Dell PowerStore

Protecting Your Data

Version 3.x

October 2023
Rev. A05

Notes, cautions, and warnings

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

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

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

Contents

Additional Resources

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

Where to get help

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

- **Product information**

  For product and feature documentation or release notes, go to the PowerStore Documentation page at https://www.dell.com/powerstoredocs.

- **Troubleshooting**

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

- **Technical support**

  For technical support and service requests, go to https://www.dell.com/support and locate the **Service Requests** page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

1

Introduction

This chapter contains the following information:

Topics:

Data protection

PowerStore provides various means for protecting your data:

- Local protection - Create snapshots (point-in-time copies) of volumes, volume groups, virtual machines, or file systems on the PowerStore system .
- Remote protection - Replicate data to a remote system, or mirror the data using metro volumes for redundancy if there is a disaster.
- Remote backup - Back up volumes and volume groups directly from PowerStore to a PowerProtect DD.

PowerStore enables you to create custom protection policies, which are sets of rules for snapshot creation, replication, and remote backup, and assign them to storage resources. Protection policies apply the defined rules on the storage resource, providing it with local protection, remote protection, and remote backup.

ⓘ **NOTE:** Remote backup rules can be applied only to volumes and volume groups.

ⓘ **NOTE:** Protection policies that include a replication rule cannot be assigned to metro volumes. See Using protection policies with metro.

ⓘ **NOTE:** As of version 3.x, protection policies cannot be applied to virtual volumes (vVols) based virtual machines. See Virtual volumes replication.

PowerStore also enables you to configure standard backup for NAS servers using NDMP. For details, see *PowerStore Configuring SMB* and *PowerStore Configuring NFS* on the PowerStore Documentation page.

Snapshots

Snapshots are read-only, point-in-time copies of data of a volume, volume group, virtual machine, or file system. Creating a snapshot saves the state of the storage resource at that particular point-in-time. Using snapshots, you can protect your data locally and restore a storage resource to a previous state.

You can manually create snapshots at any time. It is also possible to configure snapshot rules as part of a protection policy and assign them to the relevant storage resources. The system automatically creates snapshots of the relevant resource according to the schedule specified in the protection policy.

As of PowerStore 3.5, you can create secure snapshots that cannot be manually deleted by an administrator or an intruder, and are automatically deleted only when they reach their expiration time. Secure snapshots provide an additional means of protection from ransomware attacks.

If data corruption occurs or data is accidentally deleted, you can recover the data from the snapshots or restore the volume or volume group to the point in time when the snapshot was created.

For file systems, you can create two access types of read-only file snapshot: protocol and .snapshot. The default access type is protocol, which can be exported as an SMB share, NFS export, or both. You can share and mount the snapshot on a client like any other file system. For .snapshot access types, you can access the files within the snapshot from the production file system in the `.snapshot` subdirectory of each directory.

You can also create write-order consistent and application consistent snapshots of volumes:

- Write-order consistent snapshots - PowerStore holds all writes on the volume group members to provide a uniform point-in-time copy, and ensures consistent protection across all member volumes. You can generate write-order consistent snapshots from the PowerStore Manager.
- Application consistent snapshots - You can create application consistent snapshots of a volume or a volume group using AppSync. When you create an application consistent snapshot, all incoming I/O for a given application is quiesced while the snapshot is created.

To verify whether a snapshot is write-order consistent or application consistent, look at the **Write-Order Consistent** and **Application Consistent** columns in the snapshot tables for a volume or volume group in PowerStore Manager.

ⓘ **NOTE:** If you cannot see these columns, you can add them, using the **Show/Hide Table Columns** option.

Mapping snapshots to hosts is not supported in PowerStore. To allow a connected host to access a snapshot, you can create a thin clone - a writable, space efficient copy of the snapshot - and map it to a host. You can update the thin clone from different snapshots using the refresh operation.

For details on the possible snapshot-related operations you can perform, using the PowerStore Manager, see the Snapshots chapter.

Replication

Data replication is a process in which data is duplicated to a remote system, which provides enhanced redundancy in case the main production system fails. Replication minimizes the downtime-associated costs of a system failure and simplifies recovery following a natural disaster or human error.

PowerStore supports asynchronous remote replication for volumes and volume groups, NAS servers, and virtual volumes.

To configure replication for volumes and volume groups:

1. Create a remote connection between the source and destination systems.
2. Create a protection policy with a replication rule that best meets your business needs.
3. Assign a protection policy to the volume or volume groups.

To configure replication for NAS servers:

1. Configure and map the file mobility network. For details see the *PowerStore Networking Guide for PowerStore T Models* on https://www.dell.com/powerstoredocs.
2. Create a remote connection between the source and destination systems.
3. Create a protection policy with a replication rule that best meets your business needs.
4. Assign a protection policy to the NAS server.

   ⓘ **NOTE:** It is not recommended to modify the file mobility network when the peer system is unreachable. When the peer system is up again, the result may be that both NAS servers are in production mode.

To configure replication for virtual volumes (vVols):

1. Create a remote connection between the source and destination systems.
2. Creating protection policies and assigning them to virtual volumes is done on vSphere. See Virtual volumes replication.

For volume and file replication, PowerStore enables you to failover control to the remote system and reverse the direction of a remote protection session. Failover may be required in the following cases:

- If you want to migrate data to a new system, and then switch to working from it without losing data. In this case, failover can be performed with no data loss.
- When there is no access to the data in the source system, you can switch to the remote system, and continue working using the latest point-in-time remote protection copy. However, data loss might occur in this situation because the latest copy in the remote system does not include data changes that are made between the time this copy was created and the time the data in the system became inaccessible.
- When the data in the source system is accessible but its integrity may be compromised. In such a case, you should revert to the latest point-in-time protection copy created before the data was compromised.

You can perform a failover test on the destination storage resource to test the system disaster recovery readiness.

For detailed information about replication-related procedures that you can perform, see the Replication chapter.

Protection policies

A protection policy consists of snapshot rules, replication rules, and remote backup rules, that you can create to establish consistent data protection across storage resources. After configuring a protection policy, you can assign it to new or existing storage resources.

A protection policy can include one replication rule, one remote backup rule, and up to four snapshot rules. All rule types can be in multiple policies.

Protection policies manage snapshot creation, replication sessions, and remote backup, based on the rules in them. You can create policies with various rules that provide different levels of protection to meet your local and remote protection needs, and assign a policy to multiple storage resources to provide identical protection to those resources.

You can create or modify relevant rules and policies, based on your user privileges.

If you want to create a rule, ensure that you review the parameters and your business requirements with an administrator before proceeding. This helps achieve and maintain consistent policies across the system.

For detailed information about protection policies-related procedures you can perform, see the Protection Policies chapter.

Metro protection

Metro provides bi-directional synchronous replication (active/active) across two PowerStore systems. A metro volume is exposed using two distinct systems, typically in two different data centers, up to 96 km (or 60 miles) apart, or in two distant locations within the same data center. The two systems cooperate to expose a single metro volume to application hosts by providing the same SCSI image and data. The hosts and application perceive the two physical volumes that are hosted by the two systems as a single volume with multiple paths.

Metro protection enables increased availability and disaster avoidance, resource balancing across data centers, and storage migration between two PowerStore systems.

When you configure a metro volume, the content of the volume is replicated to the remote system. Protection policies are used to configure additional protection such as local snapshots.

A metro session consists of two PowerStore systems and optionally a witness server.

The witness server is a passive third party that is installed on a stand-alone host (preferably in another data center so it is not affected by power failures to the PowerStore systems). The witness observes the status of the two systems. When failure occurs, the witness server determines which system remains accessible to hosts and continues to service I/Os. A witness that is installed on a third site provides protection from single failure scenarios.

One of the systems is configured as 'preferred' while the other is configured as 'nonpreferred'. When no witness is configured or when the witness is unavailable, these roles help to guide the system behavior on failure situations. When a failure occurs (either on one of the systems or to the connection between the systems), the metro session becomes 'fractured', and the nonpreferred system stops servicing I/Os.

Metro switches between using the witness and using the system role as means for recovering from single failure situations (when the witness is not configured or is unavailable, recovery from a single failure is done manually).

The following table summarizes the allowed actions that you can perform on a metro volume depending on the current metro status and the system from which the action is initiated.

NOTE: The table addresses common use cases and does not include rare failure scenarios.

Table 1. Allowed Metro Actions

Location	Metro Status	Modify Role	Promote	Demote	Pause	Resume	End Metro
On preferred system	Operating Normally	Yes	No	No	Yes	No	Yes
	Paused	No	No	Yes	No	Yes	Yes
	Fractured	No	No	Yes	Yes	No	Yes
	Switching to Metro	No	No	No	Yes	No	Yes

Table 1. Allowed Metro Actions (continued)

Location	Metro Status	Modify Role	Promote	Demote	Pause	Resume	End Metro
	Synchronization						
On nonpreferred system	Operating Normally	Yes	No	No	Yes	No	Yes
	Paused	No	Yes (if the other system is unreachable)	No	No	Yes	Yes
	Fractured	No	Yes (if the other system is unreachable)	No	Yes	No	Yes
	Switching to Metro Synchronization	No	No	No	Yes	No	Yes

Remote backup

Remote backup enables you to back up volumes and volume groups directly from PowerStore to a PowerProtect DD.

PowerStore supports backing up to a physical PowerProtect appliance or to a PowerProtect DD Virtual Edition (DDVE).

A remote backup creates a snapshot of a volume or a volume group on the PowerProtect system. The created snapshots are crash-consistent and there is no application integration.

Once they are on the PowerProtect DD, backups can be retrieved to an existing or new PowerStore cluster. You can also browse the contents of a backup on the DD, using instant access, and gain quick temporary access to the backed-up snapshots without retrieving them to the PowerStore cluster.

When a resource is backed-up for the first time, a full copy is created. Following backups are incremental - Only the changes from the last backup are copied to improve efficiency.

When you assign a protection policy that includes a remote backup rule to a volume or volume group, a remote backup session is created. Only one remote backup session can be created per resource. Remote backup sessions are displayed in the **Backup Sessions** tab of the **Remote Backup** page.

Remote backup is initiated from PowerStore. The remote backup workflow is outlined in Remote backup basic workflow.

A remote session tracks each of the operations (backup, retrieve, and instant access). You can monitor the session progress and perform actions from the remote sessions pages.

2

Remote Systems

This chapter contains the following information:

Topics:

Overview

Metro protection requires a remote system connection between two PowerStore systems. In PowerStore, the remote system connection is associated with the replication rule. You can create a remote system connection before configuring remote replication. If you are using PowerStore manager, you can create a remote system connection while creating a replication rule. It is also possible to create a remote system when configuring metro on a volume.

It is possible to create a remote connection between systems running different versions (1.x, 2.x, 3.x). The systems versions determine the supported capabilities. Both systems must run the required PowerStore version for a capability in this version to be supported. The following conditions should be met for replication of storage objects:

- Volume replication
  - The paired systems must run version 1.x or later.
- File replication
  - The paired systems must run version 3.x or later.
  - Connection type - TCP
- Virtual volumes replication
  - The paired systems must run version 3.x or later.
  - Connection type - TCP
- Metro
  - The paired systems must run version 3.x or later.
  - Connection type - TCP (see Metro pre-requisites and limitations)
  - Network latency - Low (under five milliseconds)

If you are using jumbo frames, ensure that jumbo frames are configured on both sides of the remote system connection (PowerStore port and switch ports), and on all ports between the two storage arrays. MTU size mismatch results in a warning in the following cases:

- Configuring a remote system connection.
- Modifying remote system connection settings.
- Using the **Verify and update** option.

ⓘ **NOTE:** It is not recommended to change the MTU size of a storage network when a replication session is active.

ⓘ **NOTE:** If MTU size is changed after the remote system was created, it is required to disable and then enable (bounce) the network ports of the switch that is connected to the PowerStore replication-tagged ports, to apply the change on the remote system.

To change the MTU size:

1. Pause replication session.
2. Change the storage network MTU size (**Settings** > **Networking** > **Cluster MTU**).
3. Run **Verify and update** on the remote system to confirm that no warning is issued.
4. Resume the replication session.

Remote backup requires a remote system connection between a PowerStore system and a PowerProtect DD system. The remote connection is associated with a remote backup rule, and the PowerProtect DD system can be configured while creating the rule.

For remote backup, the following conditions should be met:

- PowerStore system must run version 3.x or later.
- PowerProtect DDOS version must be 6.2.1.x or later.
- PowerStore storage network must be able to communicate with the PowerProtect DD Data Transfer network.

The Remote Systems table (under **Protection**) displays the configured remote system connections. In the Remote Systems table you can:

- View remote systems information, such as the name and IP of the remote system, system type (storage system or PowerProtect DD), supported capabilities (visible only if supported by both systems), and data connection status. The detailed view provides IP connectivity status for all initiators.
- Select a remote system and click **Modify** to edit its attributes. You can change the management IP address, description, and network latency of a remote system connection.
- Select a remote system and click **Delete** to remove it. You cannot delete a remote system in the following instances:
    - When there are active replication sessions that are associated with the remote system.
    - When there are active remote backup sessions that are associated with the remote system.
    - When there is a replication rule that is associated with the remote system.
    - When there is a remote backup rule that is associated with the remote system.
    - When there are Metro volumes
- Monitor the management and data connection status for troubleshooting purposes.
- Select a remote system and click **More Actions** > **Verify and Update** to verify and update the connection to the remote system. Verify and update detects changes in the local and remote systems and reestablishes data connections, while also taking the Challenge Handshake Authentication Protocol (CHAP) settings into account.
- For PowerProtect DD remote systems -
    - If there is a connection loss for less than ten minutes, the remote system recovers automatically when network connectivity is restored. If the connection loss lasts longer than ten minutes, click **More Actions** > **Verify and Update** after connectivity is restored to change the remote system status to OK.
    - Select a remote system and click **More Actions** > **View Capacity Details** to view usage and historical metrics for that system over a selected time period.
    - You can check for connectivity issues in the Management/File System and Data Connection columns of the **Remote Systems** table.

Add a remote system connection for replication and metro

Configure a remote system connection between the source and destination PowerStore systems to enable asynchronous replication and metro protection.

Prerequisites

Before creating a remote system connection, ensure that you have obtained the following remote system details:

- System IP address
- User authentication credentials for connecting to the system

Steps

1. Select **Protection** > **Remote Systems**.
2. In the **Remote Systems** window, click **Add**.
3. In the **Add Remote System** slide-out panel, configure the following fields:
    - Remote system type - Select **PowerStore**.
    - Management IP address
    - Description (optional)
    - Network latency
    - Username and password
4. Click **Add**.
5. In the **User Authorization** panel, verify the remote system certificate and click **Confirm**.

Add a remote system connection for remote backup

Configure a remote system connection between a PowerStore system and a PowerProtect DD system to enable remote backup.

Prerequisites

Before adding the remote connection, ensure that you have obtained the following PowerProtect DD system details:

- PowerProtect DD appliance IP address
- Storage unit name
- Data transfer parameters

> **NOTE:** Creating a remote system with invalid storage unit user credentials, results in a data connection loss. In that case, the Status column in **Protection** > **Remote System** > **[PowerProtect DD]** > **Connectivity** displays Authentication Failure. Select **Modify** for the PowerProtect DD and correct the invalid credentials. For more information, see Dell Knowledge Base Article 000208506.

About this task

> **NOTE:** You can add a single PowerProtect DD appliance to the same PowerStore cluster multiple times, using a different storage unit ID each time. That way, you can back up different resources to different locations within a single PowerProtect DD system.

> **NOTE:** If the storage unit is removed from the DD system, a complete data connection loss occurs, and remote sessions and snapshots must be cleaned up. For more information, see Dell Knowledge Base Article 000208497.

Steps

1. Select **Protection** > **Remote Systems**.
2. In the **Remote Systems** window, click **Add**.
3. In the **Add Remote System** slide-out panel, configure the following fields:
    - Remote system type - Select **PowerProtect DD**.
    - Management IP address
    - Description (optional)
    - Management username and password
    - Storage unit name
    - Data transfer IP address, username, and password
4. Set the Enable encryption option.
    - When encryption is disabled, the connection with PowerStore does not use TLS and authentication.
    - When encryption is enabled the PowerStore connection uses the DD Boost Two Way Password authentication mode, and negotiates the encryption level that is based on the DD Boost Global Security Settings.

    > **NOTE:** It is recommended to enable encryption when the remote system is DDVE in cloud.
5. Click **Add**.
6. In the **User Authorization** panel, verify the remote system certificate and click **Confirm**. to create the remote connection.

Results

The new system is added to the **Remote Systems** list. The type of the system is PowerProtect DD, and the Capability is Remote Backup.

3

Snapshots

This chapter contains the following information:

Topics:

Create a snapshot

Creating a snapshot saves the state of the storage resource and all files and data within it at a particular point in time. You can use snapshots to restore the entire storage resource to a previous state. You can create a snapshot of a volume, volume group, file system, or virtual machine.

Before creating a snapshot, consider the following:

- Snapshots are not full copies of the original data. Do not rely on snapshots for mirrors, disaster recovery, or high-availability tools. Because snapshots are partially derived from the real-time data of the storage resources, they can become inaccessible if the storage resource becomes inaccessible.
- Although snapshots are space efficient, they consume overall system storage capacity . Ensure that the system has enough capacity to accommodate snapshots.
- When configuring snapshots, review the snapshot retention policy that is associated with the storage resource. You may want to change the retention policy in the associated rules or manually set a different retention policy, depending on the purpose of the snapshot.
- Manual snapshots that are created with PowerStore Manager are retained for one week after creation (unless configured otherwise).
- If the maximum number of snapshots is reached, no more can be created. In this case, to enable creation of new snapshots, you are required to delete existing snapshots.
- If you wish to configure secure snapshots (especially when they are configured as part of a local protection policy), it is recommended to review the business requirements with an administrator before proceeding. Secure snapshots cannot be deleted until the end of the retention period, therefore it is required to plan ahead to avoid reaching the maximum snapshot limit. For details on secure snapshots, see Secure snapshots.

If you cannot view the snapshots that are created for a storage object, add the Snapshots column to the table using the **Show/Hide Table Columns**. The Snapshots column displays the number of snapshots that are created for each object. Clicking the number opens the **Snapshots** window that provides detailed information for each snapshot.

Create a snapshot of a volume

About this task

If you want to create a single snapshot of a volume (and not as a part of an assigned protection policy), use the **Create Snapshot** option.

ⓘ **NOTE:** You can use the same procedure to create a snapshot of a volume group.

Steps

1. To open the **Volumes** window, select **Storage** > **Volumes**.
2. Click the check box next to the relevant volume to select it and then select **Protect** > **Create Snapshot**.

3. In the **Create Snapshot of Volume** slide-out panel, enter a unique name for the snapshot, and set the **Local Retention Policy**.

   ⓘ **NOTE:** Retention period is set to one week by default. You can set a different retention period or select the **No Automatic Deletion** for indefinite retention.

4. If you want to create a secure snapshot, set a retention period, and select the **Secure Snapshot** option.
5. Click **Create Snapshot**.

Create a snapshot of a file system

About this task

If you want to create a single snapshot of a file system (and not as a part of an assigned protection policy), use the **Create Snapshot** option.

Steps

1. To open the **Flie Systems** window, select **Storage** > **File Systems**.
2. Click the check box next to the relevant file system to select it and then select **Protect** > **Create Snapshot**.
3. In the **Create Snapshot of File System** slide-out panel, enter a unique name for the snapshot, and set the **Local Retention Policy**.

   ⓘ **NOTE:** Retention period is set to one week by default. You can set a different retention period or select the **No Automatic Deletion** for indefinite retention.

4. Set the File Snapshot Access Type.
5. If events publishing was configured on the NAS server, you can select to enable events publishing.
6. Click **Create Snapshot**.

Create a snapshot of a virtual machine

About this task

If you want to create a single snapshot of a virtual machine (and not as a part of an assigned protection policy), use the **Create Snapshot** option.

Steps

1. To open the **Virtual Machines** window, select **Compute** > **Virtual Machines**.
2. Click the check box next to the relevant virtual machine to select it and then select **Protect** > **Create Snapshot**.
3. In the **Create Snapshot of Virtual Machine** slide-out panel, enter a unique name for the snapshot.
4. Optionally, enter a short description.
5. Click **Create Snapshot**.

Create a thin clone

Thin clones are writable copies of a snapshot, volume, volume group, or file system that can be accessed by a host. Unlike a full clone, a thin clone is a space efficient copy that shares data blocks with its parent object and not a full backup of the original resource. A thin clone can be created directly as a copy of the parent object or using one of its snapshots.

Thin clones retain full read access to the original resource. You can modify the data within the thin clone while preserving the original snapshot.

Using thin clones, you can establish hierarchical points in time to preserve data over different stages of data modifications. If the parent resource is deleted, migrated, or replicated, the thin clone is unaffected.

Create a thin clone of a volume or volume group

About this task

You can perform the following actions on thin clones of volumes and volume groups:

- Map thin clones to different hosts.
- Refresh the thin clone.
- Restore the thin clone from a backup.
- Apply protection policies to thin clones.

Steps

1. Select **Storage** > **Volumes** or **Storage** > **Volume Groups** to open the relevant resource window.
2. Click the check box next to the relevant volume or volume group and then select **Repurpose** > **Create Thin Clone**.
3. In the **Create Thin Clone** slide-out window perform the following:
   - Enter thin clone name.
   - Enter description (optional).
   - Set performance policy (only for thin clones created from volumes) .
   - Set host connectivity (only for thin clones created from volumes).
   - Set protection policy.
4. Click **Clone**.

Create a thin clone of a file system

About this task

You can perform the following actions on thin clones of volumes and volume groups:

- Map thin clones to different hosts.
- Restore the thin clone from a backup.
- Apply protection policies to thin clones.

Steps

1. Select **Storage** > **File Systems** to open the **File Systems** window.
2. Click the check box next to the relevant file system and then select **Protect** > **Clone File System**
3. In the **Create Thin Clone** slide-out window, set the thin clone name and, optionally, a description
4. If events publishing was configured on the NAS server, you can select to enable events publishing.
5. Click **Clone**.

Create a thin clone of a snapshot

About this task

You can create a thin clone of a snapshot created for a volume, volume group, or file system.

Steps

1. Open the relevant storage resource window.
2. Click a resource to open its Overview window.
3. Click the **Protection** tab.
4. Click **Snapshots** to view the list of snapshots created for the resource.
5. Select a snapshot from the table and then select **More actions** > **Create Thin Clone using Snapshot**.

Using clones to access read-only snapshots from hosts

Mapping and unmapping block snapshots to hosts is not supported in PowerStore. To allow a connected host to access a snapshot, create a thin clone of the snapshot and map it to a host. After creating the thin clone, you can use the refresh operation to update the thin clone from different snapshots. For more information, see Refresh a storage resource.

File snapshots can be mounted on hosts either directly (to allow read-only access) or by creating a thin clone (to allow read-write access). To mount the file system directly, the snapshots can be exported as NFS export or SMB share.

You can export snapshots using one of the following access types:

- Protocol - The snapshot is exported with a new share name.
- .snapshot - You can see the snapshot on Unix/Linux under the .snapshot directory of the file system, and on Windows, by right-clicking the file system and selecting the **Previous Version** option.

Refresh a storage resource

The refresh operation is used to replace the contents of a storage resource with contents from a related resource (a clone or an indirect child snapshot). You can create a duplicate of the production environment to be used for various purposes (such as test and development, reporting etc.). To keep the duplicated environment up-to-date, it should be updated with a storage resource that includes the recent changes.

You can use the refresh operation in the following scenarios:

- Refresh a thin clone from the base volume.
- Refresh a storage resource or thin clone from another thin clone in the family.
- Refresh a storage resource or thin clone from a snapshot of a related thin clone or base volume.

For file systems, you can refresh a snapshot of a file system with its direct parent file system.

If you refresh the thin clone of a snapshot that has derivative snapshots, the derivative snapshots remain unchanged and the family hierarchy stays intact. If you refresh a volume group, the point-in-time image on all member volumes is also refreshed.

When refreshing a resource from a snapshot that was replicated from a remote system, check the creation time and source data time values to ensure that you are using the correct snapshot. The **Source Data Time** value of replicated snapshots reflects the original source data time, and the **Creation Time** value is updated to the time of replication.

ⓘ **NOTE:** Because the refresh operation replaces the contents of a storage resource, it is recommended to take a snapshot of the resource before refreshing it. Creating a backup allows you to revert to a previous point in time.

Before refreshing a snapshot, it is mandatory to shut down the application and unmount the volume or file system that is running on the production host, and then flush the host cache to prevent data corruption during the refresh operation.

Refresh a volume using a snapshot

About this task

To refresh a volume using a snapshot:

Steps

1. Open the volume list window.
2. Click the volume from which the snapshot was taken to open its Overview window.
3. Click the **Protection** tab, and then click **Snapshots**.
4. From the snapshots list, select the snapshot you want to use for the refresh operation.
5. Click **More Actions** > **Refresh using Snapshot**.
6. In the **Refresh using Snapshot** slide-out panel, select the volume or clone you want to refresh from the **Volume being refreshed** drop-down list.
7. Select whether to create a backup snapshot for the refreshed volume (the option is selected by default).
8. Click **Refresh**

Refresh a volume from a related volume

About this task

You can refresh a volume using a related volume (a clone or an indirect child snapshot).

Steps

1. Open the volume list window
2. Select a volume and then select **Repurpose** > **Refresh Using Related Volume**.
3. In the **Refresh using Related Volume** slide-out panel, click the **Select volume to refresh from** and select the source volume.
4. Click **Refresh**.

Refresh a snapshot of a file system

About this task

You can refresh a snapshot of a file system with its direct parent file system.

Steps

1. Open the file system list window.
2. Click the file system from which the snapshot was taken to open its Overview window.
3. Click the **Protection** tab, and then click **Snapshots**.
4. From the snapshots list, select the snapshot that you want to use for the refresh operation.
5. Click **More Actions** > **Refresh using Snapshot**.
6. Click **Refresh**.

Restore a storage resource from a snapshot

The restore operation is used to reconstruct an environment following an event that may have compromised its data. You can use the restore operation to replace the contents of a parent storage resource with data from a direct child snapshot. Restoring resets the data in the parent storage resource to the point in time at which the snapshot was taken.

Before restoring a snapshot, it is mandatory to shut down the application and unmount the file system that is running on the production host, and then flush the host cache to prevent data corruption during the restore operation.

If you restore a volume group, all member volumes are restored to the point in time associated with the source snapshot.

When restoring a resource from a snapshot that was replicated from a remote system, check the source data time value to ensure that you are using the correct snapshot.

Restore a volume or volume group from a snapshot

About this task

ⓘ **NOTE:** To prevent data integrity issues, before restoring a volume, it is mandatory to shut down applications that are using the volume and take the volume offline on the host.

Steps

1. Check the check box next to the volume or volume group that you want to restore.
2. Select **Protect** > **Restore from Snapshot**.
3. In the **Restore Volume from Snapshot** slide-out panel, select the snapshot to use for the restore operation.
4. Select whether to create a backup snapshot of the restored volume or volume group (the option is selected by default).
5. Click **Restore**.

Restore a file system from a snapshot

About this task

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

Steps

1. Check the check box next to the file system that you want to restore.
2. Select **Protect** > **Restore from Snapshot**.
3. In the **Restore File System from Snapshot** slide-out panel, select the snapshot to use for the restore operation.
4. Select whether to create a backup snapshot of the restored file system (the option is selected by default).
5. Click **Restore**.

Secure snapshots

Secure snapshots cannot be deleted before their expiration time. Use secure snapshots to protect your data from malicious attacks.

ⓘ **NOTE:** Secure snapshots are only supported for block snapshots that are created for volume or volume groups.

PowerStore enables you to generate secure snapshots. Unlike regular snapshots, secure snapshots cannot be manually deleted and are deleted only when they reach their expiration time.

ⓘ **NOTE:** If you want to use secure snapshots, it is recommended to review the business requirements with an administrator before proceeding, to avoid reaching the maximum snapshot limit.

Secure snapshots provide protection from accidental or malicious deletion of backup data and are effective against ransom attacks. Generating secure snapshots guarantees that you can restore data to a previous point in time.

To manually generate a secure snapshot for a volume or volume group, select the **Secure Snapshot** option in the **Create Snapshot** panel. To generate secure snapshots as part of a local protection policy, create a snapshot rule and select the **Secure Snapshot** option in the **Create Snapshot Rule** panel.

ⓘ **NOTE:** Be sure to set a retention period for the secure snapshots. The secure snapshot option is not available when **No Automatic Deletion** is selected.

ⓘ **NOTE:** When a volume group snapshot is configured as secure, all the members in the group are set as secure.

You can view and monitor secure snapshots by adding the Secure Snapshots column to the Snapshots table. You can also filter snapshot lists for secure snapshots.

It is possible to convert existing nonsecure snapshots to secure by selecting the **Secure Snapshot** option in the **Snapshot Details** panel. Similarly, you can convert a nonsecure snapshot rule to secure by selecting the **Secure Snapshot** option in the snapshot rule **Properties** panel.

ⓘ **NOTE:** Only snapshots created by the rule after modifying it to secure are secure snapshots. Snapshots created before the modification remain nonsecure.

When a secure snapshot rule is deleted or removed from a policy, or when a policy that includes a secure snapshot rule is unassigned from a resource, secure snapshots that were created by the rule remain secure and cannot be deleted until they expire. Volumes and clones that have secure snapshots cannot be deleted until the snapshots expire.

The expiration time of secure snapshots cannot be reduced but can be modified to a later date and time.

Secure snapshot and replication:

- For clusters running PowerStore version 3.5 and above, all secure snapshots that are generated on the local system are replicated as secure to the remote cluster.
- If the destination cluster is running a PowerStore version below 3.5, secure snapshots are replicated as regular snapshots on that cluster. In that case, the snapshot rule on the destination cluster is not secure. If failover occurs on a cluster running PowerStore version below 3.5, secure snapshots are not created for the storage resource.

After PowerStore upgrade to version 3.5, existing nonsecure snapshots and snapshot rules can be modified to secure.

If you must delete a secure snapshot that has not reached its expiration time, contact Dell support.

4

Protection Policies

This chapter contains the following information:

Topics:

Snapshot rules

You can create snapshot rules to control parameters such as the frequency of snapshot creation, and snapshots retention period. You can also create snapshot rules for generating secure snapshots. Snapshot rules, together with replication rules and remote backup rules enable you to configure and apply consistent data protection policies to storage resources based on the data protection requirements.

If you want to create a snapshot rule in addition to the existing rules, it is recommended to review the business requirements with an administrator before proceeding. This can help in achieving and maintaining consistent policies across the system.

Create a snapshot rule

Steps

1. Select **Protection** > **Protection Policies**.
2. In the **Protection Policies** window, click **Snapshot Rules** on the **Protection** bar .
3. In the **Snapshot Rules** window, click **Create**.
4. In the **Create Snapshot Rule** slide-out panel, enter a name for the new rule.
5. Set the following:
    - Select the days on which a snapshot will be created.
    - Set the frequency/start time:
        - For a snapshot to be taken at a fixed interval, select this option and set the number of hours after which a snapshot will be created.
        - For a snapshot to be taken at a particular time of the selected days, select the **Time of day** option and set the time and time zone.
    - Set the retention period.
    - To create secure snapshots, select the **Secure Snapshot** option. For details on secure snapshots, see Secure snapshots.

      NOTE: It is recommended to review the business requirements with an administrator before proceeding, to avoid reaching the maximum snapshot limit.
    - For file snapshots, select the file snapshot access type.
6. Click **Create**.

Replication rules

A replication rule is a set of parameters the system uses to synchronize data in a replication session. The parameters include selecting a replication destination and setting a recovery point objective (RPO).

After you have configured a replication rule, you can choose to use it in a new or existing protection policy, which then automatically changes or applies the replication session parameters for any storage resource that uses the protection policy.

You cannot change a protection policy to use a different replication rule with a different remote system. To change a protection policy with a replication rule using a different remote system, remove the old policy before assigning a new one.

NOTE: Changing a remote system requires a full synchronization.

If you want to create a new replication rule in addition to the existing rules, it is recommended to review the parameters and your business requirements with an administrator before proceeding. This can help in achieving and maintaining consistent policies across the system.

Create a replication rule

Steps

1. Select **Protection** > **Protection Policies**.
2. In the **Protection Policies** window, click **Replication Rules** on the **Protection** bar .
3. In the **Replication Rules** window, click **Create**.
4. In the **Create Replication Rule** slide-out panel, enter a name for the new rule.
5. Set the following:
   - Select an existing replication destination or configure a new destination.
   - Set the RPO.
   - Set the alert threshold.
6. Click **Create**.

Recovery point objective

Recovery point objective (RPO) indicates the acceptable amount of data, measured in units of time, that may be lost in case a failure occurs. When you set up a replication rule, you can configure automatic synchronization based on the RPO. Possible RPO values range from 5 minutes to 24 hours. The default RPO value is one hour.

NOTE: A smaller RPO interval provides more protection and consumes less space. However, it has a higher performance impact, resulting in more network traffic. A higher RPO interval may result in more space consumption, which can affect snapshot schedules and space thresholds.

Alert threshold

When you configure a replication rule, you can specify an alert threshold, which is the amount of time the system will wait before generating a compliance alert when a replication session does not meet the RPO. Setting the alert threshold to zero means that alerts will be generated if the actual synchronization time exceeds the RPO.

Remote backup rules

Create a remote backup rule and add it to a policy to enable remote backup.

A remote backup rule is a set of parameters that allow the PowerStore system to back up volumes and volume groups to a PowerProtect DD appliance. The rule specifies the destination system on which backups are created, the frequency of the backup operation and the retention time of the backups.

NOTE: Remote backup rules do not support secure snapshots.

After generating the remote backup rule, add it to an existing protection policy or generate a new policy.

NOTE: A protection policy can include only one remote backup rule.

Create a remote backup rule

Steps

1. Select **Protection** > **Protection Policies**.
2. In the **Protection Policies** window, click **Remote Backup Rules** on the **Protection** bar.
3. In the **Remote Backup Rules** window, select **Create**.
4. Set the following:
   - Rule name
   - Destination - Select a PowerProtect DD from the drop-down list or configure a new system (see Add a remote connection for remote backup.
   - Days of the week on which backup is created.
   - Frequency/Start time - Selecting **Every** sets the backup frequency in hours or days. Selecting **Time of Day** sets the backup frequency in days.
   - Retention period - Select the number of hours or days to keep the generated backups.

     ⓘ **NOTE:** Maximum retention is 25,550 days (70 years).
5. Click **Create**.

Create a protection policy

About this task

Create a protection policy to provide local and/or remote protection for your storage resources. Each protection policy can include one replication rule, one remote backup rule, and up to four snapshot rules. A rule can be in multiple policies.

Steps

1. Select **Protection** > **Protection Policies**.
2. In the **Protection Policies** window, click **Create**.
3. In the **Create Protection Policy** slide-out panel, enter a name for the new policy.
4. Optionally, select snapshot rules that you want to include in the policy or create a snapshot rule (see Create a Snapshot Rule).
5. Optionally, select a replication rule that you want to include in the policy or create a replication rule (see Create a Replication Rule).
6. Optionally, select a remote backup rule that you want to include in the policy or create a remote backup rule (see Create a remote backup rule).
7. Click **Create**.

Results

When you create a protection policy that includes a replication rule, the policy is automatically replicated to the remote system and assigned to destination resources created by the policy. The replicated policy and associated rules names consist of the policy and rules names on the source system, appended with the name of the remote system. Changes made to the original policy or included rules, are replicated to the remote system to maintain synchronization. After a replication failover, the replicated policy becomes active on the destination system.

The replicated policies and rules are managed by the system and are not displayed in the destination system policy and rules tables. However, you can see the rules details in the **Protection** tab of the replicating volumes or volume groups, by hovering over the replicated policy name. For protection policies that are assigned to metro volumes, an identical read-only policy is created on the remote system and can be viewed on the **Protection Policies** window of the remote system PowerStore Manager.

Modify a protection policy

You can modify a protection policy by adding and removing snapshot, replication, and remote backup rules.

About this task

NOTE: Changing the settings of a protection policy applies the new settings to all objects to which the protection policy is assigned. If you want to change the protection policy for one resource, it is recommended to create another protection policy, and assign it to that resource instead.

You cannot change the replication destination on a replication rule that is used in protection policies which are assigned to one or more storage resources. To reconfigure replication to a different remote system, unassign the protection policy and assign a new one with a different replication rule. Unassigning a protection policy with a replication rule deletes the associated replication session and assigning a new protection policy creates a session, which requires a full synchronization to the new destination.

Steps

1. Select **Protection** > **Protection Policies**.
2. Select the check box next to the relevant policy and click **Modify**.
3. In the **Properties** slide-out panel, you can modify the following parameters:
   - Policy name
   - Selected snapshot rules
   - Selected replication rules
   - Selected remote backup rules
4. Click **Apply**.

Assign a protection policy

Assign a protection policy to one or more storage resources to apply the snapshot, replication, and remote backup rules in the policy to the storage resources. The protection policy automatically performs snapshot operations, replication, and remote backup based on the specified parameters.

If a protection policy that meets your data protection requirements is available, you can assign it to a storage resource at any time.

You can assign a protection policy to a storage resource during the resource creation or at a later stage.

For block storage protection:

- Assign protection policies containing snapshot, replication, and/or remote backup rules to volumes and volume groups.
- When you assign a new protection policy that contains a replication rule to the storage resource, a complete initial synchronization is required.
- With remote backup, assigning a policy that includes a remote backup rule to a volume or a volume group, automatically creates a remote backup session in Idle state.
- If a policy that includes a remote backup rule is assigned to a resource that does not support remote backup, the rule is ignored.
- With metro volumes, you can assign only protection policies that include snapshot rules. A policy that includes a replication rule cannot be assigned to a metro volume.

For file storage protection:

- PowerStore supports local protection (snapshots) at the file system level and remote protection (replication) at the NAS server level.
- You can assign a protection policy to a NAS server only if it includes a replication rule. The replication rule is applied to all file systems on the NAS server and snapshot rules (if such exist) are ignored.
- You can assign a protection policy to a file system only if it includes a snapshot rule. The snapshot rule is applied to the file system and a replication rule (if such exists) is ignored.

Assign a protection policy to a storage object

About this task

Assign a protection policy to a volume, volume group, file system, or NAS server.

Steps

1. Select the check box of the storage resource to which you want to assign a protection policy.
2. For volumes, volume groups, and file systems, select **Protect** > **Assign Protection Policy**. For NAS servers, select **More Actions** > **Assign Protection Policy**.

   > ⓘ **NOTE:** If you selected an invalid resource, the assign option is inactive. Hovering over the **Assign Protection Policy** displays a tooltip explaining why it is invalid for this action.

3. From the **Assign Protection Policy** slide-out panel, select the protection policy.
4. Click **Apply**.

Assign a protection policy to multiple storage objects

About this task

Assign a protection policy to multiple storage objects of the same type (volumes, volume groups, file systems, or NAS servers).

Steps

1. Select **Protection** > **Protection Policies**.
2. Select the checkbox a policy from the list and then select **More Actions** > **Assign Protection Policy**.

   The **Assign Protection Policy** slide-out panel provides a summary of all the storage resources that are already have an assigned protection policy.
3. From the **Assign Protection Policy** slide-out panel, select the resource type and then select the relevant objects from the resource list.
4. Repeat Step 3 if you want to assign the selected policy to additional resource types.
5. Click **Assign**.

Change the protection policy assigned to a storage object

About this task

Consider the following guidelines for replication rules:

- Replacing a protection policy that includes a replication rule with a policy without a replication rule removes replication from all the resources that are assigned with that policy.
- Replacing a protection policy that includes a replication rule with a policy that has the same replication rule enables you to reconfigure local protection without disrupting replication.
- Replacing a protection policy that includes a replication rule with a policy with a different replication rule is possible only if both policies have the same remote system configured.

  > ⓘ **NOTE:** To change assignment of a protection policy with a replication rule using a different remote system, remove the old policy before assigning a new one.

Consider the following guidelines for remote backup rules:

- Replacing a protection policy that includes a remote backup rule with a policy without a remote backup rule removes remote protection to the DD remote system.
- Replacing a protection policy that includes a remote backup rule with a policy that has the same remote backup rule causes the next backup to be a full backup (and not incremental).
- Replacing a protection policy that includes a remote backup rule with a policy with a different remote backup rule and the same remote system causes the next backup to be a full backup (and not incremental).

Steps

1. Select the relevant storage resource to open its **Overview** window.
2. Click the **Protection** tab.
3. Next to the assigned protection policy name, click **Change**.
4. In the **Change Protection Policy** slide-out panel, select a different protection policy.
5. Click **Apply**.

Unassign a protection policy

Prerequisites

Removing the protection policy from a storage resource results in the following:

- Scheduled snapshots and replication, based on the rules that are associated with the policy stop.
- Existing snapshots remain, and are retained in the system, based on the snapshot rule settings when they were created.
- The destination storage resource stays in read-only mode. You can clone the destination storage resource to get a read/write copy or change the **replication destination** attribute in the **Properties** page of the storage resource.

ⓘ **NOTE:** You cannot unassign a protection policy while importing is in progress.

Steps

1. Select the check box of the storage resource to which you want to assign a protection policy.
2. For volumes, volume groups, and file systems, select **Protect** > **Unassign Protection Policy**. For NAS servers, select **More Actions** > **Unassign Protection Policy**.
3. Click **Unassign** to confirm.

5

Replication

This chapter contains the following information:

Topics:

Synchronization

PowerStore enables you to asynchronously update the destination resource with changes (such as changes in content, size, and membership) that occurred on the source resource since the last synchronization cycle.

Synchronization can occur either automatically - according to a set schedule - or manually. Snapshots are synchronized from the source system to the destination system, and maintain block sharing efficiency.

ⓘ **NOTE:** Virtual volume synchronization is supported only for Read-Only snapshots.

When a volume on the destination system is mapped to a host, the system sets the node affinity for this volume, and as a result, all I/Os are automatically directed to the selected node. You do not need to pause and resume the replication session for the I/O redirection to take effect. Setting node affinity for volumes on the destination system provides load balancing and prevents latency of replication. You can set the node affinity manually using REST API.

ⓘ **NOTE:** If you cannot see the node affinity column in the Volumes table, add it using the **Show/Hide Table Columns**.

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

For NAS servers, all file systems on a protected NAS server are synchronized from the source to destination system. When file systems are modified during an asynchronous replication session, the changes are reflected on the destination system at the next synchronization cycle.

You can synchronize a replication session when it is in the following states:

- Operating normally
- System paused

While a replication session is synchronizing, you can take the following actions:

- Perform a planned failover from the source system.
- Perform a failover from the destination system.
- Pause replication sessions from the source or destination system.
- Delete a replication session by removing a protection policy.

If synchronization fails, the replication session is placed in a system paused state. When the system recovers, the replication session continues from the same point as when the system was paused.

Failover

Failing over a replication session includes switching roles between the source and destination systems and reversing the direction of the replication session.

There are two types of failovers:

- Planned failover - User initiated, includes synchronization between source and destination to prevent data loss.
- Unplanned failover - Initiated by the destination system in response to source system failure.

During a replication session failover, the system performs the following actions:

- Stop I/Os on the source object.
- Synchronize the source and destination storage objects (occurs only in a planned failover).
- Stop the replication session.
- Reverse roles between source and destination systems.
- Promote the latest object version on the new source.
- Resume I/Os on the new source (initiated by the user).

After a failover, you can access applications on the new source system to recover data.

Perform a failover test

After you set up a replication session, you can test the connection to ensure that your sites are correctly configured and prepared for disaster recovery.

During a failover test, the system performs a failover and production access is provided to the destination site using replicated data or a point-in-time snapshot. The destination storage resource is available in read/write mode, and production access is enabled for hosts and applications. You can verify your disaster recovery configuration while replication continues to run in the background.

When you wish to stop the failover test, select one of the following actions:

- Failover to the current test data - If you made changes to the data during the failover test, you can use the updated test data. This will stop the test and preserve the test data. Any data replicated from the source during the test will be discarded and the destination system will become the source.

  NOTE: You must acknowledge these changes before failing over to the test data.
- Stop the failover test - When you stop the test, production access to the destination will be disabled for hosts and applications and the destination storage resource will be updated with the latest data synched from the source system. You can create a backup snapshot of the test data before stopping the failover test.

Restrictions

A failover test can only be performed under the following conditions:

- The PowerStore version on both the source and destination system is 2.x or later.
- The replication session state is not Initializing, Failing Over, Failed Over, Paused for NDU/Migration, or Failover Test in Progress.

During the failover test, you cannot execute the following actions on the destination system:

- Change volume group membership
- Increase volume group size
- Change volume group name
- Start migration
- Remove a protection policy

NOTE: You can still perform these actions from the source system.

You cannot perform a planned failover while a failover test is in progress. Stop the failover test to perform a planned failover. However, unplanned failovers may still occur uninterrupted in response to a disaster. If possible, it is recommended to stop the failover test before an unplanned failover, because any data replicated to the destination after the failover test started will be lost.

You can also pause and resume replication sessions during a failover test. If you delete a replication session during a failover test, the test will be cancelled.

Start a failover test

You can start a failover test from the current destination data, or from any snapshot.

There are two ways to start a failover test:

- From **Protection** > **Replication**, select the replication session you want to test, then select **Start Failover Test**.
- From the **Protection** tab of the resource, select **Replication**, then select **Start Failover Test**.

After the failover test starts, an alert is raised on the replication session. The alert is cleared after the test is stopped.

Stop a failover test

Before you stop the failover test, it is recommended that you unmount file systems and stop any running applications on the destination resource to avoid data corruption.

There are two ways to stop a failover test:

- From **Protection** > **Replication**, select the replication session that has a test in progress, then select **Stop Failover Test**.
- From the **Protection** tab of the resource with a test in progress, select **Replication**, then select **Stop Failover Test**.

You can also choose to create a snapshot to save the test data that was created during the failover test.

Planned Failover

When you perform a planned failover, the replication session is manually failed over from the source system to the destination system. Prior to the failover, the destination system is synchronized with the source system, to prevent any data loss.

Before performing a planned failover, make sure that you stop I/O operations for any applications and hosts. You cannot pause a replication session that is undergoing a planned failover.

During a planned failover, you can take the following actions:

- Perform an unplanned failover.
- Delete the replication session by removing the protection policy on the storage resource.

You cannot initiate a planned failover when a failover test is in progress.

You can initiate a planned failover test from the current source data, or from any snapshot.

There are two ways to initiate a planned failover:

- From **Protection** > **Replication**, select the relevant replication session, and then select **Planned Failover**.
- From the **Protection** tab of the resource, select **Replication**, and then select **Planned Failover**.

After a planned failover, the replication session is inactive. To synchronize the destination storage resource and resume the replication session use the **Reprotect** action. You can also select the auto-reprotect option before failing over, which automatically initiates the synchronization in the opposite direction (at the next RPO) after the failover is complete, and returns the source and the target system to a normal state.

Network disconnection during DRT

When performing DRT, it is not recommended to simulate a network failure between the local and remote systems, and then perform an unplanned failover to the destination system to enable access to the DR NAS server. Since there is no communication between the systems, PowerStore cannot ensure that both NAS servers are in a compatible state. After connection is restored, both NAS servers are in production mode (split brain). As a result, both systems switch to maintenance mode to prevent data from being written to both locations.

To resolve this state, Technical Support intervention is required.

For more information, see Dell Knowledge Base Article 000215482 (Cutting the network connection between sites...).

Unplanned Failover

Unplanned failover occurs following source system events such as source system failure, or events that leads to downtime for production access. Unplanned failover is initiated from the destination system, and provides production access to the original destination resource from a point-in-time snapshot.

When you initiate an unplanned failover, you can select whether to use the most recent data copy or a snapshot of the data (if available) as the data source.

When the connection to the source system is re-established, the original source resource is placed into destination mode. Use the **Reprotect** option to synchronize the destination storage resource, and then resume the replication session.

ⓘ **NOTE:** When performing file replication, it is not recommended to modify the file mobility network after performing an unplanned failover. After the connection between the source and destination systems is restored, the result may be that both NAS Servers are in production mode.

Additional considerations for replication

During block replication, when the source system is paused for NDU and the destination system is up, the destination system status is changed to *System_Paused*. If the destination system is down during the source system NDU, when the destination system is up again, its status remains *OK*.

During file replication, when the source system is paused for NDU, the destination system remains in *OK* state regardless of its connectivity status.

Testing disaster recovery for NAS servers under replication

A disaster recovery test performs a disaster recovery plan that enables you to check that the system can recover and restore data and operation if disaster occurs.

PowerStore provides several options to test the ability of the system to recover from a disaster and regain functionality:

- Clone a NAS server for disaster recovery testing using unique IP addresses.
- Clone a NAS server for disaster recovery testing using an isolated network with duplicate IP addresses.
- Planned failover (see section above).

Clone a NAS server for disaster recovery testing using unique IP addresses

About this task

Cloning a NAS server is the recommended option for testing DR. You can clone the NAS server using the PowerStore Manager and test it without impacting production. To enable access to the newly cloned NAS server, it is required to configure a new and unique network interface. The configured IP address cannot be in use on either the source or destination NAS servers. Unique settings are also required for joining the server to an AD domain.

Changes that are made on the cloned file systems and on production file systems do not impact each other. When the DR test is complete, the cloned server can be deleted.

You can choose one of the following options:

- Clone the NAS server on the source system, replicate it to the destination, and perform a planned failover to the destination system.
- Clone the NAS server on the destination system and access the data (failover is not required because the cloned resources are already accessible on the destination system).

Steps

1. In the PowerStore Manager, select **Storage** > **NAS Servers** .
2. Select the NAS server that you want to clone, and then select **Repurpose** > **Clone NAS Server**.
3. In the **Create Clone** window, provide a name for the clone and select the file systems that you want to clone.
4. Select **Create**.
   The cloned NAS server is added to the servers list.
5. Select the cloned NAS server name to open the server details window.
6. To add a file interface:
   a. Select the **Network** tab.
   b. Under **File Interface** select **Add**.
   c. Provide the interface information and select **Add**.

7. To set the sharing protocol:
    a. Select the **Sharing Protocols** tab.
    b. Select the relevant protocol (SMB, NFS, or FTP).
    c. Configure the necessary information and select **Apply**.
8. If you cloned the source NAS server:
    a. Replicate the NAS server to the destination system. For details, see Replication.
    b. Perform a planned failover to the destination. For details see, Planned failover.
    c. Check if the host can access the data.
9. If you cloned the replicated production server on the destination system, failing over is not required. Verify host access.

Clone a NAS server for disaster recovery testing using an isolated network with duplicate IP addresses

It is possible to test disaster recovery using the same configuration as production. Using identical settings may reduce risk and increase reproducibility in a failure scenario. However, using duplicate IP addresses creates conflicts. Running the DR test on an environment that is isolated from the production environment enables you to avoid these conflicts.

As of PowerStore version 3.6, you can create an isolated Disaster Recovery Testing environment (DRT) to help you be prepared for a disaster.

Creating an isolated environment enables you to use the same IP address and hostname as the production system, and perform a DRT for a NAS server under replication without any impact on production.

To create a DRT environment, you must set up an isolated network with a separate DRT router and to create link aggregations with the network I/O ports.

Using PSTCLI or REST API, create a dedicated networking environment on the destination server by cloning the NAS server under replication on the destination PowerStore system. The clone is a full copy of the production environment and a dedicated test environment, which is isolated from production. You can create an isolated networking environment and configure the test environment with the same IP address and hostname as the production system. The DRT NAS server has no impact on the production environment, and can run without IP address conflicts when failover and failback occur on the replication NAS server.

To test DR using an isolated test environment:

1. Create the NAS server clone on the destination. Use the `is_dr_test` flag.
2. Create a user bond interface for NAS using the same IP address as the Source NAS server.
3. Join the clone to the AD (if required).
4. Verify that hosts can access the data.

ⓘ **NOTE:** You can also use DRT on stand-alone NAS servers.

Pre-requisites and limitations

To create a DRT environment, ensure that the following requirements are met:

- Acquire the private network information:
    - Gateway
    - Netmask
    - VLAN ID (optional)
- Identify the network ports of the isolated network and the network ports of the production network.

Note the following limitations when creating a DRT environment:

- Bond interface dedicated to DRT cannot be used to create any other production NAS servers.
- A NAS server that is configured as production cannot be reconfigured as part of the DRT.
- A NAS server that is configured as part of the DRT cannot be reconfigured as production.
- A NAS server that is no longer a part of a DRT cannot be reconfigured, and must be deleted.
- After a NAS server is active and configured with network information, additional configuration (such as DNS, CAVA, and Kerberos) should be done manually.
- DRT-enabled NAS server cannot be replicated.
- Modifying and deleting the NAS server can be done using the PowerStore Manager.

Configure the disaster recovery test environment using PSTCLI

Steps

1. Acquire the name of the NAS server on the destination site (to be cloned):

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+-------------+--------+--------------------+-------------------
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

2. Clone the NAS server by providing a new name for the clone and using the `-is_dr_test true` switch:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server -name File80
clone -name File80_c -is_dr_test true
Success
```

3. Find the IP port ID for the NAS File Bond that is connected to the isolated network:

   ⓘ **NOTE:** If the NAS File Bond was not created, you can create it using PSTCLI or PowerStore Manager.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> ip_port_show -output nvp
8:   id =IP_PORT23
     current_usages =
     ip_pool_addresses =
     bond:
     name=BaseEnclosure-NodeA-bond1
```

4. Create the file interface for the cloned NAS server:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface create
-nas_server_name File80_c -ip_address "10.10.10.10" -prefix_length 24 -gateway
"10.10.10.1" -vlan_id 5
-ip_port_id IP_PORT23
Created
# |     id
--+-----------------------------------
1 |64830ae5-2760-59ce-4c90-82772509648e
```

5. View file interface:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+-------------+--------+--------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

Configure a NAS server in a DRT environment using REST API

About this task

ⓘ **NOTE:** If you are not using REST API, skip this section.

Steps

1. To clone the NAS server in the specified namespace, run `/nas_server/{id}/clone`, and specify `is_dr_test` as true.
2. To create a network interface, run `/file_interface` and specify the private network parameters.

ⓘ **NOTE:** This step creates the file interface for the cloned NAS server using the same IP address, netmask, and gateway as the production NAS server. Use the bond interface/IP_Port that is associated with the private network.

Results

The NAS server is up and can be used for DRT in the isolated network.

Virtual volumes replication

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

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

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

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

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

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

To view the details of a virtual volume replication session:

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

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

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

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

Pre-requisites

Before configuring virtual volume replication, ensure that the following pre-requisites are met:

- Both local and remote system must be connected and must have vVol capability (see Remote systems).
- Storage containers must be defined on both systems (**Storage** > **Storage Containers** > **Create**) so that they can be paired. If there is a single storage container on each system, the storage containers are paired automatically. Otherwise, it is required to manually specify the storage container destination (**Storage** > **Storage Containers** > **[storage container]** > **Protection** > **Create**).

Create a virtual volume replication session

About this task

For information about the required configuration on vSphere, see VMware SRM user documentation.

Steps

1. On PowerStore, create a replication rule.

   The replication rule is exposed to vCenter as a Replication capability.
2. On vSphere, create a policy using the exposed rule.

A read-only copy of the protection policy, with an identical name, is added to PowerStore (visible on the **Protection Policies** table and marked with a lock icon.

ⓘ **NOTE:** You can also add snapshot rules to enable local protection.

ⓘ **NOTE:** It is not possible to create, modify, or delete a read-only protection policy, and to assign or unassign the policy to virtual machines using PowerStore. To perform this actions, use Storage Policy update in vSphere.

3. On vSphere, create a virtual machine, assign a storage policy with a replication rule to it, and associate it with a replication group.

Results

The replication group and replication session are created automatically in PowerStore (visible under **Protection** > **Replication** > **[replication group session]**.

Monitoring replication group performance

When a storage policy that includes a PowerStore replication rule is created on VMware and assigned to a vVol-based VM, a replication session is created on PowerStore for the vVol resources in the same resource group. VMware SRM uses these VMware resource groups to manage the protected VMs in replication groups.

You can monitor the performance of a replication group from PowerStore. Select **Protection** > **Replication** and click the session status of a vVol replication session to display the session details (the **Resource Type** should be *Replication Group*. Click the **Replication Group Performance** tab to display performance data for the replication group. You can select to view graphs of the following data:

- Replication Remaining Data
- Replication Bandwidth (Normalized)
- Replication Transfer Time

You can also set the timeline for the displayed data.

Virtual machine recovery

Site Recovery Manager (SRM) is a VMware disaster recovery solution that automates the recovery of virtual machines during failure states.

To enable virtual machine recovery, it is required to configure a recovery plan using SRM. A recovery plan runs predefined recovery steps on selected replication groups. The recovery steps include failover, reprotect, and failover test.

A protection group is created on vSphere, that includes one or more replication groups and a recovery plan. If failure occurs, the SRM runs the recovery plan on the virtual volumes in the replication groups.

In PowerStore, you can monitor the replication session status during recovery.

For additional details, see *VMware Site Recovery Manager*.

6

Metro Protection

This chapter contains the following information:

Topics:

Pre-requisites and limitations

Before configuring metro, consider the following limitations:

- Metro support is available only with PowerStore T model appliances. Metro is not supported with PowerStore X model appliances.
- Metro protection is enabled only for volumes.
- Metro protection supports FC/SCSI or iSCSI connected VMware ESXi hosts.
- Metro witness is not supported with HCI deployments of PowerStore.

When a connection to a remote system is established, the system automatically detects the configuration and enables the supported capabilities for the remote system. To enable block metro capability, ensure that the following conditions are met on both PowerStore systems:

- The two systems are running PowerStore 3.x or later.
- The latency on the remote system is low.
- The data connection type is TCP - When local and remote PowerStore systems running version 3.x (or later) are installed , TCP connection is automatically supported. However, when one or both of the PowerStore systems are running version 2.x, you must upgrade the systems to 3.x to enable metro. Following the upgrade, an alert is displayed, requiring you to update the remote system connection type. Click the link in the displayed alert to open the **Update Remote System Transport** window. Then, click **Update Transport**.

  NOTE: The alert is cleared only after transport is updated.

To deploy a witness, ensure that the following pre-requisites are met:

- The witness must be installed on a Linux host (virtual or physical).

  NOTE: It is highly recommended to deploy the witness on a third fault domain, which is separated from the two PowerStore systems.
- Supported operating systems:
  - Red Hat 8.8
  - SUSE Linux Enterprise Server (SLES) 15 SP5
- Dependencies (required on the Linux host):
  - Java 11
  - SQLite

  NOTE: When using a package manager (such as yum or zypper), the listed dependencies are installed automatically.

- Hardware:
  - The operating system must be running on an x64 CPU architecture.
  - A minimum of 4 GB RAM
  - A minimum of 5 GB available disk space
- Ports:
  - Port 443/tcp must be open on the witness host before installing the witness.
  - Datacenter firewalls must allow traffic on port 443 to enable PowerStore to send requests to the witness.
- Network latency - Maximum latency of 100 millisecond on the management network between PowerStore and the witness
- User account access - root or sudo access is required to install the witness on the host.
- Ensure connectivity to the PowerStore Management network.
- For a virtual witness, it is recommended to use a static IP address for the witness VM. However, if you are using DHCP, add the witness to PowerStore using the Fully Qualified Domain Name (FQDN).

Configure host connectivity

NOTE: Host support is provided for VMware vSphere metro storage cluster. Both Fibre Channel and SCSI connectivity are supported.

Host metro connectivity is configured on a local and remote PowerStore systems and enables hosts and applications to perceive physical volumes from the two systems as a single volume. When you configure metro connectivity for the host, select the preferred array to determine which system retains access to the storage if failure occurs.

An ESXi host must be defined on both the local and remote systems and be connected to both systems to enable host metro connectivity.

When you create an ESXi host, the **Add Host** wizard enables you to set the host connectivity:

NOTE: The host connectivity options are graphically demonstrated in the **Add Host** wizard.

- **Local Connectivity** - Provides host access only to the local system.

  NOTE: Local connectivity can also be used with metro volumes.
- **Metro Connectivity** - Provides host access to both local and remote systems. If you select this option, set system access:
  - **Host is co-located with this system** - Host path latency is lower for the local system and higher for the remote system. The host always attempts to send I/Os to the local system (except for when the local system is down).
  - **Host is co-located with the remote system** - Host path latency is lower for the remote system. The host always attempts to send I/Os to the remote system (except when the remote system is down).
  - **Co-located with both systems** - Latency and performance of host path are equal for both local and remote systems. The host sends I/Os to the local or remote systems, based on its multipath considerations.

NOTE: Regardless of the configured connectivity, all hosts must be configured on the same vCenter cluster.

NOTE: For an ESXi host mapped to a metro volume, it is recommended to use round robin Path Selection Plugin (PSP) with latency mode enabled.

NOTE: In case one of the systems goes offline, the ESXi host enters an All Paths Down (APD) condition. To resolve this condition, it is recommended to configure vSphere HA. This configuration enables virtual machines on available ESXi hosts to restart and resolve the APD condition.

Metro witness

As of PowerStore version 3.6, you can add a witness server to metro protection to provide protection from single failure scenarios.

The witness server is a passive third party that is installed on a stand-alone host (preferably in another data center). When failure occurs, the local and remote PowerStore systems contact the witness server and request to fracture the metro session. The witness then determines which system remains accessible to hosts and continues to service I/Os. If possible, the witness gives precedence to the PowerStore system that was assigned with the preferred role. Adding the witness to a metro session provides protection from single failure scenarios, including preferred system failures which are not handled without a witness.

The witness service is simple and does not maintain critical data that cannot be re-created. As such, there is no need to backup, save, or recover the witness, and it can be removed and reinstalled whenever recovery is required.

Deploy the metro witness

If the pre-requirements are met, you can use RPM to directly install the witness. Otherwise, you can use a package manager (yum, zypper) to automatically install the dependencies. You can download the installation package from the Dell Support page.

To install the witness service on a Linux host, run the following command:

```
sudo rpm -i <rpm_file>
```

NOTE: You can use a package manager or RPM to uninstall the witness.

NOTE: Witness is not supported with HCI deployments of PowerStore.

Configure the metro witness

About this task

- Only Administrator, Security Administrator, and Storage Administrator are authorized to configure the witness.
- You can configure witness before or after configuring metro.
- Only one witness can be configured per metro cluster.
- The configured metro is used for all metro sessions and cannot be disabled for specific sessions.
- The witness status changes to Engaged only after it is configured for both local and remote PowerStore systems.
- To access the witness server installation tools (secure token generator and thumbprint), use the path:

  ```
  sles15:~ # ls /opt/dell-witness-service/scripts
  ```

NOTE: Perform the following steps for both local and remote PowerStore systems.

Steps

1. In the PowerStore Manager, select **Protection** > **Witness**.
2. In the **Metro Witness** window, select **Add**.
3. In the **Add Witness** window, configure the following fields:
   - Name
   - IP Address/FQDN
   - Security Token - To generate a security token, run the generate_token.sh script. For details see *PowerStore Security Configuration Guide* on the PowerStore Documentation page.

     NOTE: The token expires in ten minutes.
   - Description (optional)
4. Select **Add**.
5. In the **User Authorization** window, review the witness certificate thumbprint, and select **Confirm** to accept.

   NOTE: For details, see *PowerStore Security Configuration Guide* on the PowerStore Documentation page.

   The certificate is saved on the PowerStore system.

Results

The witness is created and all existing metro volumes are automatically assigned to it. Newly created metro volumes are automatically assigned to the witness. The **Metro Resources** column in the **Metro Witness** window shows the number of resources that are assigned to the witness. Clicking the number opens the **Metro Resources** window.

Witness modification and recovery

The witness service is simple and does not maintain critical data that cannot be re-created. As such, it is not necessary to backup, save, or recover the witness, and it can be removed and reinstalled whenever recovery is required.

Modify the witness parameters

About this task

From the **Witness Properties** window, you can modify the witness name and description.

ⓘ **NOTE:** If you want to change the witness IP address or FQDN, you must remove and reinstall the witness.

Steps

1. Select **Protection** > **Metro Witness**.
2. Select the checkbox next to the witness and select **Modify**.
3. Modify the necessary fields and select **Apply**.

Replace the witness

About this task

To replace the witness, remove it from the PowerStore systems and then add it. This procedure is required even if the hostname or IP address have not change, since the new witness has a different certificate that must be added to the PowerStore systems.

Steps

1. Remove the witness from each of the PowerStore systems. For details, see Remove the witness.
2. Add the witness to each of the PowerStore systems. For details, see Configure the metro witness.

Modify witness host configuration

If the host on which the witness is installed must be modified, you can do one of the following:

- Create a host with the required configuration and install the witness. Then remove the existing witness from the PowerStore systems and replace it with the new witness.
- Modify the existing host:
    - Remove the existing witness from the PowerStore systems. For details, see Remove the witness.
    - Uninstall the witness from the existing host.
    - Make the required configuration changes on the host.
    - Reinstall the witness on the host. For details, see Deploy the metro witness.
    - Add the witness to the PowerStore systems. For details, see Configure the metro witness.

Monitor the witness

Selecting **Protection** > **Metro Witness** > **[witness]** displays the witness properties.

The witness maintains communication with every node on every appliance.

The witness **Properties** window displays the connection state for each node and the overall connection state of the witness.

Possible connection states:

- Initializing - All nodes are initializing the connection to the witness.
- OK - All nodes can communicate with the witness.
- Deleting - The witness is being deleted from the cluster.
- Partially Connected - Some nodes on some appliances can communicate with the witness, or the same witness is not registered on the peer system.
- Disconnected - All nodes cannot communicate with the witness.

After the witness is configured, each metro session independently attempts to engage with it. Each metro session has a state which indicates whether the metro session can use the witness when failure occurs. Possible witness states for a metro session:

- Initializing - The witness is initializing but not engaged.
- Disengaged - The metro session is paused or fractured.

- Engaged - All nodes on all appliances are connected to the witness and can use it if failure occurs.
- Disengaged Invalid Configuration or Unavailable - The witness configuration is invalid (for example, witness is configured only on one PowerStore system, or two different witnesses are configured on the local and remote systems), or the witness is unavailable.
- Disengaged Failed to Initialize - The witness failed to initialize with the metro session.
- Unconfigure in Progress - The witness is being removed from the PowerStore system.

When the cluster has multiple appliances, some of the appliances may be connected to the witness while others are not. As a result, the witness may not be engaged for all existing metro sessions.

Remove the witness

You can remove the witness from PowerStore at any point, regardless if it is assigned to metro sessions.

To remove the witness, select **Protecton** > **Metro Witness**, then check the box next to the witness and select **Delete**.

Deleting the witness, removes it from all metro sessions and the sessions revert to using preference rules as a means to determine system behavior if failure occurs.

If an error occurs during the deletion of the witness, it remains in Unconfigure in Progress state until the error is resolved and then resumes deletion.

Witness - failure scenarios

When a failure occurs in a metro environment with witness, the system behaves as follows:

When connection between the local and remote systems is lost, the metro session is fractured. Both systems request to fracture the witness session. The witness responds with Success to the first request and Error to the second request. The system that received Success as a reply, maintains host I/O access to the metro volume while the system that received Error demotes itself.

The nonpreferred system sends the request to the witness a few seconds after the preferred system. As a result, if the preferred system is up, it receives the Success response and is selected to maintain host I/O access.

If the preferred system is down, it does not send a request to the witness, and the nonpreferred receives the Success response.

When one of the systems loses connection to the host, there is no impact since both systems are still up, and the host can access them. If connection loss between the system occurs, the system that still has connection to the witness receives a Success response and maintains host I/O access.

Configure a metro volume

About this task

Enabling metro configuration for a volume makes it visible to hosts from two PowerStore systems with a remote system connection.

The following volumes cannot be configured as metro:

- A volume clone
- A volume that is assigned with a protection policy that includes a replication rule
- A volume that is a member of a volume group
- A volume with a read-only protection policy
- A volume that is being migrated or imported
- A volume that is a read-only replication destination, left after replication is removed

ⓘ **NOTE:** If a witness was configured for this PowerStore system, the metro volume is automatically assigned to the witness.

Steps

1. Select **Storage** > **Volume** and select the checkbox of a volume.
2. Select **Protect** > **Configure Metro Volume**.
   The **Configure Metro Volume** slide-out panel is displayed.
3. Select a remote system or configure a new remote system.

4. Optionally, select the placement of the volume on the remote system.
5. Click **Configure**.
6. On the remote system, map the configured metro volume to a host.

Setting metro role

The system from which the metro volume is configured is automatically set as preferred upon metro volume configuration. When the metro volume is fractured or paused, and if metro witness is not configured, the preferred system keeps host and production access and an active association with a protection policy.

When the metro volume state is Operating Normally (active/active), you can change the metro volume role from preferred to nonpreferred or nonpreferred to preferred using the following options:

- **Modify Preferred Role** - Use this option to change the current role of a selected metro volume. This option can be used from both the preferred or nonpreferred system.

  ⓘ **NOTE:** This option is in the metro volume details window.
- **Set Local Role to Preferred** - Use this option to set the role of multiple selected nonpreferred metro volumes to preferred. This option should be used before shutting down the preferred system for planned maintenance. Setting the nonpreferred metro volumes to preferred allows the metro volume to continue host and production access during the shutdown.

Monitor metro resources

About this task

You can monitor all the metro objects in the system and perform actions on selected resources or monitor the status of a selected metro volume.

Steps

1. From the Dashboard, select **Protection** > **Metro** to open the list of metro resources and details.

   ⓘ **NOTE:** If metro witness is configured, you can also access the metro resource list by selecting **Protection** > **Metro Witness** > **Metro Resources**.
2. Select the checkbox of a metro resource to view the possible actions that you can perform on that resource.
3. To view detailed information about a specific metro resource, click the status of the resource in the **Metro Status** column.

   You can also view detailed information about a metro resource from the **Storage** > **Volumes** page:

   a. Click the name of a metro volume on the **Storage** > **Volumes** page to display the volume information page.
   b. Select the **Protection** card and then select the **Metro Volume** tab to display the metro volume information.

Pause a metro volume

About this task

Temporarily pausing a metro volume is required in the following scenarios:

- When there are required configuration changes that cannot be performed when the volume is operating normally, such as changing the volume properties.
- When the preferred or nonpreferred systems require maintenance, such as replacement of faulty hardware components or changes in network infrastructure.
- When there is a failure on the preferred system that requires promoting the nonpreferred system to enable controlled recovery.

Pause can be initiated from either the preferred or nonpreferred system. When a metro volume is paused, the synchronization between the systems is temporarily stopped. Production access and protection policies remain active on the preferred system.

When a metro volume is fractured, and there is no connection between the local and remote system, pause is implemented only on the local system (where it was implemented):

- When pause is initiated from the preferred system

    - Host and production access remains enabled on a paused, preferred metro volume.
    - Host and production access remains unchanged on the nonpreferred metro volume.
- When pause is initiated from the nonpreferred system:
    - Host and production access remains disabled, unless the metro volume has been promoted.
    - Since there is not network connectivity, the pause does not modify the preferred metro volume state.
- When connectivity is resolved, pause should be initiated from the remote system as well.

Steps

1. Select **Protection** > **Metro**.
2. Select the check box of the metro volume to pause and click **Pause**.
   The **Pause Metro Volume** slide-out panel is displayed.
3. Click **Pause** to confirm.

Resume a metro volume

About this task

Resume can be initiated either from the preferred or from the nonpreferred system.

When you resume a preferred, paused metro volume, the preferred system starts synchronizing data with the nonpreferred system. After synchronization is complete, the Metro volume status returns to an active/active state.

When you resume a promoted (previously nonpreferred), paused metro volume, the nonpreferred system starts synchronizing with the preferred system (Reprotecting state) to return to active/active state.

ⓘ **NOTE:** If a metro volume was paused for a long time, synchronization may take a while due to data accumulation on the preferred system.

If the nonpreferred system was promoted, resuming the metro volume from the promoted nonpreferred system synchronizes data from the promoted nonpreferred system to the preferred.

Steps

1. Select **Protection** > **Metro**.
2. Select the check box of the metro volume to resume and click **Resume**.
   The **Resume Metro Volume** dialog box is displayed.
3. Click **Resume** to confirm.

Promote a metro volume

Prerequisites

Promoting a metro volume is allowed in a `Fractured` or `Paused` state.

About this task

When the link between the two storage systems fails or when the nonpreferred system is down, the synchronization between the systems is stopped and the metro volume becomes fractured. The preferred system remains active and continues to service I/Os. If the user is on the preferred system, no action is required and the systems synchronize when the issue is resolved.

When a failure occurs on the preferred system, the synchronization between the systems is stopped and the metro volume becomes fractured. Both systems stop servicing I/Os. To be able to access the metro volume, the user must promote the metro volume on the nonpreferred system to enable host and production access to it until the preferred system recovers. If the user verifies that the preferred system is available, the metro volume on the nonpreferred system can be promoted with no implication. When the user is on the nonpreferred system, it is not possible to know the status of the preferred system (whether the system is down or the link between the system is down). In this case, promoting the metro volume on the nonpreferred system may result in a situation where both systems continue to service I/O but do not synchronize.

Steps

1. Select **Protection** > **Metro**.

The Metro page lists all the metro resources and enables you to evaluate all the impacted volume and prioritize promoting according to your considerations.

ⓘ **NOTE:** The metro status of the volume should be `Fractured`.

2. Click the status of the metro volume to display the Metro Volume page and click **Promote**.
   The **Promote Metro Volume** slide-out panel is displayed.

   ⓘ **NOTE:** Before the promotion takes place, a snapshot of the metro volume is taken.
3. Verify that you understand the implication of promoting the metro volume in case the remote system is servicing I/Os and verify that the remote system is down if possible.
4. Select the confirmation checkbox at the bottom of the **Promote Metro Volume** slide-out panel, and select **Promote**.
   The promoted state of the volume is indicated in the Metro Volume Details section of the **Metro Volume** page.

Demote a metro volume

About this task

When the preferred system runs out of storage space, the synchronization between the systems is stopped and the metro volume becomes fractured. Both systems stop servicing I/Os. In that case, the metro volume on the nonpreferred system must be promoted to enable host and production access to it until the preferred system resolves the problem. To enable this state, the metro volume on the preferred system must be demoted first.

Steps

1. Select **Protection** > **Metro**.

   ⓘ **NOTE:** The Metro page lists all the metro resources, and enables you to evaluate all the impacted volume and prioritize promoting according to your considerations.
2. Click the status of a metro volume to display the Metro Volume page and click **Demote**.
   The **Demote Metro Volume** slide-out panel is displayed.
3. Verify that you understand the implication of demoting the metro volume in case the remote system is servicing I/Os and verify that the remote system is down if possible.
4. Click **Demote**.
   The demoted state of the volume is indicated in the Metro Volume Details section of the Metro Volume page.

End a metro volume

About this task

When you end a metro volume, the metro configuration is removed, resulting in two independent volumes. If the remote volume is not deleted, the system removes the protection policy that is assigned to it, unmaps the hosts and assigns it with a new, different SCSI WWN. You can end a metro volume either from the preferred or the nonpreferred system.

Steps

1. Select **Storage** > **Volume** and select the checkbox of a volume.
2. Select **Protect** > **End Metro Volume**.
   The **End Metro Volume** slide-out panel is displayed.
3. Select one of the following options from the slide-out panel:
   - End metro and keep the volume on both the local and remote system.

     ⓘ **NOTE:** The remote system unmaps the hosts and assigns a different SCSI WWN to the volume.
   - End metro and delete the volume and any associated snapshots on the remote system.
4. Click **End**.

Using protection policies with metro

When an existing metro volume is assigned with a protection policy, or a volume with a protection policy is configured for metro, the same protection is applied to the metro volume on both systems. The protection policy that is created on the remote system is read-only. Changes to the protection policy and snapshot rules can only be made to the policy created by the user (regardless of the storage system it was created on). The read-only policy is synchronized with the changes every 15 minutes.

User-initiated snapshots that are created on one storage system are also generated on the other system.

NOTE: Asynchronous replication is not supported with metro volumes. A protection policy that contains a replication rule cannot be assigned to a metro volume.

Assigning a protection policy can be done on either the local or remote system (either preferred or nonpreferred).

Unassigning the protection policy should be done on the storage system where it was assigned. After the protection policy is unassigned from the volume in the local system, it is unassigned from the volume on the other system as well. Once the read-only protection policy is no longer being used by any metro volumes, it is automatically deleted from the system.

NOTE: When the policy cannot be unassigned from the storage system where it was assigned, due to a metro volume failure, the following is allowed:

- A read-only policy can be unassigned or swapped for a read/write policy from a preferred metro volume when it is fractured.
- A read-only policy can be unassigned or swapped for a read/write policy from a promoted nonpreferred metro volume.

NOTE: When the metro volume is fractured or a metro session is paused, snapshots are generated only on the active system. When the metro volume is self-healed or the session is resumed, the snapshots are not copied to the remote system and remain on the local system until they expire or are deleted.

7

Remote Backup

This chapter contains the following information:

Topics:

Terminology

Table 2. Remote backup terminology

TERM	DESCRIPTION
PowerProtect DD	A new generation Data Domain appliance designed primarily for data backup.
PowerProtect Data Manager	A centralized management application for managing one or more physical or in-cloud PowerProtect DD.
DD Storage Unit	A logical unit on PowerProtect DD that is exposed to backup applications using DD Boost protocol.
PowerProtect DD Remote System	A storage unit on the PowerProtect DD system.
Remote Session	A remote snapshot session that reflects the state and progress of an operation on a PowerProtect DD remote system. The session type can be Backup, Retrieve, or Instant Access.
Remote Snapshot	A representation of the data that is backed up on the PowerProtect DD and can be retrieved or browsed using instant access.

Pre-requirements and limitations

When using remote backup, consider the following limitations:

- Only one remote backup session can be created per resource (volume or volume group).
- Only one retrieve or instant access session can be created per remote snapshot.
- Up to two instant access sessions can be created per node.
- Remote backup and retrieve sessions and instant access sessions are mutually exclusive - when an instant access session is active, remote backup and retrieve sessions cannot run, and when remote backup and retrieve sessions are active, instant access sessions cannot run.
- When NDU or network reconfiguration is in progress, remote backup, retrieve, and instant access sessions cannot run.
- An instant access session can be created for a volume group that consists of up to four volumes.

- For optimal system performance, it is recommended that up to 125 volumes be backed up to PowerProtect DD per appliance.
- For optimal system performance, it is recommended that up to 125 remote backup sessions be created per appliance.
- Support for DDVE in-cloud is only available with AWS cloud provider.
- Deduplication is disabled on the client side, but is enabled on the PowerProtect appliance side.
- HA is not supported for instant access. Instant access fails if the cluster reboots or fails over. For details, see Dell Knowledge Base Article 000208509 (Instant Access sessions show failed state after node reboot).

Documentation resources

See the following resources for additional information:

Table 3. Documentation resources

Document	Description	Location
PowerProtect Data Manager Administration and User Guide	This document provides configuration information for PowerProtect Data Manager.	https://www.dell.com/support/home/en-us/product-support/product/enterprise-copy-data-management/docs
Dell PowerProtect Data Manager: Data Protection for Dell PowerStore Storage Arrays	This document focuses on backup and recovery of block volume data on PowerStore storage arrays using PowerProtect Data Manager.	https://infohub.delltechnologies.com/t/dell-powerprotect-data-manager-data-protection-for-dell-powerstore-storage-arrays/
PowerStore Online Help	The Online Help provides context-sensitive information for the page that is opened in PowerStore Manager.	Embedded in PowerStore Manager

Remote backup basic workflow

Backing up resources to a PowerProtect DD is the basic action that you can perform. When backups are created on a PowerProtect DD, you can browse and retrieve them. Every remote backup action is linked to a remote backup session that enables you to track its progress.

About this task

Perform the following steps to create a remote backup session:

Steps

1. Add a remote system connection for remote backup.
2. Create a remote backup rule.
3. Create a protection policy—Only one remote backup rule can be added to a protection policy.
4. Assign a protection policy—Assign a policy that includes a remote backup rule to a volume or volume group.
   A remote backup session is created and displayed in the **Backup Sessions** tab of the **Remote Backup** page.

Session states

Remote backup, retrieve, and instant access sessions, go through various states that indicate the sessions progress and possible issues.

The session possible states are:

- **Initializing**—The session is being created. After creation is completed, the status changes to Idle.
- **Idle**—No data is transferred to the remote appliance. The session remains in Idle state until the scheduled remote backup rule is triggered, or if you initiate a manual backup.
- **Prepare**—The PowerStore system is preparing to perform a backup. If there are multiple active sessions, the session may remain in Prepare state until it reaches the top of the queue.
- **IO Forwarding** (applies only to instant access sessions)—The session is forwarding the host I/O.

- **In Progress**—The system creates the backup on the remote system. During this state, you can click the status link to monitor the backup progress and view more details.
- **Completed** (applies only to retrieve sessions)—The session is successfully completed.
- **System Paused**—The session is paused by a nondisruptive upgrade or migration.
- **Paused**—The session is paused.
- **Cancelling**—The session is being cancelled.
- **Cancelled**—The session was explicitly cancelled. Sessions in Prepare, In Progress, and Paused states can be cancelled.
- **Deleting**—The session is being deleted.
- **Failed**—The session has failed to create the backup.
- **Rollback in Progress**—An error occurred while the session was active and changes are reverted.
- **Failed Cleanup Required**—An error occurred while changes were reverted (as a result of a previous error). The cleanup service, which runs periodically, automatically resolves the problem and the session state is changed to Failed. For remote backup sessions, scheduled backups cannot run while the session is in this state.
- **Cancel Cleanup Required**—An error occurred during the session cancel operation. The cleanup service, which runs periodically, automatically resolves the problem and the session state is changed to Cancelled. For remote backup sessions, scheduled backups cannot run while the session is in this state.
- **Cleanup Required**—The session is successfully completed, but an error occurred during the local cleanup phase. The cleanup service, which runs periodically, automatically resolves the problem and the session state is changed to Idle or Completed. For remote backup sessions, scheduled backups cannot run while the session is in this state.
- **Cleanup In Progress**—A cleanup is in progress.

Managing remote backup sessions

When you assign a protection policy that includes a remote backup rule to a volume or a volume group, a remote backup session is created and displayed in the **Backup Sessions** tab of the **Remote backup** page.

From the **Backup Sessions** tab, you can perform the following actions on a remote backup session:

- **Backup**—You can perform on-demand manual backup when the session is Idle. For example, if the resource was not backed up for a long period.

  NOTE: A manually created backup is subjected to the retention policy set in the remote backup rule.
- **Pause**—Pausing a session in an Idle state causes the session to be paused immediately. If you pause a session is when it is In Progress, the session is paused only after the current running backup is completed. Subsequent backups are not performed while the session is paused.
- **Resume**—Use this option to resume a paused backup session. The next backup occurs according to the set schedule.
- **Delete**—You can use this option only to delete a session for a resource that is protected by an external policy. For resources protected by PowerStore policy, you can delete the associated remote backup session by unassigning the policy from the resource, or removing the remote backup rule from the assigned policy.
- **Cancel**—You can use this option to cancel a backup session only when it is In Progress. Cancelling a session causes the current backup to be cancelled and copied data to be discarded.

  NOTE: When the session is in Prepare state, other sessions may be queued before it. When you click **Cancel**, the session state changes to **Canceling**, but the session is cancelled only when it reaches the top of the queue and becomes active (In Progress state).

Resources

The Resources tab displays all the volumes and volume groups which have associated remote snapshots.

A resource is added to the **Resources** table after a remote backup session that was created for the resource triggers the creation of a remote snapshot.

If a volume or a volume group that has associated remote snapshots is deleted from PowerStore, the remote snapshots are not impacted. The deleted resource remains listed on the Resources table until all its associated remote snapshots are expired. To see whether a resource is deleted, add the **Source Deleted** column to the Resources table, using the **Show/Hide Table Columns** option.

From the **Resources** tab, you can perform the following actions:

- Manage Snapshots—Selecting a resource from the list and clicking **Manage Snapshots**, displays all the remote snapshots that are created for this resource:

- The expiration time of both automatic and manually created snapshots is based on the retention time that was configured in the remote backup rule.
    - The expiration time of a remote snapshot cannot be changed. Changing the retention period in a remote backup rule does not affect existing snapshots.
    - For automatically generated snapshots, a remote snapshot name includes the name of the remote backup rule that created it.
    - Selecting a snapshot from the list and clicking **Retrieve** creates a retrieve session for this snapshot. See Retrieve a remote snapshot to the same PowerStore cluster for details.
    - Selecting one or more snapshots and clicking **Delete** deletes the snapshots.

  ⓘ **NOTE:** You can also see the remote snapshots for a resource and perform related actions by clicking the resource and then selecting the **Remote Snapshots** tab.
- Instant Access—Selecting a resource from the list and clicking **Instant Access** initiates the process for enabling instant access for the selected remote snapshot. For details, see Create an instant access session.
- Discover Remote Snapshots—Use this option when you want to retrieve a remote snapshot of a resource on a different PowerStore cluster. For details, see Retrieve a remote snapshot to a different cluster.

Retrieve sessions

Snapshots of volumes and volume groups that are backed up on a PowerProtect DD can be retrieved to the same or to other PowerStore clusters.

You may want to retrieve a remote snapshot for restoring the source resource or creating a thin clone.

Retrieve a remote snapshot to the same PowerStore cluster:

- If the source volume or volume group of the retrieved backup still exists in the system, a local snapshot is created on the PowerStore cluster. If possible, the retrieval is incremental.
- If the source volume or volume group of the retrieved backup no longer exists in the system, both a new volume and a local snapshot are created, and the new volume is restored with the snapshot data.

Retrieve a remote snapshot to a different PowerStore cluster:

- Since the source volume never existed on that cluster, both a new volume and a local snapshot are created. The new volume is restored with the snapshot data.

For each retrieve operation, a retrieve session is created. The initial status of the session is Prepare. Once the session starts copying the snapshot, the status changes to In-Progress and after the snapshot is copied, the state changes to Completed.

You can view and monitor the retrieve sessions progress in the **Retrieve Sessions** tab (**Protection** > **Remote Backup**). You can also perform the following actions:

- Delete—Use this option to delete a retrieve session in a **Completed** status.
- Cancel—Use this option to cancel a retrieve session in **In Progress** status.

  ⓘ **NOTE:** When the session status is **In Progress**, other sessions may be queued before it. When you click **Cancel**, the session state changes to **Canceling**, but the session is cancelled only when it reaches the top of the queue and becomes active.

After a backup is retrieved, it functions as any local snapshot. You can use a retrieved backup to restore a primary volume or to create a clone. The retrieved snapshot is set to No Automatic Deletion. You can change that setting by configuring a retention period. You can also modify it to a secure snapshot.

Retrieve a remote snapshot to the same PowerStore cluster

About this task

You may want to retrieve a remote snapshot to the same PowerStore cluster on which the source resource resides, when you must restore the parent resource or create a thin clone. You can retrieve a remote snapshot of a resource whether it still exists or is deleted.

Steps

1. Click **Protection** > **Remote Backup** and select the **Resources** tab.

   The **Resources** tab displays all resources (volumes and volume groups) that have associated remote snapshots.

2. In the Resources list, click the checkbox next to the resource and select **Manage Snapshots** to view all the backups created for that resource.
3. In the **Manage Snapshots** panel, select the snapshot that you want to retrieve and click **Retrieve**.
4. In the confirmation message, click **Retrieve**.
   A Retrieve session is created for the snapshot and added to the Retrieve Sessions table. If the source resource exists on the cluster, a local snapshot is created under the source resource, and the retrieved backup is copied to it. The retrieval can be of a full copy or include only of the differences between the backup and the resource (incremental copy), depending on the last backup. If the source resource no longer exists on the cluster, a new volume or volume group is created on the PowerStore cluster, as well as a local snapshot to which the remote snapshot is copied.

   You can monitor the progress of the retrieve session in **Protection** > **Remote Backup** > **Retrieve Sessions**.

Retrieve a remote snapshot to a different cluster

About this task

When you retrieve a remote snapshot to a PowerStore cluster other than the cluster that has the source resource, a new volume or volume group is created on the PowerStore cluster, as well as a local snapshot to which the remote snapshot is copied.

Steps

1. Click **Protection** > **Remote Backup** and select the **Resources** tab.
2. Click **Discover Remote Snapshots**.
3. In the **Discover Remote Snapshots** panel, set the following:
   - PowerProtect DD Remote System—Select the PowerProtect DD from which you want to retrieve the backup.
   - PowerStore Global ID—Specify the global unique identifier for the PowerStore cluster from which the backup was initiated. You can see the global ID of the cluster under **Settings** > **Cluster** > **Properties**.
   - From—Specify the starting date and time to search for remote snapshots.
   - To—Specify the ending date and time to search for remote snapshots.
4. Click **Next**.
5. From the list of discovered snapshot, select the snapshot that you want to retrieve, and click **Next**.

   NOTE: You can only select snapshots that were created by a PowerStore cluster.
6. Review the information summary and click **Retrieve**.

Results

PowerStore creates a retrieve session that can be viewed on the **Retrieve sessions** tab. When the session is complete, the retrieved snapshot and a new volume are created on the local cluster.

Retrieve - additional considerations

- When the original source of a backup snapshot that is retrieved from the DD no longer exists (orphan snapshot), blocks on the newly created volume that were not written to when the original volume was backed up, are allocated and written with zeros. As a result, the physical and logical capacities are the same (when looking at the retrieved backup capacity data). When the new volume is mapped to a host, the used and free space are displayed correctly. For details, see Dell Knowledge Base Article 000208504 (After retrieving PowerStore from Data Domain...).
- When a source volume or volume group no longer exists on the PowerStore cluster, retrieving the respective backup always results in the creation of a new source together with the retrieved snapshot.
- If the size of the retrieved snapshot does not match the size of the source volume, the retrieval is full (the entire snapshot is copied from PowerProtect to PowerStore.
- Incremental retrieval (retrieving only the changes that occurred since the backup), occurs if the following conditions are fulfilled:
  - The size of the source volume has not changed since it was backed up.
  - Both the source volume and the latest remote backup exist on the PowerStore cluster.
- The average transfer rate for an incremental retrieval may not always be accurate, although the retrieval progress percentage accurately reflects the amount of retrieved data.

Instant access sessions

Instant access allows you to access remote snapshots on a PowerProtect DD without having to retrieve them to the PowerStore cluster.

- Use the instant access option to browse a remote snapshot before deciding whether to retrieve it, or to access a snapshot of a deleted, corrupted, or modified resource and copy it to the host.
- Only one instant access session is allowed per remote snapshot.
- An instant access session can be created for volume groups that include up to four members.
- When an instant access session is running, the PowerStore cluster does not perform backup and retrieve operations, and local resources are not protected.
- Instant access fails when a cluster reboots or fails over. To reinitiate instant access in this case, unmap the instant access volume from the host, delete the session, and then re-create the session.
- The system sets node affinity to instant access sessions at creation. If the host cannot access the node that the instant access session has affinity to, the instant access session does not failover to the other node, and the host will have problems accessing the instant access resource data.

The following information is provided on the **Instant Access Sessions** tab:

- Status—The session status is I/O Forwarding.
- Local Resource—Displays the new volume or volume group that is created as part of the session. Clicking the local resource hyperlink opens the Details page for this resource, where you can view the volume details or volume group members. You can also view performance data, check issued alerts, and map or unmap hosts to the resource.

From the Instant Access Sessions tab, you can end an instant access session. To end the session, you must first remove all host mappings to the local resource.

The volumes and volume groups that are created as part of instant access sessions are also displayed under **Storage** > **Volumes** > **Instant Access** and **Storage** > **Volume Groups** > **Instant Access**.

Create an instant access session

Instant access allows you to gain access to remote snapshots on the PowerProtect DD without having to retrieve them to the PowerStore cluster.

Steps

1. Select **Protection** > **Remote Backup** > **Resources**.
2. From the resources list, check the checkbox next to the resource and click **Instant Access**.

   The **Enable Instant Access** panel displays all available remote snapshots for the selected resource.
3. Select the snapshot that you want to access.

   NOTE: You can also select the resource and then, select **Remote Snapshots** > **remote snapshot** > **Enable Instant Acess**.
4. Optionally, you can map hosts to the volume that is created when the instant access session initiates. Click **Map Hosts**, select the hosts that you want to map, and click **Apply**.
   The mapped hosts are listed in the Host Connectivity section.

   NOTE: This option exists only for volumes and not for volume groups. Mapping hosts to members of a volume group is possible only after you create the instant access session (see details below).
5. Click **Enable**.
   An instant access session is created and added to the **Instant Access Sessions** tab. A local associated volume or volume group is created for the session and can be viewed on the **Instant Access** tab on the **Volumes** or **Volume Groups** window.

   NOTE: The **Instant Access** tab is displayed only when PowerProtect DD is added as a remote system.

   The created resource is Read/Write. Data is written temporarily on the PowerProtect DD appliance while the remote snapshot remains unchanged. When the session is deleted, all writes are lost.

Results

after you create an instant access for a volume group, you can map hosts to members of the volume group that was created for the session:

1. Select **Protection** > **Remote Backup** > **Instant Access Sessions**.
2. Click the volume group link in the **Local Resource** column to view its members.
3. Select the members you want to map and click **Map** to open the **Map Hosts** panel.

Instant access - additional considerations

- Instant access is supported for all block resources except VMware vStorage VMFS datastores. If you must access data within a remote snapshot, retrieve the remote snapshot, and then create and mount a thin clone.
- HA is not supported for instant access - See High availability and Dell Knowledge Base article 000208509 (Instant Access sessions show failed state after node reboot).
- Instant Access is not supported for DDVE in-cloud.

High availability

High availability is supported (but not guaranteed) for remote backup sessions and retrieve sessions but not for instant access sessions:

- When a node is down or a node reboots -
  - Backup and retrieve sessions failover to the peer node and continue on it.
  - Instant access sessions are node-specific. When the node on which the session is running is unreachable or down, the session moves to failed state. Unmap the volume from the host and delete the session, and then create the session again.
- When an appliance powers off or reboots -
  - All backup and retrieve sessions resume when the appliance is up again.
  - Instant access sessions move to failed state. Unmap the volume from the host and delete the session, and then create the session again.

Remote backup alerts

The **Alerts** tab (located under **Monitoring**) displays general alerts that are generated for remote backup sessions, such as session creation and completion, adding or removing a remote system, and so on. You can filter remote backup alerts by selecting **Remote Session** and **Remote System** as Resource Type.

Alerts are also issued when failures occur. The number of alerts is displayed in the **Backup Sessions** and **Retrieve Sessions** tabs. Clicking the number opens the **Alerts** tab.

A

Use cases

This chapter contains the following information:

Topics:

Snapshot and thin clone use cases

You can use snapshots and thin clones to restore corrupted volumes and create test environments.

Snapshots are read-only copies that can be used to save the current state of an object. You can use snapshots to quickly recover data if there is corruption or user error. Snapshots cannot be directly accessed by a host.

Thin clones are writable copies of a snapshot, volume, or volume group that can be accessed by a host. Thin clones can be created directly as a copy of the parent object or using one of its snapshots. Both snapshots and thin clones are space efficient copies that share data blocks with their parent object.

Using snapshots and thin clones for partial recovery of a volume

You can use snapshots and thin clones to recover part of a volume, such as individual files or database records, from a previous point in time. First, create a thin clone using the snapshot that contains the data you need to recover. Then, provide host access to the clone, and recover data from the host.

Using snapshots to restore a volume or volume group

You can use snapshots to roll back a volume to a previous point of time, if there is corruption. To revert a volume or volume group to a previous point in time, use the volume restore operation and supply a snapshot from before the corruption occurred. The restore operation is instantaneous. You can also create a backup snapshot to save the state of the volume or volume group before you use the restore operation.

Using thin clones to test a patch before applying it to the production volume

Before installing a patch or software update of a critical application on a volume, you can take a thin clone of the volume, then apply the update to the thin clone. After you have installed the update and verified that the update is safe for your environment, you can install the update on the other volumes.

Create thin clones for development use

Instead of provisioning volumes or volume groups for each individual developer, you can create thin clones. Creating thin clones of the volume or volume group enables you to distribute the same data and configuration to each developer. The thin clones also take up less space than if you had created a full clone of the volume, or provisioned individual volumes or volume groups. You can also take snapshots of thin clones and replicate them.

Replication use cases

You can use replication for planned downtime, such as during inter-cluster migration, the installation of a major software update, and disaster recovery.

Intercluster migration

If you need to migrate a storage object to another PowerStore cluster, you can set up a one-time replication between the two clusters, followed by a planned fail over to the new cluster to complete the migration. After the migration, dismantle the source object to reclaim space on the original cluster.

Using replication for planned downtime

Planned downtime is a situation where you take the source system offline for maintenance or testing, while operating off the destination system. Before the planned downtime, both the source and destination are running with an active replication session. There is no data loss in planned downtime.

In this scenario, the source system, Boston, is taken offline for maintenance, and the destination system, New York, is used as the production system during the maintenance period. After maintenance is over, return production to the Boston system.

To start planned downtime, select **Planned Failover** on the Boston source system. The New York destination system is fully synchronized with the source to ensure that there is no data loss. The session remains paused, while the Boston source system becomes read-only and the destination becomes read/write. The New York destination storage resource can provide access to the host. On the New York destination storage resource, select **Reprotect** to resume replication in the reverse direction.

To resume operations on the Boston system after maintenance, select **Planned Failover** on the New York system. After the failover is complete, **Reprotect** on the Boston system.

ⓘ **NOTE:** To replicate data from the destination to the source with the reprotect operation, ensure that there is a replication policy on the destination system that has a replication rule pointing to the source system. For example, if the regular replication session is from a site in Boston to a site in New York, the replication policy on the destination storage resource in New York must point to Boston.

Using replication for disaster recovery

In this disaster recovery scenario, the source system, Boston, is unavailable due to a natural or human-caused disaster. A destination system, New York, was created, which contains a full copy, or replica, of the production data. Data access can be restored by failing over to New York because a replication session was configured between the Boston and New York systems.

Using replicas for disaster recovery minimizes potential data loss. The replica is up-to-date with the last time that the destination synchronized with the source, as specified in the associated replication rule. The amount of potential data loss is based on the recovery point objective (RPO) setting in the associated replication rule. The replication session can be failed over to the New York destination system, using the latest data that was replicated from Boston.

After the session is failed over to the New York system, it becomes read/write. When originally establishing a replication session between the source and destination systems, the storage resource was given the correct access permissions to the host and share. Creating the correct host access on the destination system ahead of time reduces downtime in an event of a disaster.

To resume operations on the Boston system, when it is available:

1. From the New York system, select the **Reprotect** option, which resumes the replication session in the reverse direction.
2. After the systems are synchronized, select the **Planned Failover** option on the New York system.
3. Select the checkbox to auto-reprotect the system after failing over. Or, after the failover is complete, on the Boston system, select **Reprotect**.

ⓘ **NOTE:** To replicate data from the destination to the source with the reprotect operation, ensure that there is a replication policy on the destination system that has a replication rule pointing to the source system. For example, if the replication session is from a site in Boston to a site in New York, the replication policy on the target storage resource in New York must point to Boston.

Metro protection use cases

Use Metro protection to ensure data high availability, load balancing and migration.

Using metro for high availability

A Metro volume is exposed using two distinct storage arrays that cooperate to expose a single Metro volume to application hosts by providing the same SCSI image and data. The hosts and applications running on them perceive two physical volumes as a single volume with multiple paths. As a result, hosts can access both sides of the Metro volume. If there is a link loss or failure of one of the systems, host access can still be maintained to the active system.

Metro protection provides bi-directional synchronous replication, where both sides of the Metro volume can be used for production. Instead of disaster recovery (by failing over a replication session to a remote system), Metro enables disaster avoidance by providing automatic synchronization between the systems without downtime.

Using metro for load balancing

With PowerStore metro volume, the data centers can be optimized to fully use PowerStore systems through an active/active environment that enables workload balancing across PowerStore systems. Moving applications non-disruptively between PowerStore systems is simple and easy and can be done when capacity or performance balancing is required.

Using metro for migration

You can use metro volumes when there is a need to migrate workloads between PowerStore systems. Using metro volumes for migration is simple and easy to use, and it reduces the risk for data loss. With the metro volume option, the migration is non-disruptive and, when migration is complete, the metro volume can be either removed or kept for allowing an extremely fast recovery in the event of a system failure or even a full site failure.