snapshot Access Type** are displayed within the **Details of Snapshot** page but cannot be edited.



Details of Snapshot

Name: Hourly_Snapshots_Engineering_2022-05-13T15:00:20Z_083600545

Description (Optional): Created by snap rule Hourly Snapshots

Local Retention Policy

○ No Automatic Deletion

● Retain until

2022-05-16 11:00 AM

File Snapshot Access Type

● Protocol (Read-Only)

○ Snapshot (Read-Only)

Enable Events Publishing

Figure 7. Details of Snapshot page for a file system snapshot

Delete

A user can select one or more snapshots of a resource and delete them on demand. From PowerStore Manager, if a single snapshot is chosen within the **Protection** tab in the properties of a resource and **Delete** is selected, a confirmation window appears listing the snapshot name and if the user wants to delete the snapshot. When multiple snapshots are selected, the confirmation window displays a full list of all selected snapshots when the show more option is used. If the snapshot is of a virtual machine, the snapshot is also removed from vSphere.

Deleting a snapshot within PowerStore may return free space back to the appliance. If the snapshot was recently created, the snapshot has pointers to most, if not all, data contained within the parent resource. Also, as PowerStore uses deduplication and compression mechanisms to reduce the amount of data stored within the system, a snapshot may not only have blocks in common with the parent resource, but other resources within the system. Blocks of data only unique to a given snapshot are deleted and space is returned to the system for use by other resources.

Refresh

Volume and volume groups

The refresh operation has different meanings depending on the resource type. For volumes and their thin clones, the refresh operation replaces the contents of an object with the data of another resource within the same family. For volume groups and volume group thin clones with write-order consistency enabled, the contents for all members of the group are replaced. When write-order consistency is disabled, individual volumes within a volume group can be refreshed. After a refresh operation is started, the process quickly completes since only pointer updates for the resource are changed. The refresh operation differs from a restore operation, which returns the object to a previous point-in-time copy of itself. A storage resource family consists of the parent storage resource, which is the original resource, any thin clones, and snapshots in the tree. An example is shown in Figure 8.

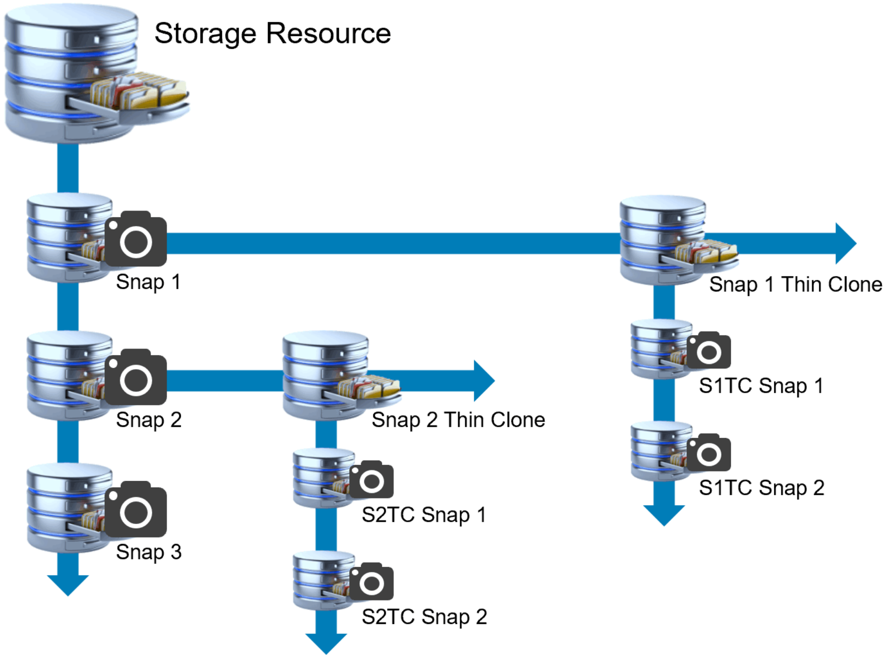


Figure 8. Storage resource family example

When using the refresh operation, obtaining a backup snapshot of the current state of the resource is highly recommended. Shut down applications using the volume, take the volume offline on the hosts, and take a backup snapshot of the current state of the resource. Not only does this guard against data corruption, but it also preserves a point-in-time copy of the dataset in case it is needed. When a refresh operation is issued from PowerStore Manager, an option to take a backup snapshot is provided. This option, which is selected by default, takes a snapshot right before the refresh operation is started.

Table 2 outlines the refresh operations that are allowed for volumes, volume groups, and thin clones. The table is organized by the object to refresh, the object to refresh from, and if the operation is allowed. Footnotes below the table provide more information about the supported operations.

Table 2. Volume and volume group refresh operations

Object to refresh	Object to refresh from	Operation allowed
Parent volume	Thin clone	Yes
Parent volume	Thin clone snapshot	Yes
Parent volume	Parent volume snapshot	No[1]
Volume thin clone	Parent volume	Yes
Volume thin clone	Parent volume snapshot	Yes

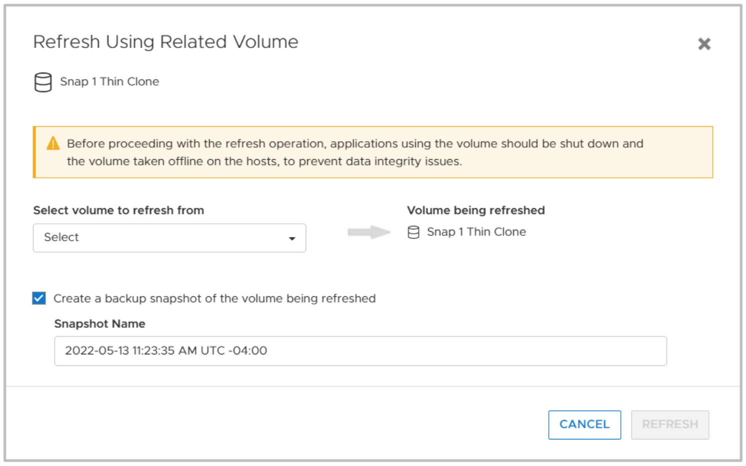
Object to refresh	Object to refresh from	Operation allowed
Volume thin clone	Thin clone snapshot	Yes[2]
Parent volume group	Thin clone	Yes
Parent volume group	Thin clone snapshot	Yes
Parent volume group	Parent volume snapshot	No[1]
Volume group thin clone	Volume group parent volume	Yes
Volume group thin clone	Volume group snapshot	Yes
Volume group thin clone	Volume group thin clone snapshot	Yes[2]

[1] Use the restore operation to complete this operation.

[2] Refreshing from a snapshot of a peer, in-family, thin clone is supported. If the snapshot is of the thin clone that is being refreshed, use the restore operation.

To refresh a volume, volume group, or a thin clone from another resource, select the resource from the volume or volume group page, click **Repurpose**, and click **Refresh Using Related Volume**. The **Repurpose** drop-down menu replaced the **More Actions** drop-down menu seen in earlier versions of PowerStoreOS. In the following example, the resources in Figure 8 were re-created to show the objects that can be used as a source of the refresh operation. Select **Snap 1 Thin Clone**, **Repurpose**, and **Refresh Using Related Volume**, and the screen in Figure 9 is shown.

In this window, a warning is shown to remind the user to shut down applications using the volume and take the volume offline on the hosts. These operations should be performed prior to the refresh operation to prevent data integrity issues. The user is also provided with information about the resource being refreshed, in this case Snap 1 Thin Clone, and a drop-down to select the source of the new data. The **Create a backup snapshot of the volume being refreshed** option is also provided. As previously stated, the option to take the snapshot is enabled by default. The user can disable it, and they can customize the name of the snapshot being taken.


Refresh Using Related Volume

Snap 1 Thin Clone

Before proceeding with the refresh operation, applications using the volume should be shut down and the volume taken offline on the hosts, to prevent data integrity issues.

Select volume to refresh from: Select

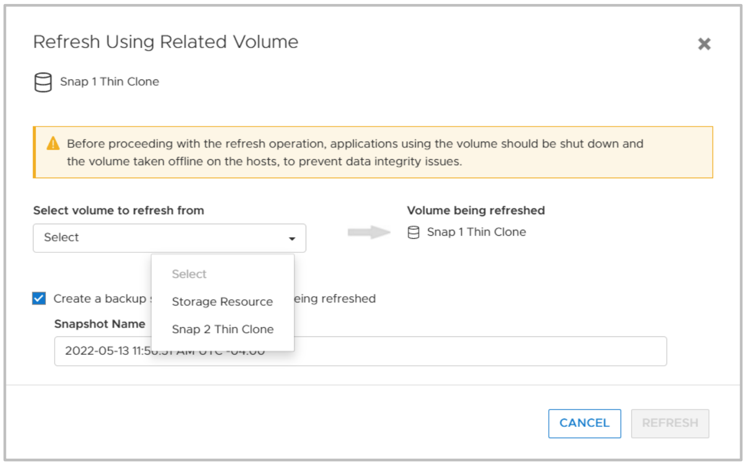
Volume being refreshed: Snap 1 Thin Clone

☑ Create a backup snapshot of the volume being refreshed

Snapshot Name: 2022-05-13 11:23:35 AM UTC -04:00

Figure 9. Refresh Using Related Volume example

Figure 10 shows the drop-down option that is expanded, and the volumes available as a source of the refresh operation for Snap 1 Thin Clone. In this resource family, Snap 1 Thin Clone can be refreshed using the data from the parent resource, **Storage Resource**, or another thin clone, Snap 2 Thin Clone. If Snap 1 Thin Clone was used for backups or a test or development environment, **Refresh** can be used to quickly update the contents of the resource to provide the latest information to the user or application.



Refresh Using Related Volume

Snap 1 Thin Clone

Before proceeding with the refresh operation, applications using the volume should be shut down and the volume taken offline on the hosts, to prevent data integrity issues.

Select volume to refresh from: Select

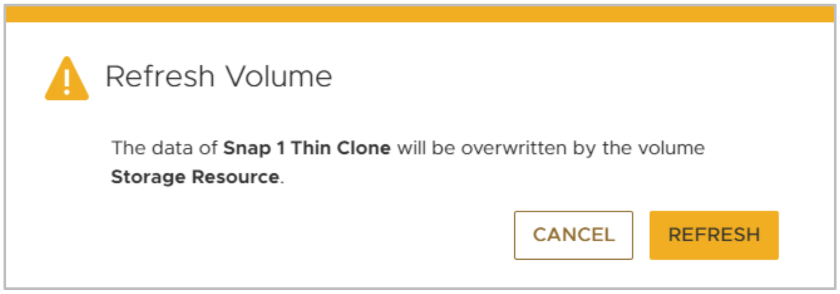
Volume being refreshed: Snap 1 Thin Clone

☑ Create a backup … eing refreshed

Snapshot Name: 2022-05-13 11:5…

Figure 10. Refresh Using Related Volume—Volumes available example

After selecting the source resource for the refresh operation and clicking **Refresh**, a confirmation window appears. To complete the operation, click **Refresh**. An example of the confirmation window is shown in Figure 11.



Refresh Volume

The data of **Snap 1 Thin Clone** will be overwritten by the volume **Storage Resource**.

Figure 11. Refresh Using Related Volume example

Alternatively, to refresh a volume, volume group, or any thin clones of the resource from a supported snapshot, select the snapshot from the Snapshot page within the **Protection** tab, click **More Actions**, then **Refresh Using Snapshot**. A window like the one in Figure 9 appears and allows the user to select a volume, volume group, or a thin clone to refresh. When it is complete, the resource contains the data that is found within the snapshot.

File systems

A file system refresh operation deletes the current contents of a snapshot and replaces it with the current data within the parent file system or file system thin clone. As with the volume and volume group refresh operation, only pointer updates occur so the operation completes quickly. This operation allows any users or applications accessing the snapshot to quickly have access to the latest information within the production file system. Figure 12 shows an example of the supported refresh operations.

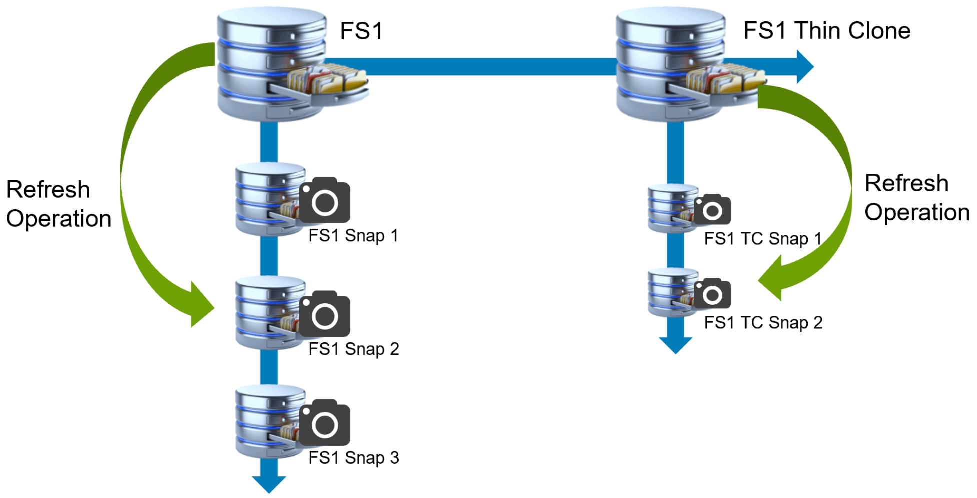
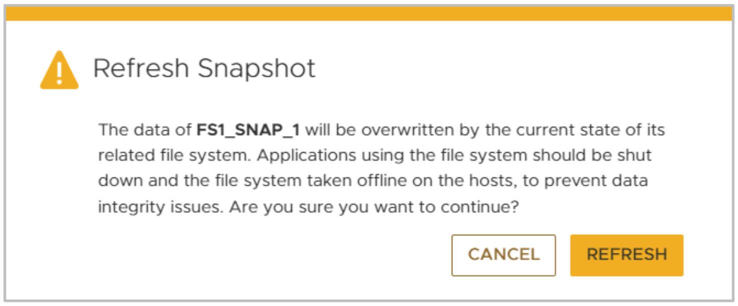


Figure 12. File system and file system thin clones refresh operation example

When a snapshot is created, values for the **Creation Time** and the **Expiration Time** are saved and displayed for the snapshot. To know which snapshots have been refreshed, the system tracks the **Last Refresh Time**. By default, this property does not have a value, but it is populated once the snapshot is refreshed. The **Last Refresh Time** is a column that is hidden by default within the **Snapshots** tab under the **Protection** tab of a resource.

To refresh the contents of a snapshot for a file system or file system thin clone, go to the properties page of the resource within PowerStore Manager. Then, select the **Protection** tab, select the checkbox in front of the snapshot to refresh, click **More Actions**, and click **Refresh Using Snapshot**. A window appears that confirms the **Refresh Snapshot** operation. An example of this window is shown in Figure 13.



Refresh Snapshot

The data of **FS1_SNAP_1** will be overwritten by the current state of its related file system. Applications using the file system should be shut down and the file system taken offline on the hosts, to prevent data integrity issues. Are you sure you want to continue?

Figure 13. Refresh Snapshot confirmation window

Restore

A restore operation reverts a parent resource dataset to a previous point-in-time when a snapshot was taken. Only snapshots directly taken of the resource can be used as the source for the restore operation. When a restore operation is started, pointer updates occur, and the entire resource dataset is reverted to the previous point-in-time contained within the snapshot. Restore is supported on volumes, volume groups, file systems, and any thin clones of these resources. The restore operation is not supported on virtual machines, but users can use the **Revert** option in vCenter. If you restore a volume group or volume group thin clone, all member volumes are restored to the point-in-time associated with the source snapshot. More information about volume groups can be found in Snapshot interoperability.

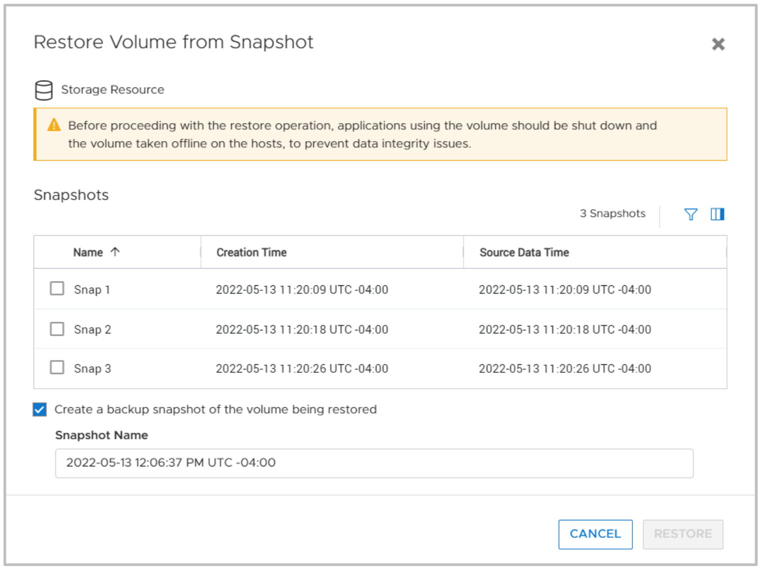
Note: File systems that have File-Level Retention Compliance (FLR-C) enabled do not support the Restore operation.

As mentioned, a restore operation reverts the entire resource back to a previous point-in-time copy of itself. If only a select amount of data must be recovered from a volume or volume group snapshot, accessing a thin clone created using the snapshot in question avoids losing any data that is updated after the snapshot was created. If the resource is a file system or file system thin clone, accessing the protocol (read-only) snapshot through an SMB share or NFS export also avoids the Restore operation when only a subset of data is needed. Accessing file system and file system thin clone snapshots is discussed in detail in Snapshot access.

Volume shrink is not supported on PowerStore. Restoring a volume, volume group, or thin clone from a snapshot does not reduce the size of the resource even if the snapshot was taken when the resource was the previous size. Instead, the resource size remains at the current size, but with the original dataset restored. For instance, if the snapshot was taken of the parent volume when it was 500 GBs, and it is now 750 GBs, the operation restores the data to the 750 GB volume.

For file systems and thin clones, this behavior is different since file system shrink is supported. The size of the object being restored changes based on the size of the resource when the snapshot was taken. For instance, if the snapshot was taken of the parent file system when it was 100 GBs, and it is now 200 GBs, the restore operation updates the size of the resource to be 100 GBs and the original data is restored.

Issuing a restore operation for volumes, volume groups, file systems, and any thin clones of these resources can be completed multiple ways. One method is to select the resource directly within the volumes, volume groups, or file systems page within PowerStore Manager. Click **Protect** and select **Restore from Snapshot**. A window like the one shown in Figure 14 appears. As with refresh, a warning is shown to remind the user to shut down applications using the volume and take the volume offline on the hosts. These operations should be performed prior to the restore operation to prevent data integrity issues. Taking a backup snapshot is also suggested. Now, the user can select a snapshot from the list to use as the restore point. As with other operations, the option to create a backup snapshot is also provided. Selected by default, this option creates a snapshot of the current point-in-time to preserve it in case it is needed in the future.



Restore Volume from Snapshot ×

Storage Resource

⚠ Before proceeding with the restore operation, applications using the volume should be shut down and the volume taken offline on the hosts, to prevent data integrity issues.

Snapshots

3 Snapshots

	Name ↑	Creation Time	Source Data Time
□	Snap 1	2022-05-13 11:20:09 UTC -04:00	2022-05-13 11:20:09 UTC -04:00
□	Snap 2	2022-05-13 11:20:18 UTC -04:00	2022-05-13 11:20:18 UTC -04:00
□	Snap 3	2022-05-13 11:20:26 UTC -04:00	2022-05-13 11:20:26 UTC -04:00

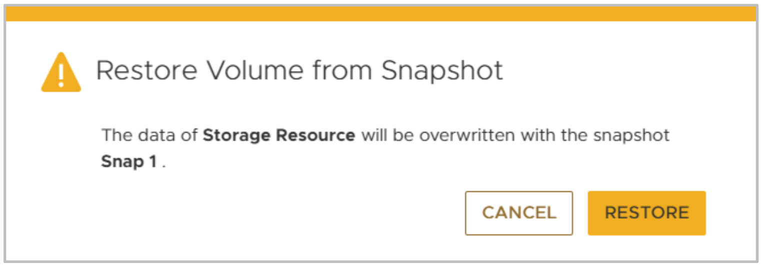
☑ Create a backup snapshot of the volume being restored

Snapshot Name

2022-05-13 12:06:37 PM UTC -04:00

Figure 14. Restore Volume from Snapshot window

A restore operation can also be completed from the **Snapshots** tab on the **Protection** tab within the properties of the resource. Using this method, the user can select which snapshot to restore from, then select **More Actions**, and lastly **Restore from Snapshot**. A window similar to the one displayed in Figure 14 is shown, and the snapshot that was previously selected is automatically checked. After the **Restore** button is selected and before the operation starts, the user is provided with a confirmation window similar to the one shown in Figure 15.The user can then click **Restore** to take a backup snapshot and restore the parent object.



Restore Volume from Snapshot

The data of **Storage Resource** will be overwritten with the snapshot **Snap 1** .

Figure 15. Restore confirmation window

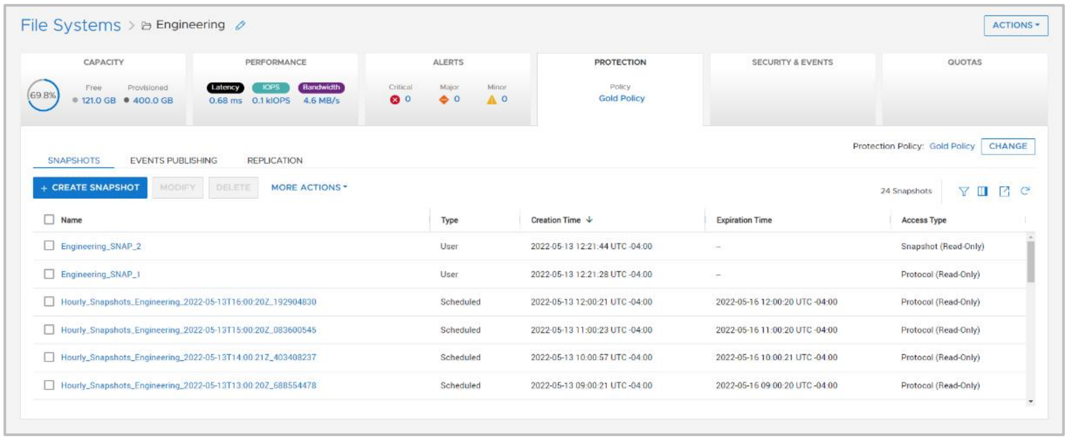
Snapshot access

The ability and method to access data within a snapshot of a resource directly depends on the resource type. For snapshots created on volumes, volume groups, or thin clones, direct access to the data within the snapshot is not allowed. Instead, a thin clone can be created and mapped to a host to provide access to the data. Thin clones are discussed later in Thin clone overview.

For file system and file system thin clone snapshots, the method of access directly depends on the type of snapshot that was taken. File systems and thin clones support **Protocol (Read-Only)** snapshots and **Snapshot (Read-Only)** snapshots. Both snapshot types allow read-only access to the point-in-time copy of the data within the snapshot, but the method to access the protocol and Snapshot-type snapshots varies.

A protocol snapshot is not shared by default. To gain read-only access to the data within a protocol snapshot, export the snapshot as an SMB share or NFS export. This process can be completed manually, or it can be scripted. When a share/export is created, access is provided through the same NAS server as the parent resource. Protocol snapshots are the default type for snapshots that are created by a snapshot rule, or when a snapshot is manually created. Creating and modifying a snapshot rule is covered in Snapshot rules.

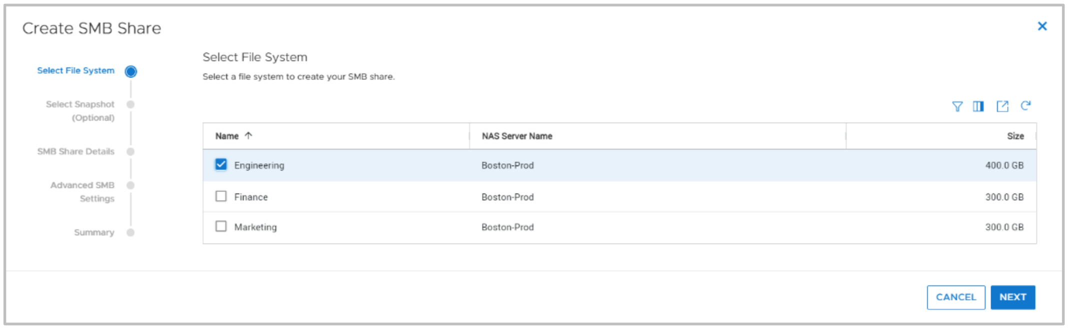
Figure 16 shows the **Snapshots** tab on the **Protection** tab within the properties of a file system. This example focuses on the file system named Engineering. It shows the snapshots that are created on this resource, along with other information such as the **Access Type**, **Name**, **Type**, **Creation Time**, and **Expiration Time**. To access any of the protocol snapshots, export them as an SMB share, NFS export, or both.



Name	Type	Creation Time	Expiration Time	Access Type
Engineering_SNAP_2	User	2022-05-13 12:21:44 UTC -04:00	–	Snapshot (Read-Only)
Engineering_SNAP_1	User	2022-05-13 12:21:28 UTC -04:00	–	Protocol (Read-Only)
Hourly_Snapshots_Engineering_2022-05-13T16:00:20Z_192904830	Scheduled	2022-05-13 12:00:21 UTC -04:00	2022-05-16 12:00:20 UTC -04:00	Protocol (Read-Only)
Hourly_Snapshots_Engineering_2022-05-13T15:00:20Z_083600545	Scheduled	2022-05-13 11:00:23 UTC -04:00	2022-05-16 11:00:20 UTC -04:00	Protocol (Read-Only)
Hourly_Snapshots_Engineering_2022-05-13T14:00:21Z_403408237	Scheduled	2022-05-13 10:00:57 UTC -04:00	2022-05-16 10:00:21 UTC -04:00	Protocol (Read-Only)
Hourly_Snapshots_Engineering_2022-05-13T13:00:20Z_688554478	Scheduled	2022-05-13 09:00:21 UTC -04:00	2022-05-16 09:00:20 UTC -04:00	Protocol (Read-Only)

Figure 16. File system properties page > Snapshots tab

To share access to the protocol snapshot, go to either the **SMB Shares** or **NFS Exports** tab on the **File Systems** page and click **Create**. In Figure 17, the example creates an SMB share that is based on a snapshot that is created on the Engineering file system.



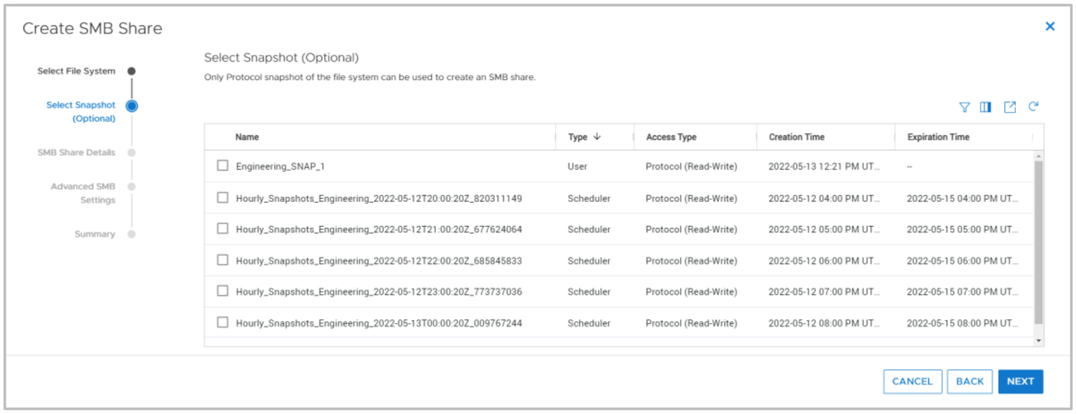
Select File System

Select a file system to create your SMB share.

Name	NAS Server Name	Size
☑ Engineering	Boston-Prod	400.0 GB
□ Finance	Boston-Prod	300.0 GB
□ Marketing	Boston-Prod	300.0 GB

Figure 17. Create SMB Share window > Select File System step

Select the file system and click **Next**, and the **Select Snapshot** step is shown. An example of this window is shown in Figure 18. The **Select Snapshot** step is optional and is only used when sharing a snapshot of a file system. If a snapshot is not being shared, skip this step by clicking **Next**. On this step, all protocol snapshots on the file system are shown. From here, select the chosen snapshot and click **Next**. After completing the remainder of the share creation workflow, access the snapshot through the share created.



Create SMB Share

Select Snapshot (Optional)

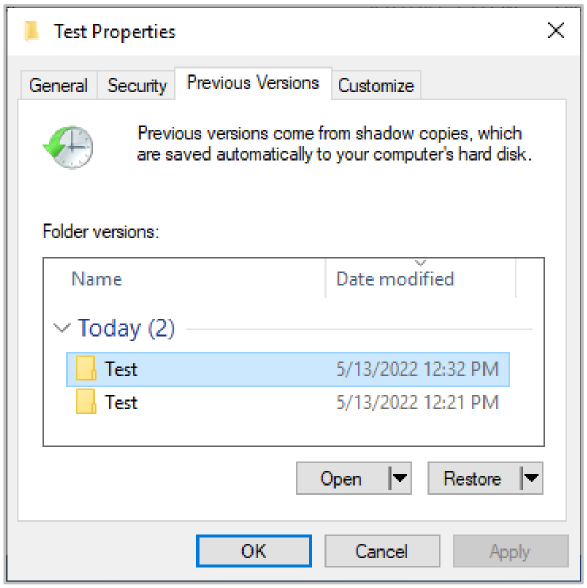
Only Protocol snapshot of the file system can be used to create an SMB share.

	Name	Type ↓	Access Type	Creation Time	Expiration Time
□	Engineering_SNAP_1	User	Protocol (Read-Write)	2022-05-13 12:21 PM UT...	--
□	Hourly_Snapshots_Engineering_2022-05-12T20:00:20Z_820311149	Scheduler	Protocol (Read-Write)	2022-05-12 04:00 PM UT...	2022-05-15 04:00 PM UT...
□	Hourly_Snapshots_Engineering_2022-05-12T21:00:20Z_677624064	Scheduler	Protocol (Read-Write)	2022-05-12 05:00 PM UT...	2022-05-15 05:00 PM UT...
□	Hourly_Snapshots_Engineering_2022-05-12T22:00:20Z_685845833	Scheduler	Protocol (Read-Write)	2022-05-12 06:00 PM UT...	2022-05-15 06:00 PM UT...
□	Hourly_Snapshots_Engineering_2022-05-12T23:00:20Z_773737036	Scheduler	Protocol (Read-Write)	2022-05-12 07:00 PM UT...	2022-05-15 07:00 PM UT...
□	Hourly_Snapshots_Engineering_2022-05-13T00:00:20Z_009767244	Scheduler	Protocol (Read-Write)	2022-05-12 08:00 PM UT...	2022-05-15 08:00 PM UT...

Figure 18. Create SMB Share window > Select Snapshot (Optional) step

For Snapshot-type snapshots, access is always available through SMB or NFS, depending on how the parent file system is shared. Having access to a Snapshot-type snapshot allows the user to easily access and restore previous versions of one or more files directly from the share at any time. For SMB, viewing the **Previous Versions** tab within the properties window of a folder in a file system brings up Snapshot-type snapshots on the resource. Navigating into the snapshot allows access to previous version of the data. For NFS, accessing the hidden Snapshot folder in the file system brings up access to the snapshots. This snapshot type is always mounted and counts towards the maximum number of mounted file systems, Snapshots, and mounted protocol snapshots. See the document *Dell PowerStore Support Matrix* on Dell.com/powerstoredocs for more information about limits.

Figure 19 shows an example of the SMB and NFS access methods to Snapshot-type snapshots. The top window shows the properties of the **Test** folder within the file system, and the **Previous Versions** tab is selected. Two snapshots are listed which provide access to the data they contain at those points in time. On the bottom, a mounted NFS export is opened and the Snapshot folder is accessed to view the available snapshots on the file system.

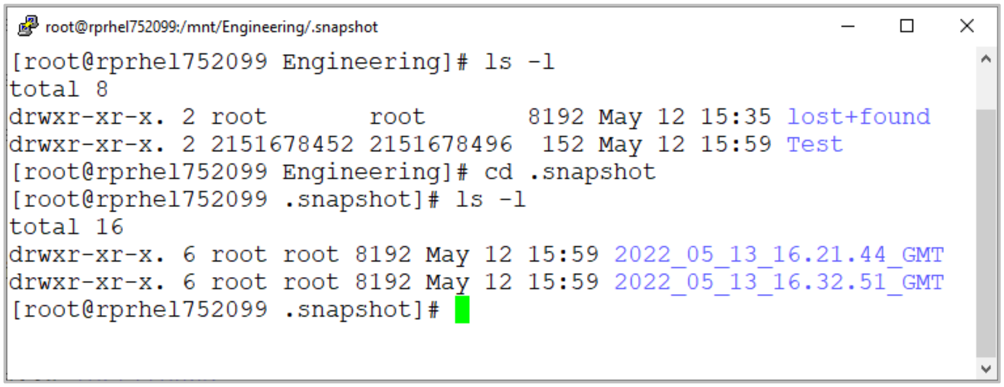


Test Properties

Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.

Folder versions:

Name	Date modified
Today (2)	
Test	5/13/2022 12:32 PM
Test	5/13/2022 12:21 PM



root@rprhel752099:/mnt/Engineering/.snapshot

```
[root@rprhel752099 Engineering]# ls -l
total 8
drwxr-xr-x. 2 root       root       8192 May 12 15:35 lost+found
drwxr-xr-x. 2 2151678452 2151678496  152 May 12 15:59 Test
[root@rprhel752099 Engineering]# cd .snapshot
[root@rprhel752099 .snapshot]# ls -l
total 16
drwxr-xr-x. 6 root root 8192 May 12 15:59 2022_05_13_16.21.44_GMT
drwxr-xr-x. 6 root root 8192 May 12 15:59 2022_05_13_16.32.51_GMT
[root@rprhel752099 .snapshot]# 
```

Figure 19. Example of SMB Previous Versions and NFS .snapshot folder access

Snapshot aging

When a snapshot is created manually, regardless of the resource type, the user can specify **No Automatic Deletion** or the **Retain Until** value. The **Retain Until** value is the integrated retention value for when the snapshot should be automatically deleted by the system. This option does not restrict the user from manually deleting a snapshot at any point-in-time. When **No Automatic Deletion** is selected, the snapshot is not deleted by the system under any circumstances until the user deletes the snapshot manually. Snapshots are not automatically deleted as the usable capacity becomes depleted on a PowerStore system.

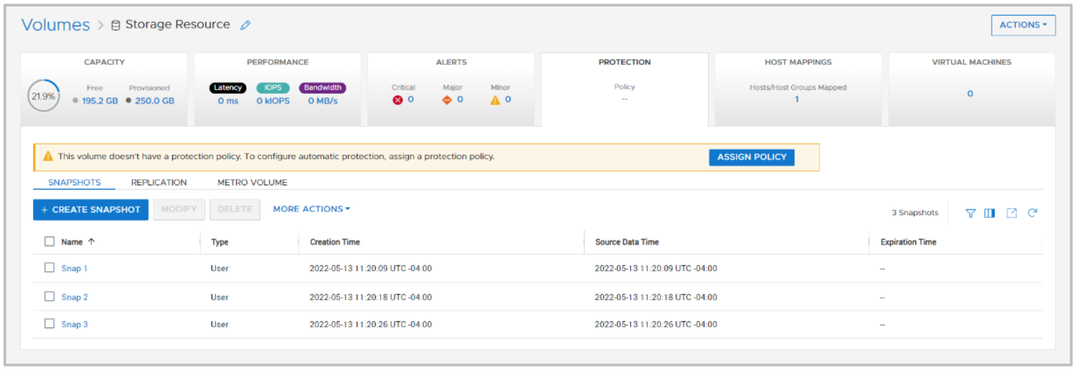
The **Retain Until** value can be set by the user during manual snapshot creation. The **Retain Until** value is automatically set when a snapshot is created by a snapshot rule. At any time, the user can update the **Retain Until** value or edit the snapshot and set it to **No Automatic Deletion**. When updating the **Retain Until** value, the user can either shorten or extend the life of the snapshot by setting the value to a chosen date and time.

The PowerStore system uses a snapshot-aging service which runs every minute in the background. This service is controlled by the system and cannot be modified. When the service runs, it identifies snapshots across the cluster with a **Retain Until** value which has occurred in the past and marks the snapshot for deletion. Snapshots are then deleted in batches across the appliances to stagger the deletion process. This method not only guards against the chance of impacting host I/O when hundreds to potentially thousands of snapshots must be deleted, but also increases the efficiency of the deletion process.

Snapshot properties

As snapshots are created, modified, refreshed, and deleted on the system, the information is logged or updated depending on the action taken. These values provide useful information to the user about each snapshot and can help with locating a specific point-in-time image of the parent resource. Figure 20 shows an example of the **Snapshots** tab within the **Protection** tab in the properties window for a volume. Listed in this example is the **Name**, **Type**, **Creation Time**, **Source Data Time**, and **Expiration Time** for each snapshot. Multiple other columns can be added to the view. This is completed by clicking the **Show/Hide Table Columns** button and selecting which columns to display.

Snapshot properties



This volume doesn't have a protection policy. To configure automatic protection, assign a protection policy.

□ Name ↑	Type	Creation Time	Source Data Time	Expiration Time
□ Snap 1	User	2022-05-13 11:20:09 UTC -04:00	2022-05-13 11:20:09 UTC -04:00	--
□ Snap 2	User	2022-05-13 11:20:18 UTC -04:00	2022-05-13 11:20:18 UTC -04:00	--
□ Snap 3	User	2022-05-13 11:20:26 UTC -04:00	2022-05-13 11:20:26 UTC -04:00	--

Figure 20. Snapshots tab within the Protection tab of a volume

The following information is available for snapshots:

Name: This is the current name of the snapshot. Depending on the resource type, this name may be updated. The default name for a user-created snapshot includes the date and timestamp for when the snapshot was created in Coordinated Universal Time (UTC) time. For snapshots created by a snapshot rule, the default name includes the snapshot rule name, resource name, and date and timestamp in UTC format. Snapshot names must be unique within a storage resource family.

Type: Defines the type of snapshot that was created. The Type can either be User (for user created snapshots) or Scheduled (for snapshots created by a snapshot rule within the system).

Creation Time: The date and time the snapshot was created. PowerStore Manager adjusts this value and displays it in the local time zone of the user.

Expiration Time: The date and time the snapshot is due to be automatically deleted by the system. PowerStore Manager adjusts this value and displays it in the user's local time zone.

Source Data Time: The date and time the snapshot was created. When the snapshot is replicated, it is the creation time of the source snapshot.

State: The current state of the snapshot. The states can either be Ready (operating normally), Initializing (snapshot is being created), Offline (the snapshot is not available due to an issue on the system), and Destroying (the snapshot is being deleted).

Application Consistent: Defines if the snapshot is taken by an application or script which guarantees application consistency. The possible values are Yes and No.

Write-Order Consistent (volume groups only): Defines if the snapshot was created with the volume group write-order consistency setting enabled or disabled.

Volume Members (volume groups only): Displays the number of volumes within the volume group when the snapshot was taken.

VG Snapshot Name (volume groups only): Displays the name of the equivalent snapshot at the volume group level.

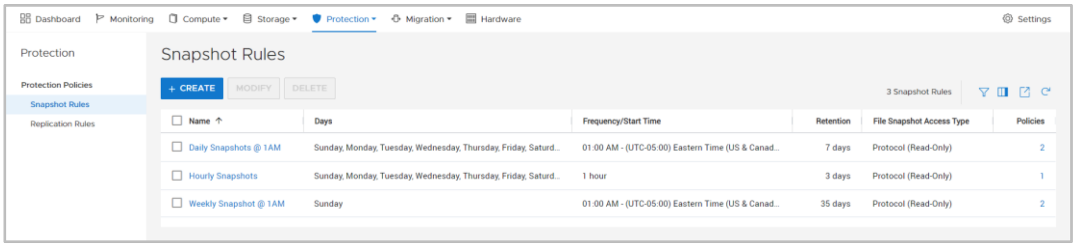
Access Type (file systems only): Displays the type of access allowed to the snapshot. The type of snapshot can either be Protocol (read-only) or Snapshot (read-only).

Last Refresh Time (file systems only): Displays the date and time the snapshot was last refreshed. If the snapshot has not been refreshed, -- is displayed.

Snapshot rules

In addition to being created manually, snapshots can be created automatically by the system at a specific time of day, or at a defined interval. Within PowerStore, protection policies are used to achieve automatic data protection on resources. A protection policy is a group of user-defined rules that are used to establish local or remote data protection on an assigned storage resource. In PowerStore, administrators can assign a protection policy to the resource which defines the level of protection. Protection policies are also created on the cluster, and not an individual appliance. This means that any resource on any appliance in a multi-appliance cluster can leverage a protection policy once it is created. Only one protection policy can be assigned to a resource at a time.

To achieve automatic snapshot creation and deletion on a resource, this first step is to create a snapshot rule. To create a snapshot rule in PowerStore Manager, go to **Protection** > **Protection Policies** > **Snapshot Rules**. An example is shown in Figure 21. On this page the current snapshot rules are displayed, along with information about each rule. To create a rule, click **Create**.



Snapshot Rules

3 Snapshot Rules

□ Name ↑	Days	Frequency/Start Time	Retention	File Snapshot Access Type	Policies
□ Daily Snapshots @ 1AM	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturd...	01:00 AM - (UTC-05:00) Eastern Time (US & Canad...	7 days	Protocol (Read-Only)	2
□ Hourly Snapshots	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturd...	1 hour	3 days	Protocol (Read-Only)	1
□ Weekly Snapshot @ 1AM	Sunday	01:00 AM - (UTC-05:00) Eastern Time (US & Canad...	35 days	Protocol (Read-Only)	2

Figure 21. PowerStore Manager Snapshot Rules page

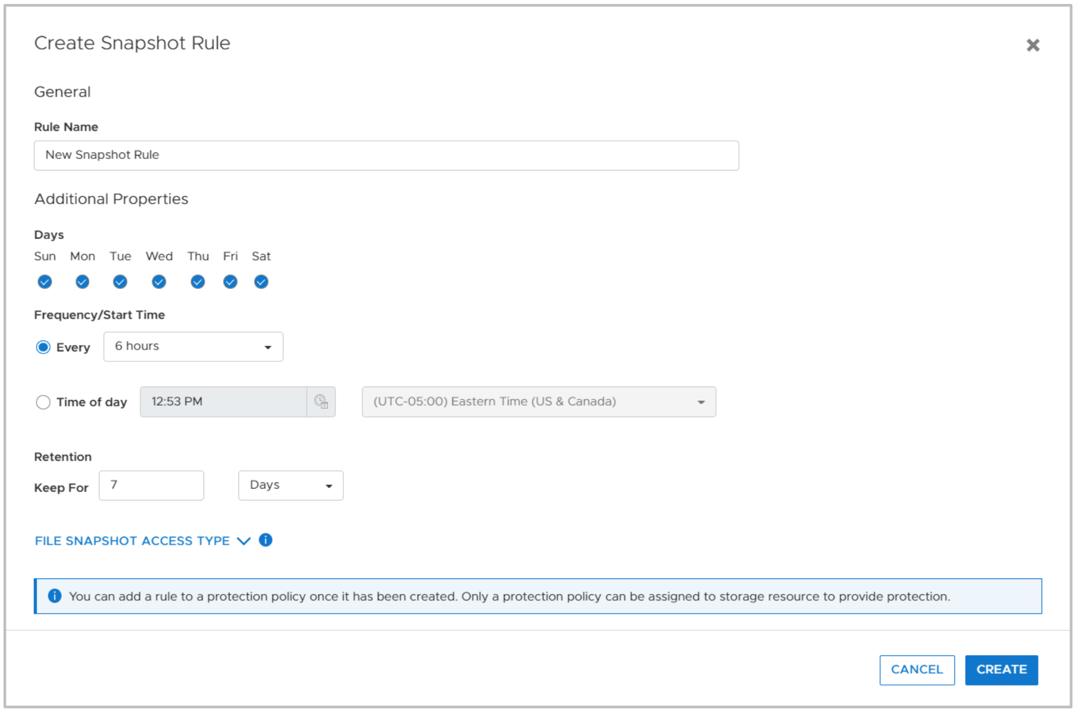
The **Create Snapshot Rule** window is then displayed. This allows the user to customize when snapshots are automatically created within the system. An example of this window is shown in Figure 22. The first entry in the snapshot rule is the **Rule Name**. Providing a unique name allows the user to quickly identify what protection the rule is set to achieve, such as the names used in Figure 21. In the example, names such as **Daily Snapshot @ 1AM** and **Weekly Snapshot @ 1AM** are used.

Next is **Days**, which defines which days of the week to run the snapshot rule and create a snapshot. By default, all days of the week are selected. The user can clear the box for days where a snapshot is not needed. This action may be done to limit the rule to one day per week, or on certain days such as workdays.

Next is the **Frequency/Start Time**, which tells the system how often to create snapshots automatically within the system. The user can either choose a fixed interval to create snapshots or specify a specific time. By default, **Every 6 hours** is selected. The drop-down box next to **Every** allows the user to choose other intervals, ranging from 5 minutes to 24 hours. The **Time of day** option allows the user to choose a particular time of day to create snapshots.

The next option is **Retention**, which tells the system when to automatically delete the snapshot. Snapshots that are created by a snapshot rule always have a retention value set, but the **Retain Until** value can be changed on an individual snapshot by the user at any time. The retention value is based on a **Keep For** value, which indicates to the system the number of **Hours** or **Days** to retain the snapshot. When the snapshot is created, the **Retain Until** value for the snapshot is set to match the retention value of the snapshot rule.

The available choices for the **Keep For** value directly depends on the **Frequency/Start Time**. The more often the snapshots are set to be created, the shorter the available retention period. This behavior ensures that the snapshot rule does not exceed the maximum number of snapshots that are allowed for a resource. If the resource has a protection policy that is assigned to it that contains several snapshot rules, then the oldest snapshot set with an expiration date is deleted automatically to allow for the new snapshot to be created. When configuring protection policies, ensure that the selected rules do not result in exceeding the maximum number of snapshots that are supported on the resources. System limits can be found in the *Dell PowerStore Support Matrix*.



Create Snapshot Rule

General

Rule Name: New Snapshot Rule

Additional Properties

Days: Sun ✓ Mon ✓ Tue ✓ Wed ✓ Thu ✓ Fri ✓ Sat ✓

Frequency/Start Time

● Every: 6 hours

○ Time of day: 12:53 PM (UTC-05:00) Eastern Time (US & Canada)

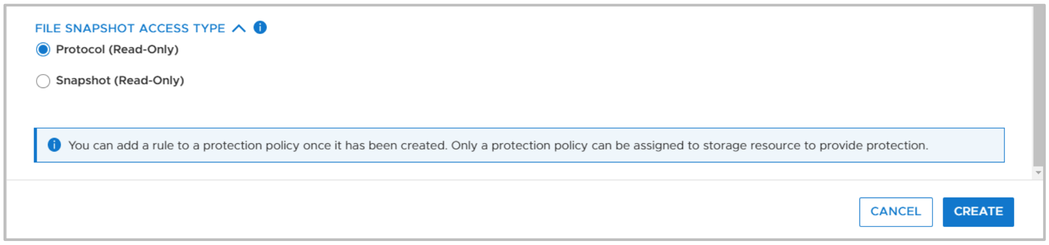
Retention

Keep For: 7 Days

You can add a rule to a protection policy once it has been created. Only a protection policy can be assigned to storage resource to provide protection.

Figure 22. Create Snapshot Rule window

The last option in the **Create Snapshot Rule** window is the **File Snapshot Access Type** setting. This setting, which is displayed in Figure 23, is only enforced for file-based resources. By default, a **Protocol (Read-Only)** snapshot is created on file systems and file system thin clones by the snapshot rule. The user can optionally create **Snapshot (Read-Only)** snapshots by the rule.



● Protocol (Read-Only)

○ Snapshot (Read-Only)

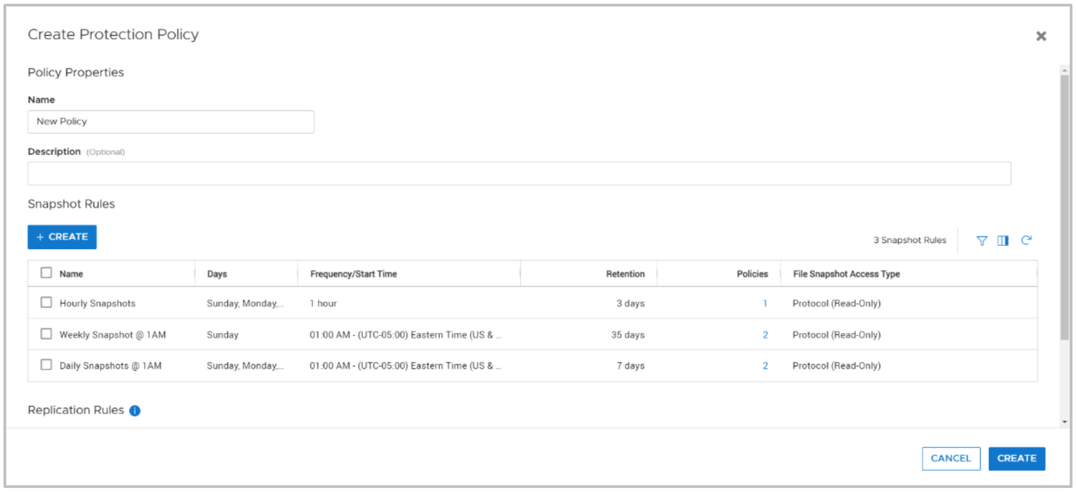
You can add a rule to a protection policy once it has been created. Only a protection policy can be assigned to storage resource to provide protection.

Figure 23. Create Snapshot Rule window > File Snapshot Access Type option

In PowerStore Manager, the times that are displayed are adjusted to the local time zone. When the snapshot rule is created and the **Time of day** option is used, systems running PowerStoreOS 1.0 takes the value and stores it in UTC format. UTC does not adjust for seasonal time changes. If you live in an area where seasonal time changes occur, the snapshot creation time does not adjust to account for this change. It is possible for snapshots that are automatically taken to be taken one hour prior or one hour past the target time due to seasonal time changes, depending on when the rule was created. To correct this issue, edit the snapshot rule and change the time to overwrite the time stored within the system.

Available in PowerStoreOS 2.0, snapshot rules configured with the **Time of day** option will be associated with a time zone. This time zone association ensures that snapshots will be taken at the correct time if the specified time zone practices Daylight Saving Time (DST). DST is the process of advancing clocks during warmer months so that darkness falls later each day according to the clock. If the specified time zone practices DST, the rule will automatically adjust when the time is advanced or set back based on this practice. The default time zone will reflect the local time zone of the client; however, administrators can modify the time zone if they so choose. Prior to this feature, the **Time of day** setting selected will be converted to UTC on the system. This can result in a timing shift of snapshots relative to the client time, depending on when the rule was created and if the time zone is entering or leaving DST.

After a snapshot rule is created, it must be added to a protection policy and assigned to a resource before snapshots are automatically taken. On the **Protection Policies** page, click **Create** to create a protection policy, or modify an existing policy to add the rule. Click **Create**, and the window in Figure 24 is displayed. The user can specify the name of the protection policy and assign snapshot rules and a replication rule to it. A protection policy can contain up to four snapshot rules, and one replication rule. Users can also create a snapshot or replication rule now if needed.



Create Protection Policy

Policy Properties

Name: New Policy

Description (Optional)

Snapshot Rules

+ CREATE

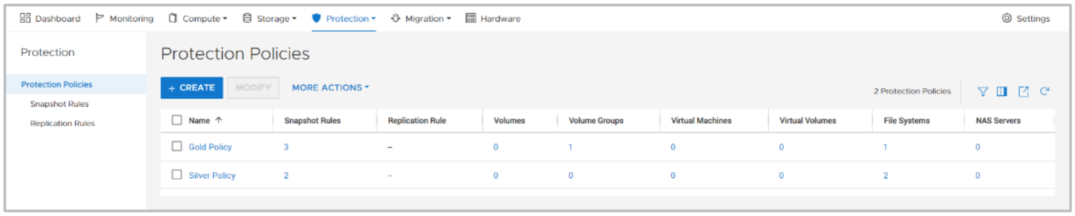
3 Snapshot Rules

☐ Name	Days	Frequency/Start Time	Retention	Policies	File Snapshot Access Type
☐ Hourly Snapshots	Sunday, Monday,...	1 hour	3 days	1	Protocol (Read-Only)
☐ Weekly Snapshot @ 1AM	Sunday	01:00 AM - (UTC-05:00) Eastern Time (US & ...	35 days	2	Protocol (Read-Only)
☐ Daily Snapshots @ 1AM	Sunday, Monday,...	01:00 AM - (UTC-05:00) Eastern Time (US & ...	7 days	2	Protocol (Read-Only)

Replication Rules

Figure 24. Create Protection Policy window

Once the protection policy is created, it is displayed on the **Protection Policies** page. On this page, you can see the number of snapshot rules that are contained within each protection policy, the replication rule that is assigned to the policy (if one exists), and how many resources have the policy assigned to it. In this example, multiple protection policies have been created based on the needs of the business. The Gold Policy has one more snapshot policy that is assigned to it compared to the Silver Policy. The names that are displayed here are only used as an example.



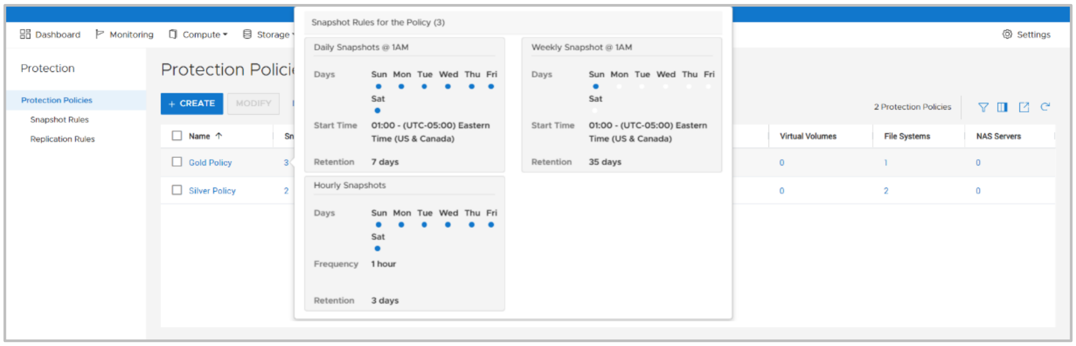
Protection Policies

2 Protection Policies

☐ Name	Snapshot Rules	Replication Rule	Volumes	Volume Groups	Virtual Machines	Virtual Volumes	File Systems	NAS Servers
☐ Gold Policy	3	–	0	1	0	0	1	0
☐ Silver Policy	2	–	0	0	0	0	2	0

Figure 25. Protection Policies page

To quickly view which snapshot rules are assigned to a protection policy, hover over the value within the **Snapshot Rules** column. This action gives a quick glance as to which snapshot rules are contained within the protection policy.



Snapshot Rules for the Policy (3)

Daily Snapshots @ 1AM
Days: Sun ● Mon ● Tue ● Wed ● Thu ● Fri ● Sat ●
Start Time: 01:00 - (UTC-05:00) Eastern Time (US & Canada)
Retention: 7 days

Weekly Snapshot @ 1AM
Days: Sun ● Mon Tue Wed Thu Fri Sat
Start Time: 01:00 - (UTC-05:00) Eastern Time (US & Canada)
Retention: 35 days

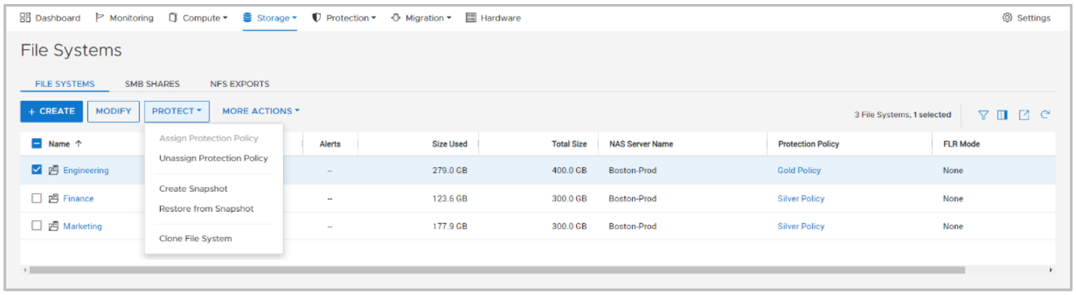
Hourly Snapshots
Days: Sun ● Mon ● Tue ● Wed ● Thu ● Fri ● Sat ●
Frequency: 1 hour
Retention: 3 days

Figure 26. Protection Policies page

Assigning a protection policy to a resource can be completed multiple ways. This task can be completed from the resource list page for volumes, volume groups, or file systems, and from the **Snapshots** tab within the **Protection** tab within the properties of a resource.

Figure 27 shows an example of the **File Systems** page and the **Protect** drop-down menu. From here, a user can either assign or unassign protection policies from multiple resources at a time. The volumes and volume groups pages have similar methods. In each of these windows, the **Protection Policy** column is available and lists the protection policy that is assigned to the resource.

Note: In PowerStoreOS 3.0 and later, protection policies can no longer be assigned to Virtual Machines. For automatic snapshot creation, VMware vSphere storage policies should be used. Any existing protection policies added to virtual machines on previous codes will remain and can be unassigned at any time. For more information about VMware and data protection, see the *Dell PowerStore: Virtualization Integration* white paper on the PowerStore Info Hub.

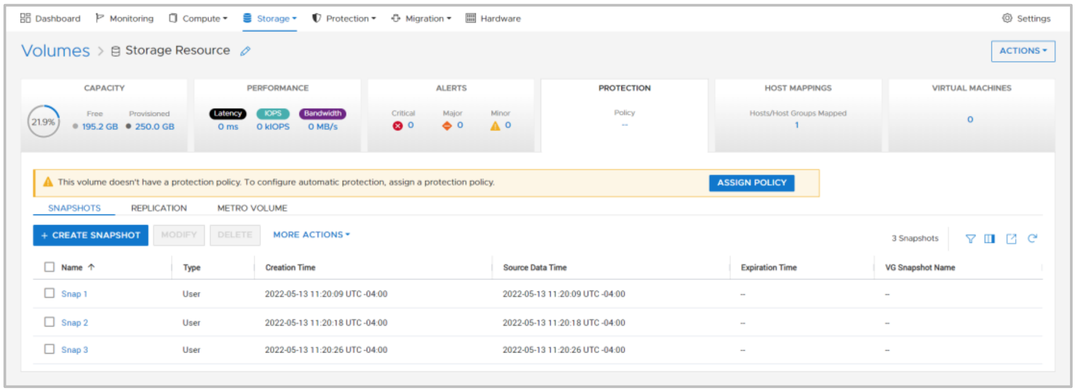


3 File Systems, 1 selected

Name	Alerts	Size Used	Total Size	NAS Server Name	Protection Policy	FLR Mode
☑ Engineering	--	279.0 GB	400.0 GB	Boston-Prod	Gold Policy	None
□ Finance	--	123.6 GB	300.0 GB	Boston-Prod	Silver Policy	None
□ Marketing	--	177.9 GB	300.0 GB	Boston-Prod	Silver Policy	None

Figure 27. File Systems page > Protection drop-down menu

When viewing the **Snapshots** tab under the **Protection** tab within the properties of a resource, the option to assign a policy is available. For resources that do not have a policy applied, the message in Figure 28 is displayed. The user can optionally click the **Assign Policy** button to add a protection policy to the resource.



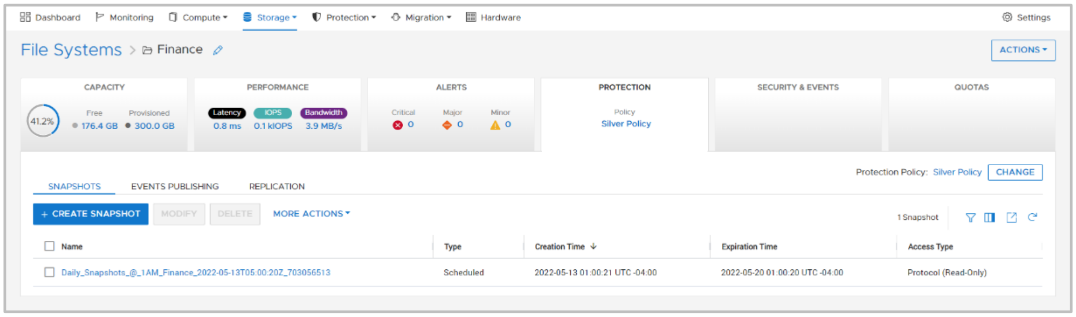
This volume doesn't have a protection policy. To configure automatic protection, assign a protection policy.

3 Snapshots

Name	Type	Creation Time	Source Data Time	Expiration Time	VG Snapshot Name
□ Snap 1	User	2022-05-13 11:20:09 UTC -04:00	2022-05-13 11:20:09 UTC -04:00	--	--
□ Snap 2	User	2022-05-13 11:20:18 UTC -04:00	2022-05-13 11:20:18 UTC -04:00	--	--
□ Snap 3	User	2022-05-13 11:20:26 UTC -04:00	2022-05-13 11:20:26 UTC -04:00	--	--

Figure 28. Snapshots tab within the Protection tab of a volume

If a policy is assigned, the name of the policy is displayed on the **Protection** tab itself, and in the **Snapshots** tab within the same window. An example is shown in Figure 29. From the **Snapshots** tab, the protection policy that is assigned to the resource can be updated by clicking the **Change** button.



File Systems > Finance

CAPACITY: 41.2% — Free 176.4 GB, Provisioned 300.0 GB

PERFORMANCE: Latency 0.8 ms, IOPS 0.1 kIOPS, Bandwidth 3.9 MB/s

ALERTS: Critical 0, Major 0, Minor 0

PROTECTION: Policy Silver Policy

Protection Policy: Silver Policy

1 Snapshot

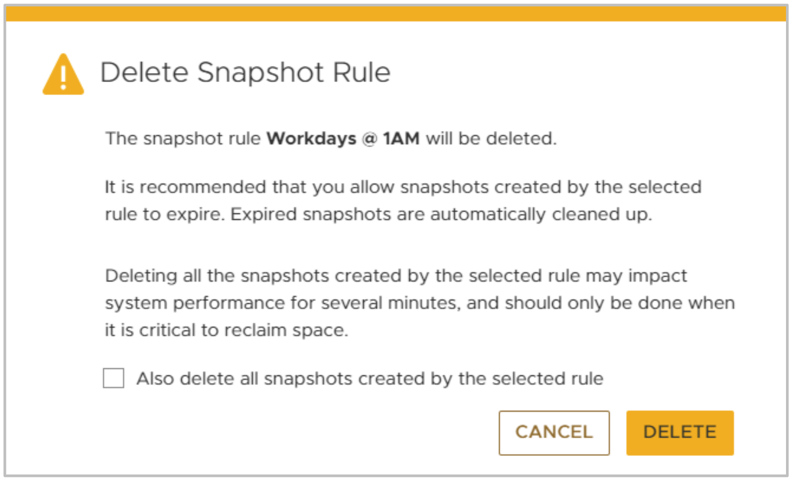
Name	Type	Creation Time	Expiration Time	Access Type
Daily_Snapshots_@_1AM_Finance_2022-05-13T05:00:20Z_703056513	Scheduled	2022-05-13 01:00:21 UTC -04:00	2022-05-20 01:00:20 UTC -04:00	Protocol (Read-Only)

Figure 29. Volume properties window > Protection tab > Snapshots tab

To quickly view the rules contained within the protection policy, hover over the protection policy name within the **Protection** tab or the **Snapshot** tab. This action provides an easy way to view the current rules rather than browsing back to the **Snapshot Rules** page.

Protection policies and snapshot rules can be edited at any time. Users can quickly add and remove rules from protection policies as needed. If a snapshot rule is edited, the changes are automatically propagated to any protection policies and resources that are currently using the rule. As an example, the user may choose to change the retention for the snapshots created by a particular snapshot rule. If this action is done, any new snapshots are created with the new retention policy. Also, any snapshots that were created using the rule also have their retention updated to reflect the new retention value.

If a snapshot rule is no longer needed, it can only be deleted if it is not in use by any protection policies. Figure 30 shows the **Delete Snapshot Rule** window. When deleting a snapshot rule, the user also can optionally delete any snapshots that are created by the rule. This action allows the user to quickly delete snapshots that are no longer needed.



Delete Snapshot Rule

The snapshot rule **Workdays @ 1AM** will be deleted.

It is recommended that you allow snapshots created by the selected rule to expire. Expired snapshots are automatically cleaned up.

Deleting all the snapshots created by the selected rule may impact system performance for several minutes, and should only be done when it is critical to reclaim space.

□ Also delete all snapshots created by the selected rule

Figure 30. Delete Snapshot Rule window

Snapshot interoperability

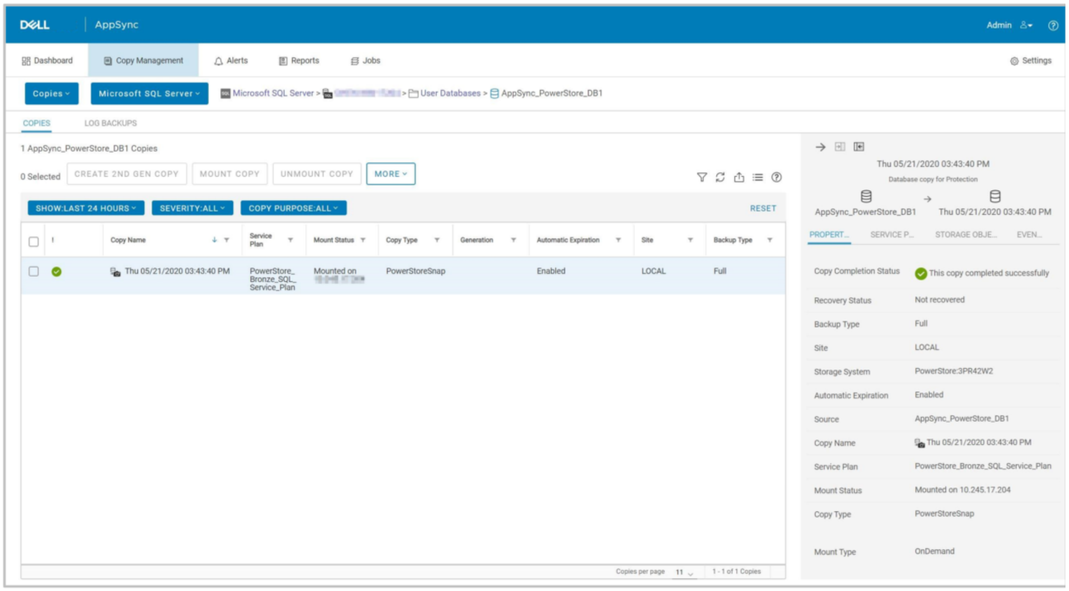
Introduction

Snapshots are fully compatible with other features of the system. They provide local data protection to the resources within the system regardless of the configuration or use case. The following are several features and software applications that interact with snapshots. The following provides additional information along with considerations for each.

AppSync

As previously discussed, snapshots that are created within a PowerStore system, either manually or automatically by a snapshot rule, are considered crash consistent. To achieve application-consistent snapshots, users can deploy AppSync in their environment for supported configurations. AppSync simplifies and automates the process of generating application-consistent snapshots, and the creation and consumption of copies of production data using thin clones.

AppSync integrates with PowerStore by handling the quiescing of host applications, and the creation of PowerStore application-consistent snapshots. When a snapshot is taken, AppSync marks the Application Consistent property of the snapshot to yes within PowerStore. Users can then review the Application Consistent property on each snapshot, and confirm which snapshots are application consistent. If application consistency is required, use AppSync and not snapshot rules to create snapshots. An example of the AppSync interface displaying a PowerStore snapshot is shown in Figure 31.



Microsoft SQL Server > [redacted] > User Databases > AppSync_PowerStore_DB1

1 AppSync_PowerStore_DB1 Copies

0 Selected

	!	Copy Name	Service Plan	Mount Status	Copy Type	Generation	Automatic Expiration	Site	Backup Type
☐	✓	Thu 05/21/2020 03:43:40 PM	PowerStore_Bronze_SQL_Service_Plan	Mounted on [redacted]	PowerStoreSnap		Enabled	LOCAL	Full

Copies per page 11 | 1 - 1 of 1 Copies

Thu 05/21/2020 03:43:40 PM
Database copy for Protection
AppSync_PowerStore_DB1 → Thu 05/21/2020 03:43:40 PM

Copy Completion Status	✓ This copy completed successfully
Recovery Status	Not recovered
Backup Type	Full
Site	LOCAL
Storage System	PowerStore:3PR42W2
Automatic Expiration	Enabled
Source	AppSync_PowerStore_DB1
Copy Name	Thu 05/21/2020 03:43:40 PM
Service Plan	PowerStore_Bronze_SQL_Service_Plan
Mount Status	Mounted on 10.245.17.204
Copy Type	PowerStoreSnap
Mount Type	OnDemand

Figure 31. AppSync snapshot example

Data reduction

Snapshots are fully compatible with the data-reduction methods that PowerStore uses, which includes deduplication and compression. Since all blocks written to the drives within the system are shared by all resources within the appliance, all resources, their snapshots, and thin clones support the thin, deduplication, and compression efficiency features of a PowerStore system.

File Level Retention

In PowerStoreOS 3.0 and later, users can enable File Level Retention (FLR) on General type file systems. FLR is used to prevent modification or deletion of locked files within the file system until a specified retention date has passed. PowerStore supports both FLR-Enterprise (FLR-E) and FLR-Compliance (FLR-C), which have different functionality and use cases. Both FLR types support snapshot creation, the modification of a limited number of snapshot properties, snapshot refresh, and snapshot deletion. The snapshot Restore operation is only supported on FLR-E file systems and cannot be run on FLR-C file systems.

For more information about file system types and File Level Retention, review the *Dell PowerStore: File Capabilities* white paper on the PowerStore Info Hub.

Migration: Import

PowerStore has a native migration capability that you can use to import storage resources from supported storage systems. This capability is integrated in the PowerStore system without requiring an external appliance. When creating an import session, you can assign a Protection Policy that contains one or more Snapshot Rules to the target of a block resource import session. For file resources, you can add a Protection Policy directly to the file systems after the import session is created. You can also create snapshots manually on the target resource after the import session is created.

For more information about migrations, see the *Dell PowerStore: Migration Technologies* white paper on the PowerStore Info Hub.

Migration: Internal migrations

The internal migration feature is used to move volumes or volume groups to another appliance in the same cluster without interrupting access to the hosts. Moving resources to another appliance can help balance the capacity or performance across appliances within the cluster. This feature can also be used to migrate storage resources to another appliance to prevent disruption, such as when the appliance is being removed from the cluster or being shut down for maintenance. When you migrate a volume or volume group, all associated snapshots and thin clones also migrate with the storage resource.

Replication

Within PowerStore, snapshots are used by asynchronous replication to provide point-in-time images as the source of Recovery Point Objective (RPO) based updates to the destination. These snapshots are used to maintain the common base images between the source and replicated resource across systems. Snapshots that are created and maintained by replication are not visible to the user within PowerStore Manager.

When replication is configured on a volume, volume group, or their thin clones, any snapshots that are created on the source resource are automatically replicated to the destination system during the next RPO-based update. These snapshots can be viewed on the destination, but user operations such as the restore operation are not allowed at the destination for a replicated object. If access to destination snapshots is required, thin clones can be leveraged to provide host access to the data. Snapshot replication is not supported on file resources. For more information, see the white paper Dell PowerStore: Replication Technologies on the PowerStore Info Hub.

Volume groups

Snapshots are fully supported with volume groups on a PowerStore system. A protection policy containing a snapshot rule can be assigned to the volume group to take snapshots at a defined interval. Snapshots can also be taken manually on the volume group or on individual volumes within the volume group at any time. This task can be done from the **Snapshots** tab within the **Protection** tab of the volume group or member volume.

Volumes can also be added or removed from a volume group without affecting data protection on the group. When a volume is removed from a volume group, no snapshots on the group are deleted or otherwise changed. If replication is configured, it continues and any changes to the group are propagated to the destination during the next sync. If the volume group has a protection policy that is assigned to it and a volume is removed, the policy is automatically assigned to the volume that is removed from the group to continue data protection. Replication on the volume that is being removed from the volume group will continue once a sync occurs on the volume group it was removed from.

When attempting the restore or refresh operations on a snapshot of a volume group, ensure that the number of volumes that were in the group when the snapshot was taken match the number of volumes in the volume group that is being restored or refreshed. For instance, if the snapshot was taken when the group had five members, it cannot be used for a restore if the group does not currently contain the five original members. To access this data, you can create a thin clone from the snapshot. To view the number of members of the group when the snapshot was taken, reference the Volume Members column on the snapshot tab.

The write-order consistency setting is a property of the volume group. This setting is enabled by default but can be changed at the creation of the volume group or later. The write-order consistency setting controls whether a snapshot is created at a consistent time across all members of the group. If enabled, the system takes a snapshot at the exact same time across all objects to keep the point-in-time image consistent for the entire group. If disabled, there is a chance that the snapshots on individual volumes within volume group are taken at slightly different times with possibly newly written data. When the snapshot is taken, the write-order consistency setting is marked as a property of the snapshot and affects what operations can be done on the snapshot. A column in the snapshot list for volume groups exists to view the write-order consistent property for each snapshot.

When write-order consistency is Yes for a snapshot, the restore and refresh operations have different capabilities than when it is No. When enabled on the snapshot, the restore and refresh operations affect the entire volume group, regardless of the current setting on the volume group. For instance, if Restore is used, all members of the group are restored from the snapshot image. This behavior is the same for the refresh operation. If write-order consistency is No for the snapshot, the restore and refresh operations can be issued to individual volumes within a volume group.

The write-order consistency setting also affects the ability to assign a protection policy to a volume group and its members. When write-order consistency is enabled on the group, users can only assign a protection policy to the volume group itself. Assigning a protection policy to an individual member is not supported. When write-order consistency is disabled on the volume group, users can choose to assign a policy to the group, or its individual members, but not both. This action provides flexibility for protecting the various members of the group with different protection policies.

When a volume group is deleted, the user can delete the volume group and retain its members or delete the group along with its members. When only the volume group is deleted, all snapshots taken of the group are also deleted. Any snapshots that are taken of the individual volumes remain. In either case, any thin clones that are created of the volume group or from a snapshot of the volume group also remain unaffected.

VMware

PowerStore systems are deeply integrated with VMware. For virtual machines that are created on a PowerStore storage container, snapshots can either be created manually or automatically through an assigned VMware storage policy that contains a snapshot rule. Snapshots can be created within vCenter or PowerStore Manager and are displayed in either interface. When taking snapshots, vSphere enforces a limit of 31 snapshots per

VM, but it is possible to apply a storage policy that exceeds this limit. If this limit is reached, the oldest snapshot is automatically deleted in order when the next snapshot is created by the policy. Manually created snapshots are never deleted automatically.

In large environments, it is possible to initiate many snapshots requests to vCenter at once. To prevent overloading vCenter, PowerStore sends a maximum of five simultaneous create snapshot operations to vCenter. The remaining operations are queued and started as each create snapshot operation completes. PowerStore also sends a maximum of five simultaneous delete snapshot operations to vCenter. Although create snapshot operations are sent individually, delete snapshot operations can be sent in batches, up to the limit of five. Because these two limits are different, it is possible to have a total of five create and five delete snapshot operations simultaneously on different VMs.

In PowerStoreOS 3.0 and later, users have the option to create either a General file system or a VMware file system. The VMware file system type is added in the 3.0 release. For VMware environments, the VMware file system type is recommended because it has been designed and optimized for VMware specific workloads and operations. For all other use cases, the General type file system should be used. Both General and VMware file systems support snapshots and all snapshot operations.

For more information about PowerStore and VMware, see the white paper *Dell PowerStore: Virtualization Integration*. For more information about file system types and the new VMware file system, review the *Dell PowerStore: File Capabilities* white paper. Both of these documents can be found on the PowerStore Info Hub.

Thin clone overview

A thin clone is a read/write copy of a volume, volume group, file system, or a snapshot of these resource types. In PowerStoreOS 3.0 and later, a NAS server can be cloned. Thin clones are essentially thin copies of the object from which it was created. As with snapshots, thin clones are thin, pointer-based objects that use redirect-on-write technology that provides immediate access to the data contained in the source of the thin clone. Thin clones are not full copies of the original source and because they share data blocks with the parent resource, they should not be used for disaster recovery scenarios. Figure 32 shows an example of a thin clone that is created from a supported resource. When initially created, the thin clone shares all blocks with the resource from which it was created. Due to redirect-on-write technology, as new writes to the original resource or the thin clone are made, new space is consumed, and original data remains until it is no longer in use.

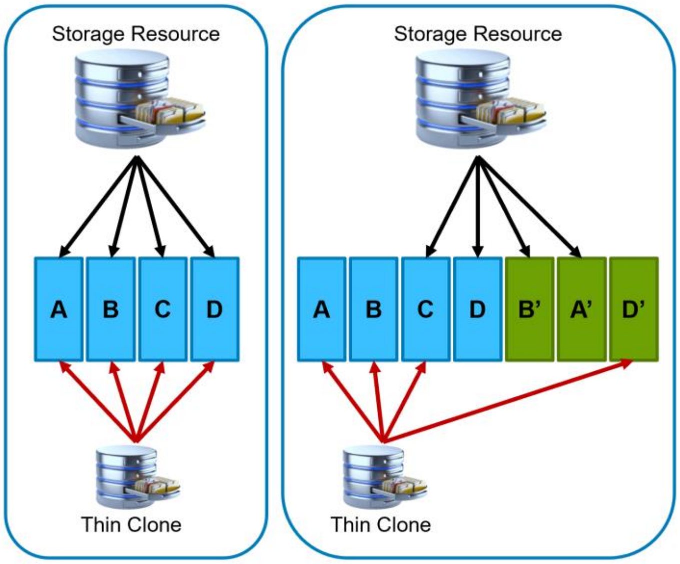


Figure 32. Thin clone redirect-on-write example

When creating a thin clone of a file resource, the user can either clone a file system or a NAS server. When cloning a file system, the resulting clone is automatically added to the same NAS server as the source file system. After the clone is created, an SMB share or NFS export must be created to access the clone. When cloning a NAS server, the user can choose which file systems to include from the source NAS server. After creation, the user needs to configure one or more file interfaces on the cloned NAS server to access the data. If the NAS server will be attached to an active directory domain, a new **SMB Computer Name** must be provided that differs from the original NAS server.

Thin clones also support local and remote data protection. For a thin clone to be protected, manual snapshots can be taken at any time, or a protection policy can be assigned to it. Figure 33 shows an example of a thin clone with a protection policy assigned. It contains a snapshot rule and an RPO-based replication rule. The resource is also mapped to a host for access.

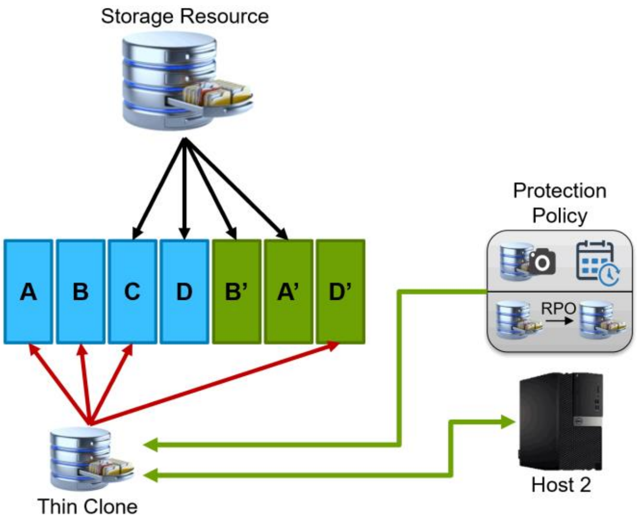


Figure 33. Thin clone data protection example

Thin clones within PowerStore are treated as an autonomous resource, as if they were a separate volume, volume group, NAS server, or file system. When created, they are listed on the main resource page, such as the **Volumes** or **File Systems** page. The properties window for a thin clone contains the same information as other resources, and the method to delete a thin clone is also the same. As an added benefit, parent resources can be deleted without deleting their thin clones. This action does not impact the thin clone or any snapshots the thin clone may have.

Use thin clones 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 test and development personnel to work with real workloads and use all data services that are 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**: Use thin clones to maintain hot backup copies of production systems. If there is corruption in the production data set, the read/write workload can be immediately resumed using the thin clones.
- **System deployment**: Use thin clones to build and deploy templates for identical or near-identical environments. For example, create a test template that is thin cloned as needed for predictable testing.

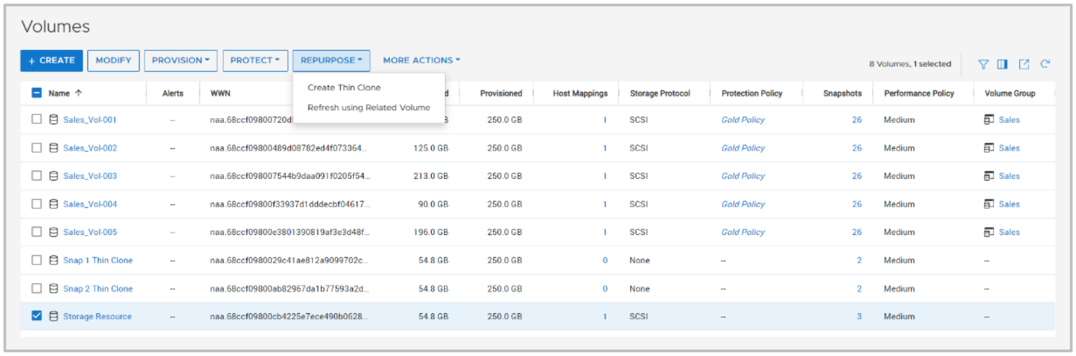
Thin clone operations

Introduction

There are multiple operations available for thin clones including the ability to create, refresh, restore, edit the properties, and delete. Each of these operations can be completed using PowerStore Manager, PowerStore CLI, or REST API. The following sections provide more information about the various operations that are supported on thin clones.

Create

Thin clones can be created using the latest data available within a volume, volume group, file system, or a previous point-in-time by using a snapshot of these resource types. To create a thin clone using the latest information in the parent object (not a snapshot), go to the page of the resource. To create a thin clone of a volume, select the object, select **Repurpose**, then **Create Thin Clone Using Volume**. In previous versions of PowerStoreOS, this option is contained under the **More Actions** dropdown. An example of these steps can be seen in Figure 34. In this example, the checkbox in front of **Storage Resource** is checked and **Repurpose** is selected. **Create Thin Clone Using Volume** can be found under **Repurpose**. The process is similar for volume groups, file systems, and NAS servers.



	Name	Alerts	WWN	d	Provisioned	Host Mappings	Storage Protocol	Protection Policy	Snapshots	Performance Policy	Volume Group
□	Sales_Vol-001	--	naa.68ccf09800720d	B	250.0 GB	1	SCSI	Gold Policy	26	Medium	Sales
□	Sales_Vol-002	--	naa.68ccf09800489d08782ed4f073364...	125.0 GB	250.0 GB	1	SCSI	Gold Policy	26	Medium	Sales
□	Sales_Vol-003	--	naa.68ccf098007544b9daa091f0205f54...	213.0 GB	250.0 GB	1	SCSI	Gold Policy	26	Medium	Sales
□	Sales_Vol-004	--	naa.68ccf09800f33937d1dddecbf04617...	90.0 GB	250.0 GB	1	SCSI	Gold Policy	26	Medium	Sales
□	Sales_Vol-005	--	naa.68ccf09800e3801390819af3e3d48f...	196.0 GB	250.0 GB	1	SCSI	Gold Policy	26	Medium	Sales
□	Snap 1 Thin Clone	--	naa.68ccf0980029c41ae812a9099702c...	54.8 GB	250.0 GB	0	None	--	2	Medium	--
□	Snap 2 Thin Clone	--	naa.68ccf09800ab82967da1b77593a2d...	54.8 GB	250.0 GB	0	None	--	2	Medium	--
☑	Storage Resource	--	naa.68ccf09800cb4225e7ece490b0628...	54.8 GB	250.0 GB	1	SCSI	--	3	Medium	--

Figure 34. Create thin clone of a volume example

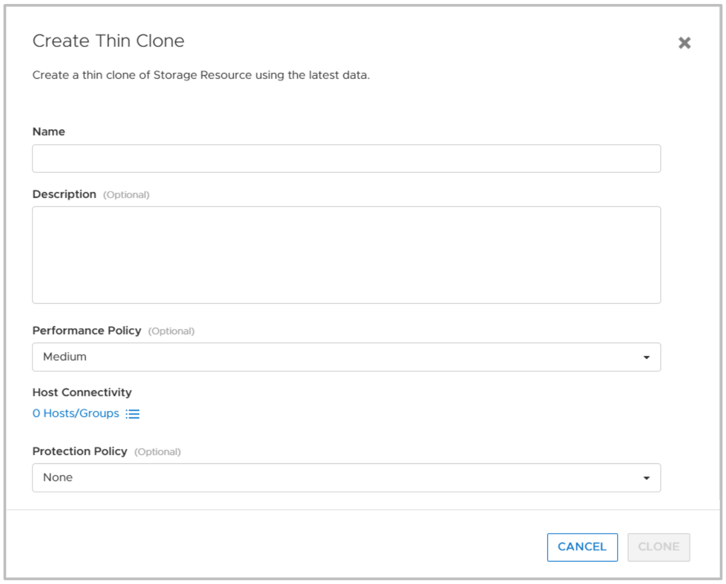
Note: In PowerStoreOS 3.0 and later, users have the option of enabling File Level Retention (FLR) on General type file systems. When creating a clone of a file system with FLR enabled, the cloned file system will be of the same FLR mode, which cannot be modified.

When a thin clone of the latest image of a resource is created, multiple options are provided to customize the thin clone. The options that are provided depend directly on the type of resource selected. Figure 35 shows the **Create Thin Clone** window for a volume, where the user can specify the **Name**, **Description**, **Performance Policy**, **Host Connectivity**, and **Protection Policy**.

For volume groups, the **Name**, **Description**, and **Protection Policy** can be customized. All other customizations occur at the individual volume level. When a thin clone of a volume group or volume group snapshot is created, all volumes within the group are cloned. For instance, if the volume group contains six volumes, the volume group thin clone being created will contain a thin clone for each of the six volumes.

For file systems, only the **Name** and **Description** can be customized. The protection policy assigned to the file system is automatically assigned to the thin clone upon creation. By default, the file system thin clone is not automatically shared. Create an SMB share or NFS export to access the data.

A clone of a NAS server can only be created from the NAS Server page. When cloning a NAS server, the user specifies the **NAS Server Name** and also selects which file systems to include from the source NAS server. After creation, the user needs to configure one or more file interfaces on the cloned NAS server to access the data. If the NAS server will be attached to an active directory domain, a new **SMB Computer Name** must be provided that differs from the original NAS server.



Create Thin Clone

Create a thin clone of Storage Resource using the latest data.

Name

Description (Optional)

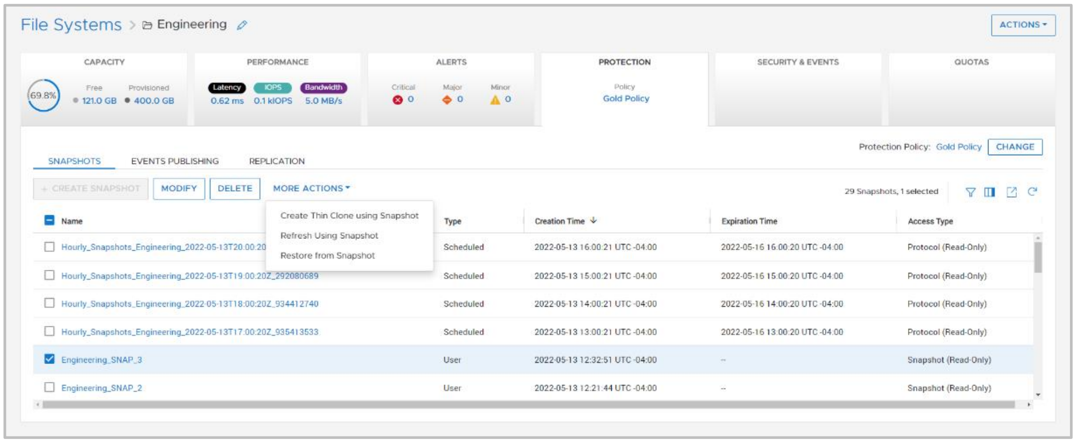
Performance Policy (Optional): Medium

Host Connectivity: 0 Hosts/Groups

Protection Policy (Optional): None

Figure 35. Create thin clone of a volume example

When a thin clone from a snapshot of a volume, volume group, or file system is created, the data within the snapshot is used as the source data to create the thin clone. To create the thin clone, go to the **Snapshot** tab within the **Protection** tab of the properties of the resource. After selecting a snapshot to create a thin clone, select **More Actions**, then **Create Thin Clone Using Snapshot**. A file system example is shown in Figure 36. After selecting **Create Thin Clone Using Snapshot**, the same options available when creating a thin clone from the main resource appears.



File Systems > Engineering

CAPACITY	PERFORMANCE	ALERTS	PROTECTION	SECURITY & EVENTS	QUOTAS
69.8% Free 121.0 GB Provisioned 400.0 GB	Latency 0.62 ms IOPS 0.1 kIOPS Bandwidth 5.0 MB/s	Critical 0 Major 0 Minor 0	Policy Gold Policy		

Protection Policy: Gold Policy

29 Snapshots, 1 selected

	Name	Type	Creation Time ↓	Expiration Time	Access Type
□	Hourly_Snapshots_Engineering_2022-05-13T20:00:20	Scheduled	2022-05-13 16:00:21 UTC -04:00	2022-05-16 16:00:20 UTC -04:00	Protocol (Read-Only)
□	Hourly_Snapshots_Engineering_2022-05-13T19:00:20Z_292080689	Scheduled	2022-05-13 15:00:21 UTC -04:00	2022-05-16 15:00:20 UTC -04:00	Protocol (Read-Only)
□	Hourly_Snapshots_Engineering_2022-05-13T18:00:20Z_934412740	Scheduled	2022-05-13 14:00:21 UTC -04:00	2022-05-16 14:00:20 UTC -04:00	Protocol (Read-Only)
□	Hourly_Snapshots_Engineering_2022-05-13T17:00:20Z_935413533	Scheduled	2022-05-13 13:00:21 UTC -04:00	2022-05-16 13:00:20 UTC -04:00	Protocol (Read-Only)
☑	Engineering_SNAP_3	User	2022-05-13 12:32:51 UTC -04:00	--	Snapshot (Read-Only)
□	Engineering_SNAP_2	User	2022-05-13 12:21:44 UTC -04:00	--	Snapshot (Read-Only)

Figure 36. Create thin clone using snapshot of a file system

Refresh

For volume and volume group thin clones, a refresh operation replaces the contents of the thin clone with the data of another resource within the same family. For volume group thin clones with write-order consistency enabled, the contents for all members of the group are replaced. When write-order consistency is disabled, individual volumes within a volume group can be refreshed. After a refresh operation is started, the process completes quickly, as only pointer updates for the resource are changed. A storage resource family contains the parent storage resource, which is the original resource, thin clones, and snapshots in the tree. An example is shown in Figure 37.

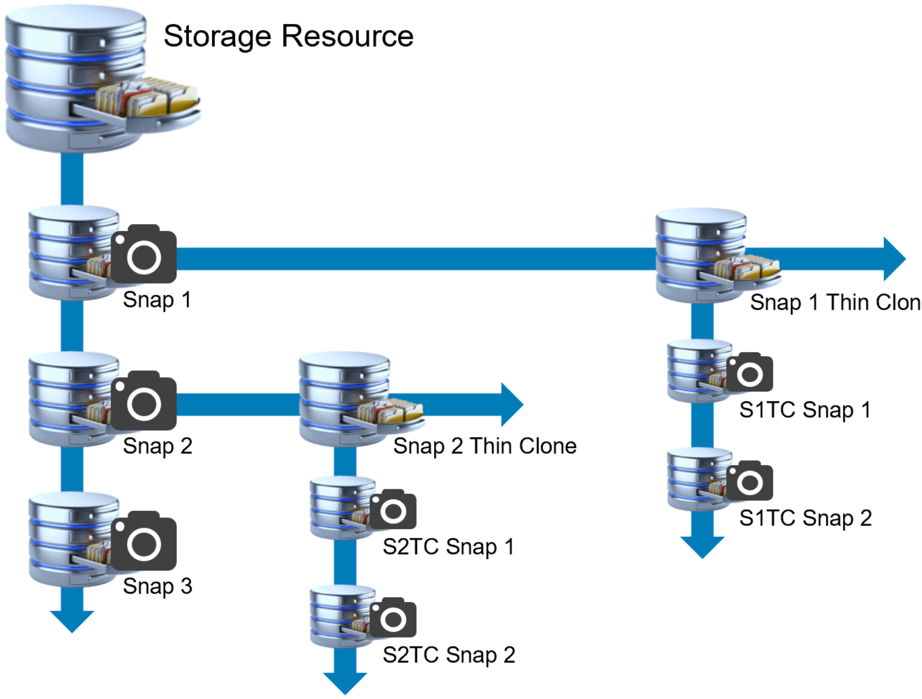


Figure 37. Storage resource family example

When using a refresh operation, it is highly suggested to shut down applications using the volume, take the volume offline on the hosts, and take a backup snapshot of the current state of the resource. Not only does this guard against corruption, but it also preserves a point-in-time copy of the dataset in case it is needed. When a refresh operation is issued from PowerStore Manager, an option to take a backup snapshot is provided. This option, which is selected by default, takes a backup right before the refresh operation is started.

Table 3 outlines the refresh operations that are allowed for volumes and volume group thin clones. The table is organized by the object to refresh, the object to refresh from, and if the operation is allowed. Notes below the table provide more information about the supported operations.

Table 3. Volume and volume group refresh operations

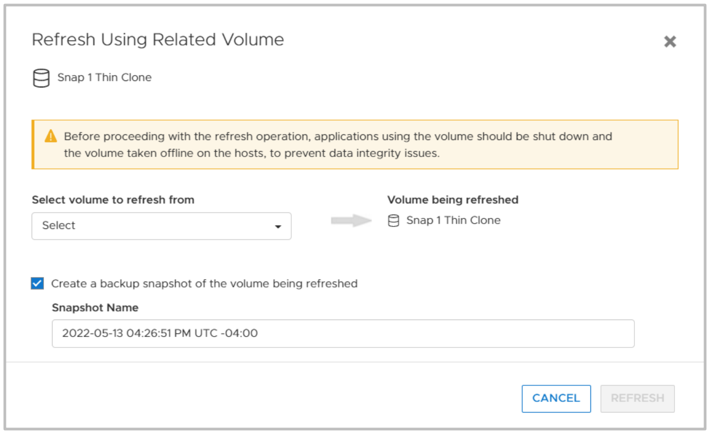
Object to refresh	Object to refresh from	Operation allowed
Volume thin clone	Parent volume	Yes
Volume thin clone	Parent volume snapshot	Yes
Volume thin clone	Thin clone snapshot	Yes[1]
Volume group thin clone	Volume group parent volume	Yes
Volume group thin clone	Volume group snapshot	Yes
Volume group thin clone	Volume group thin clone snapshot	Yes[1]

[1] Refreshing from a snapshot of a peer, in-family, thin clone snapshot is also supported.

To refresh a volume or volume group thin clone from another resource, select the volume or volume group thin clone from the resource list page, select **Repurpose**, and select **Refresh Using Related Volume**. In previous versions of PowerStoreOS, this option was found under the **More** Actions dropdown. In the following example, the resources in Figure 37 were re-created to show the objects that can be used as a source of the refresh operation.

After **Snap 1 Thin Clone**, **Repurpose**, and **Refresh Using Related Volume** is selected, the screen in Figure 38 is shown.

In this window, a warning is shown to remind the user to shut down applications using the volume and take the volume offline on the hosts. These operations should be performed prior to the refresh operation to prevent data integrity issues. The user is also provided information about the resource being refreshed, and a drop-down to select the source of the new data. The **Create a backup snapshot of the volume being refreshed** option is also provided. As previously stated, the option to take the snapshot is enabled by default. The user can disable it, and they can customize the name of the snapshot being taken.



Refresh Using Related Volume

Snap 1 Thin Clone

Before proceeding with the refresh operation, applications using the volume should be shut down and the volume taken offline on the hosts, to prevent data integrity issues.

Select volume to refresh from: Select

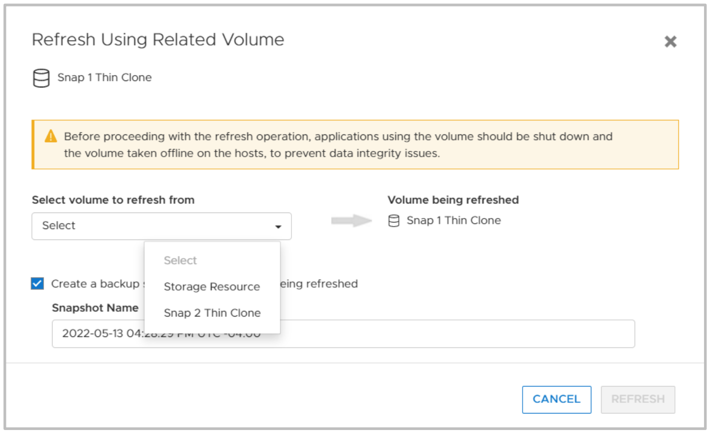
Volume being refreshed: Snap 1 Thin Clone

☑ Create a backup snapshot of the volume being refreshed

Snapshot Name: 2022-05-13 04:26:51 PM UTC -04:00

Figure 38. Refresh Using Related Volume

Figure 39 shows the drop-down option expanded, and the volumes available as a source of the refresh operation for Snap 1 Thin Clone. In this resource family, Snap 1 Thin Clone can be refreshed using the data from the parent resource, **Storage Resource**, or another thin clone, Snap 2 Thin Clone. If Snap 1 Thin Clone is used for backups or a test or development environment, Refresh can be used to quickly update the contents of the resource to provide the latest information to the user or application. After selecting the source resource for the refresh operation and clicking **Refresh**, a confirmation window appears. To complete the operation, click **Refresh**.



Refresh Using Related Volume

Snap 1 Thin Clone

Before proceeding with the refresh operation, applications using the volume should be shut down and the volume taken offline on the hosts, to prevent data integrity issues.

Select volume to refresh from: Select

Volume being refreshed: Snap 1 Thin Clone

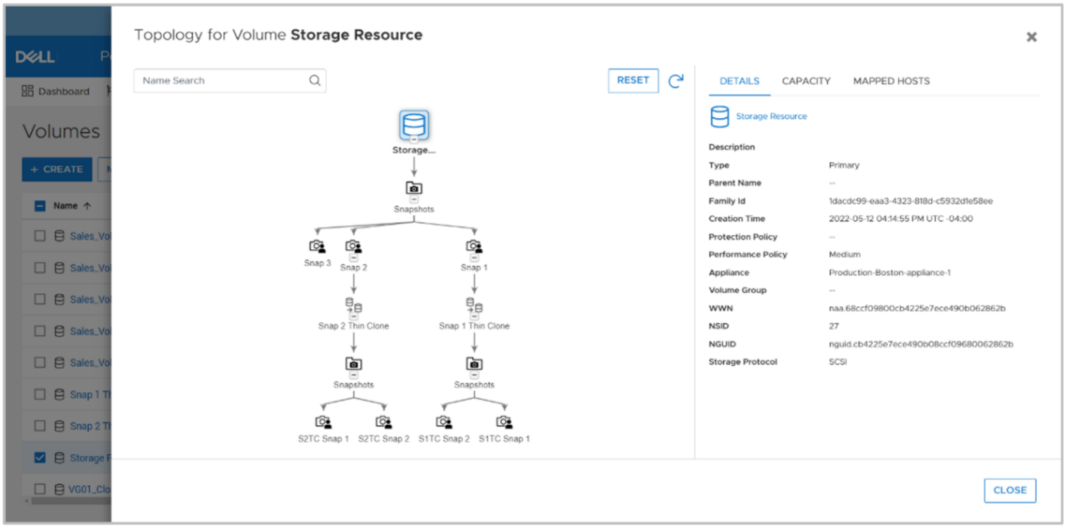
☑ Create a backup s... eing refreshed

Snapshot Name: 2022-05-13 04:28:29 PM UTC -04:00

Figure 39. Refresh Using Related Volume

To refresh a volume or volume group thin clone from a supported snapshot, select the snapshot from the **Snapshot** tab within the **Protection** tab, click **More Actions**, then **Refresh Using Snapshot**. A window similar to the one shown in Figure 38 appears and allows the user to select a volume or volume group thin clone to refresh. Once complete, the resource contains the data that is found within the snapshot.

In PowerStoreOS 3.0 and later, a volume or volume groups' topology can be viewed. The topology gives a graphical representation of the resource family, along with the parent object and any snapshots and thin clones. Depending on the resource selected in the view, details about the resource, capacity information, and any mapped hosts are also displayed. To view the topology of a resource, navigate to either the Volumes or Volume Groups page, select either a volume, volume group, or a thin clone, then click More Actions > View Topology. An example of the View Topology page can be found below, which is a representation of the storage resource family example found in Figure 37.



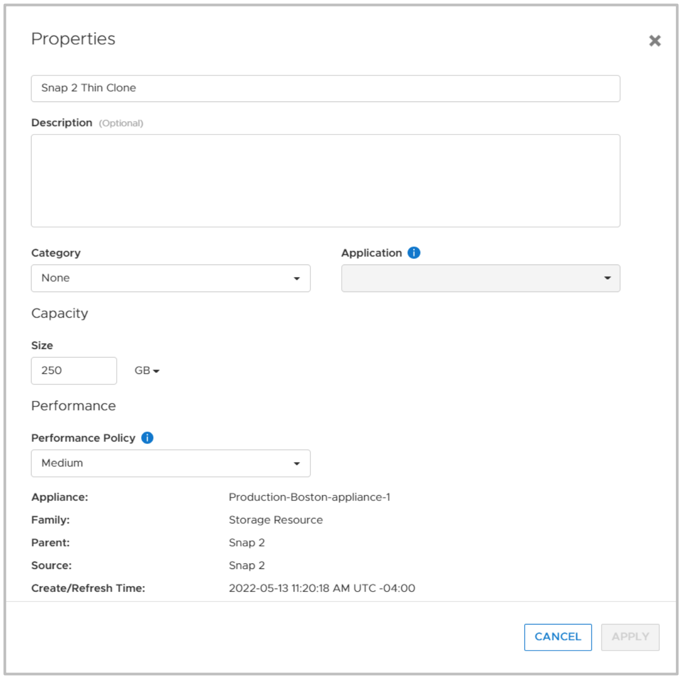
Topology for Volume **Storage Resource**

Storage Resource

Description	
Type	Primary
Parent Name	--
Family Id	1dacdc99-eaa3-4323-818d-c5932d1e58ee
Creation Time	2022-05-12 04:14:55 PM UTC -04:00
Protection Policy	--
Performance Policy	Medium
Appliance	Production-Boston-appliance-1
Volume Group	--
WWN	naa.68ccf09800cb4225e7ece490b062862b
NSID	27
NGUID	nguid.cb4225e7ece490b08ccf09680062862b
Storage Protocol	SCSI

Figure 40. View Topology page

In PowerStoreOS 3.0 and later, you can view a volume or volume groups' thin clone hierarchy. Within the properties of a thin clone, information regarding the **Family**, **Parent**, **Source**, and **Create/Refresh Time** is shown (Figure 41). The **Family** lists the base storage object for all related clones and snapshots. The **Parent** lists the object from which the clone was created. The **Source** lists the source of the data for either the creation of the clone or the resource that was the source of the latest refresh. The **Create/Refresh Time** lists the time the clone was created or last refreshed.



Properties

Snap 2 Thin Clone

Description (Optional)

Category: None

Application

Capacity

Size: 250 GB

Performance

Performance Policy: Medium

Appliance:	Production-Boston-appliance-1
Family:	Storage Resource
Parent:	Snap 2
Source:	Snap 2
Create/Refresh Time:	2022-05-13 11:20:18 AM UTC -04:00

Figure 41. Create thin clone of a volume example

Conclusion

Snapshots within the PowerStore system provide an easy-to-use local data protection solution to protect the data within volumes, volume groups, file systems, virtual machines, and thin clones. Using customizable snapshot rules and protection policies, a consistent and predictable data protection solution can be configured across the various resources of the system. Because snapshots are compatible with the various features within the PowerStore system, they can be used to protect user data in a wide array of environments and use cases.

Thin clones within PowerStore provide space-efficient copies of production environments which can be used for several use cases. For example, thin clones can be:

- Used to quickly deploy new test and development environments. Multiple thin clones can run processing jobs in parallel.
- Used to build and deploy templates for identical or near-identical environments.
- Refreshed using data from the parent resource to quickly provide the latest information to where it is needed.
- Support protection policies, which can provide local and remote protection for supported resources.

PowerStore snapshots and thin clones are features that provide significant flexibility, data protection and added value to a customer application environment.

Appendix: Technical support and resources

The Dell Technologies Info Hub > Storage site provides expertise that helps to ensure customer success with Dell storage platforms.

Dell.com/powerstoredocs provides detailed documentation about how to install, configure, and manage Dell PowerStore systems.