Dell PowerStore

Configuring SMB

4.1

February 2025
Rev. A07

DELL Technologies

Notes, cautions, and warnings

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

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

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

Contents

Preface

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

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

Where to get help

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

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

1

Overview

This chapter contains the following information:

Topics:

SMB support

PowerStore T model and PowerStore Q model support SMB 1 through SMB 3.1.1. When SMB support is enabled on the NAS server, you can create SMB-enabled file systems. The NAS server with SMB support can either be stand-alone, or Active Directory domain-joined. Domain-joined NAS servers are placed in the OU=Computers, OU=EMC NAS Servers organizational unit by default.

NOTE: Client access using the SMB1 protocol is disabled by default, due to potential security vulnerabilities. If client access using SMB1 is required, you can enable it by modifying the `cifs.smb1.disabled` parameter. It is recommended to use SMB2 at a minimum for enhanced security and increased efficiency.

SMB file systems and shares have the following advanced protocol options:

NOTE: These options, except for Oplocks Enabled, are disabled by default.

Table 1. SMB advanced protocol options

Protocol option	Level
Sync Writes Enabled	File system
Oplocks Enabled	File system
Notify on Write Enabled	File system
Notify on Access Enabled	File system
Continuous Availability	Share
Protocol Encryption	Share
Access-Based Enumeration	Share
Branch Cache Enabled	Share
Offline Availability	Share

Planning considerations

Review the following information before configuring NAS servers and file systems:

File storage support is only available with PowerStore T model and PowerStore Q model appliances.

NAS server networks

Configure the following before configuring NAS servers with SMB protocol:

1. Configure one or more DNS servers.

2. If you are joining the NAS server to the Active Directory (AD), configure at least one NTP server on the storage system to synchronize the date and time. It is recommended that you set up a minimum of two NTP servers per domain to avoid a single point of failure.

   NOTE: During AD creation, NTP is configured.

3. Create a domain account in Active Directory.

Creating network VLANs and IP addresses is optional for NAS servers. If you plan to create a VLAN for NAS servers, the VLAN cannot be shared with the PowerStore T model and the PowerStore Q model management, or storage networks. Also, be sure to work with your network administrator to reserve the network resources and configure the network on the switch. See the *PowerStore T and Q Networking Guide for Storage Services* for details.

Scalability

In PowerStoreOS 3.5 and later, there is a shared limit for file systems volumes and vVols. The total number of objects is determined according to the highest limit of the three object types.

To view the limit for file systems per platform, see *Dell Technologies PowerStore Simple Support Matrix* on the PowerStore Documentation page.

Deployment requirements

NAS services are only available on PowerStore T model and PowerStore Q model appliances.

You must have chosen **Unified** during initial configuration of your PowerStore T model and PowerStore Q model appliances. If you chose **Block Optimized** while running the Initial Configuration Wizard, NAS services were not installed. To install NAS services, a technical support representative must reinitialize your system. Reinitializing the system:

- Sets the appliance back to the factory state.
- Removes all configuration that was done on the system through the **Initial Configuration Wizard**.
- Removes any configuration that is performed in PowerStore after initial configuration.

More considerations

Both nodes on the appliance must be up and running to create a NAS server. If one of the nodes is down on the appliance, NAS server creation will fail.

Create the network interface for NAS traffic

You can configure a NAS network using Link Aggregation Control Protocol (LACP) bonds or by creating a Fail-Safe Network for NAS traffic.

Create LACP bonds for NAS traffic

If your switches are configured with MC-LAG, you can use network bonding by creating a Link Aggregate Group (LAG) for NAS traffic.

About this task

When the Top-of-Rack (ToR) switches are configured with an MC-LAG interconnect, it is recommended to configure the NAS interface over LACP bonds using Link Aggregation Groups (LAG). LACP bonding is a process in which two or more network interfaces are combined to a single interface. Using LACP bonding provides performance improvements and redundancy by increasing the network throughput and bandwidth. If one of the combined interfaces is down, the other interfaces are used to maintain a stable connection.

Steps

1. Select **Hardware** > **[Appliance]** > **Ports**.

2. From the ports list, select two to four ports of the same speed on the node on which you want to aggregate for Link Aggregate Control Protocol (LACP) Bond to service NAS traffic.

   NOTE: The configuration is symmetrical across the peer node.

3. Select **Link Aggregation** > **Aggregate Links**.
4. Optionally, provide a description for the bond.
5. Select **Aggregate**.
6. Scroll through the ports list and locate the generated bond name.

   NOTE: You must select the bond name when you create the NAS server.

Create a Fail-Safe Network

About this task

A Fail-Safe Network (FSN) should be created when the Top-of-Rack (ToR) switches have not been configured with an MC-Lag interconnect. An FSN extends link failover into the network by providing switch level redundancy. An FSN can be configured on a port, a link aggregation, or any combination of the two.

Steps

1. Select **Hardware** > **[Appliance]** > **Ports**.
2. If you plan to use aggregated links for the FSN, first create the Link Aggregation Groups. For details, see Create LACP bonds for NAS traffic.
3. From the list, select two ports or two link aggregations, or a combination of a port and a link aggregation group that you want to use for the FSN on node A and select **FSN** > **Create FSN**.
4. In the **Create FSN** panel, select which ports or link aggregation to use as the primary (active) network.

   NOTE: The primary port cannot be modified once it is used to create a NAS server.

5. Optionally, add a description of the Fail-Safe Network.
6. Click **Create**.

   PowerStore Manager automatically creates a name for the Fail-Safe Network using the format: "BaseEnclosure-<Node>-fsn<nextLACPbondcreated>"

   - BaseEnclosure is constant.
   - Node is the node that is displayed in the **Node-Module-Name** list.
   - nextLACPbondcreated is a numeral value that is determined by the order in which the bond was created in PowerStore Manager, starting with zero for the first created bond.

   The first FSN created in PowerStore Manager on node A would be named BaseEnclosure-NodeA-FSN0.

   The same FSN is configured on the opposite node. For example, if you configured the FSN on node A, the same FSN would be configured on node B.

7. Create a NAS server with the Fail-Safe Network.

   The Fail-Safe Network is applied to the NAS server while creating the NAS server in PowerStore Manager. See Create NAS server for SMB file systems.

Creating SMB shares

Complete the following before you can create SMB shares in PowerStore:

1. Create NAS servers with SMB protocol
2. Create a file system for SMB shares

Documentation resources

See the following for additional information:

Table 2. Documentation resources

Document	Description	Location
PowerStore T and Q Networking Guide for Storage Services	Provides network planning and configuration information.	dell.com/powerstoredocs
PowerStore Configuring NFS Guide	Provides information necessary to configure NFS Exports with PowerStore Manager.	
PowerStore File Capabilities White Paper	Discusses the features, functionality, and protocols supported by Dell PowerStore file architecture.	
PowerStore Online Help	Provides context-sensitive information for the page opened in PowerStore Manager.	Embedded in PowerStore Manager

2

Create NAS servers

This chapter contains the following information:

Topics:

Overview of configuring NAS servers

Before you can provision file storage on the PowerStore cluster, a NAS server must be running on the system. A NAS server is a file server that supports the SMB protocol, NFS protocol, or both to share data with host clients. It also catalogs, organizes, and optimizes read and write operations to the associated file systems.

This document describes how to configure a NAS server with SMB protocol, on which file systems with SMB shares can be created.

Create NAS server for SMB file systems

You create a NAS server before creating file systems.

Prerequisites

Obtain the following information:

- Network port, IP Address, Subnet Mask/Prefix Length, Gateway information for the NAS Server.

  NOTE: IP Address and Subnet Mask/Prefix Length are mandatory.

- VLAN identifier, if the switch port supports VLAN tagging.

  NOTE: You cannot reuse VLANs that are being used for the management and storage networks.

- If you are configuring a stand-alone NAS server, obtain the workgroup and NetBIOS name. Then define what to use for the stand-alone local administrator of the SMB server account.
- If you are joining the NAS server to the Active Directory (AD), ensure that NTP is configured on your storage system. Then obtain the SMB system name (used to access SMB shares), Windows domain name, and the username and password of a domain administrator or domain user who has a sufficient domain access level to join the AD.

Steps

1. Select **Storage** > **NAS Servers**.
2. Select **Create**.
3. Continue to work through the **Create NAS Server** wizard.

Wizard Screen	Description
Details	• NAS server Name • NAS server description • Network interface - Select a Link Aggregation Group or Fail-Safe Network (see Create the network interface for NAS traffic).

Wizard Screen	Description
	NOTE: If you select a Fail-Safe Network (FSN), the primary network cannot be modified once a NAS server has been configured using the FSN. • Network information
Sharing Protocol	**Select Sharing Protocol** Select **SMB**. **NOTE:** If you select both SMB and NFS protocols, you automatically enable the NAS server to support multiprotocol. Multiprotocol configuration is not described in this document. **Windows Server Settings** Select **Standalone** to create a stand-alone SMB server or **Join to the Active Directory Domain** to create a domain member SMB server. If you join the NAS server to the AD, optionally Select **Advanced** to change the default NetBios name and organizational unit. **DNS** If you selected to **Join to the Active Directory Domain**, it is mandatory to add a DNS server. Optionally, enable DNS if you want to use a DNS server for your stand-alone SMB server. **User Mapping** The **User Mapping** page displays if you have selected to join the active directory domain. Keep the default **Enable automatic mapping for unmapped Windows accounts/users**, to support joining the active directory domain. Automatic mapping is required when joining the active directory domain.
Protection Policy	Optionally, select a protection policy from the list.
File QoS Policy	Optionally, select a file QoS policy from the list.
Summary	Review the content and Select **Previous** to go back and make any corrections.

4. Select **Create NAS Server**.
   The **Status** window opens, and you are redirected to the **NAS Servers** page once the server is created.

Next steps

Once you have created the NAS server for SMB, you can continue to configure the server settings, or create file systems.

Select the NAS server to continue to configure, or modify the NAS server settings.

Change NAS server settings

Once you have created a NAS server, you can make configuration changes to the server.

About this task

NOTE: When there is a remote system connection, it may take up to 15 minutes for NAS server configuration changes to be reflected on the remote NAS server.

Steps

1. Select **Storage** > **NAS Servers** > **[nas server]**.
2. On the **Network** page, optionally configure the network interfaces or the routes to external networks as described in Configure NAS server networks.
3. On the **Naming Services** page, optionally add, modify, or delete NAS server DNS servers.

NOTE: You cannot disable DNS for NAS servers that support SMB file sharing and that are joined to an Active Directory (AD).

4. On the **Sharing Protocols** page:
   - Select the **SMB Server** card to enable or disable support for Windows shares, or to change the type of lookup the SMB server uses.

     NOTE: If you change the **Windows Server Type** from **Standalone** to **Join to the Active Directory Domain**, then you must go to the **User Mapping** tab and select **Enable automatic mapping for unmapped Windows accounts/users**.

   - Select the **FTP** card to enable or disable FTP or SFTP, change FTP or SFTP properties, configure user authentication, a user home directory, and authentication message settings. For details see Configure FTP sharing protocol.
   - Select **User Mapping** to enable the server to use automatic mapping for unmapped Windows account/users, or the default account for unmapped Windows account users.
5. On the **Protection** page, enable or disable NDMP.

   For details see Enable NDMP Protection and Events.
6. On the **Security & Events** tab:
   - Select **Kerberos** to add the active directory (AD) realm for Kerberos authentication or to configure a custom Kerberos realm.
   - Select **Antivirus** to enable or disable the anti-virus service and to retrieve or upload the anti-virus configuration file.

   For details see Configure NAS Server Security.

3

More NAS server features

This chapter contains the following information:

Topics:

Configure an FTP or SFTP sharing protocol

You can configure FTP or FTP over SSH (SFTP) after the NAS server has been created.

Prerequisites

Passive mode FTP is not supported.

About this task

FTP access can be authenticated using the same methods as SMB. Once authentication is complete, access is the same as SMB for security and permission purposes. If the format is `domain@user` or `domain\user`, SMB authentication is used. SMB authentication uses the Windows domain controller.

Steps

1. Select the **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **FTP** tab.
2. Under **FTP**, if Disabled in on, slide the button to **Enable**.
3. Optionally also enable SSH FTP. Under **SFTP**, if Disabled in on, slide the button to **Enable**.
4. Select which type of authenticated users have access to the files.
5. Optionally, show the **Home Directory and Audit** options.
   - Select or clear the **Home directory restrictions**. If disabled, enter the **Default home directory**.
   - Select or clear **Enable FTP/SFTP Auditing**. If checked, enter the directory location of where to save the audit files, and the maximum size allowed for the audit file.
6. Optionally, **Show Messages**, and enter a default welcome message, and message of the day.
7. Optionally, show the **Access Control List**, and add a list of users, groups, and hosts that are allowed, or denied FTP access.
8. Select **Apply**.

Configure NAS server networks

You can modify or configure NAS server networks.

Configure the following for NAS server networks:

- The file interfaces
- Routes to external services such as hosts.

Configure file interfaces for a NAS server

You can configure the file interfaces for a NAS server after the server has been added to PowerStore.

About this task

You can add more file interfaces, and define which is the preferred interface to use. Also, you can define which interface to use for production and backup, or for IPv4, or IPv6.

Steps

1. Select **Storage** > **NAS Servers** > **[nas server]**.
2. On the **Network** page, click **Add** to add another file interface to the NAS server.
3. Enter the File Interface properties.

   NOTE: Do not reuse VLANs that are being used for the management and storage networks.

4. You can perform the following on a File Interface by selecting a file interface from the list. Select:

Option	Description
Modify	To change the properties of the file interface properties.
Delete	To delete the file interface from the NAS server.
Ping	To test the connectivity from the NAS server to the external IP address.
Preferred Interface	To define which interface PowerStore should default to using when multiple production and backup interfaces have been defined.

Configure routes for the file interface for external connections

You can configure the routes that the file system uses for external connections.

Prerequisites

You can use the **Ping** option from the **File Interface** card to determine if the file interface has access to the external resource.

About this task

Usually, the NAS server interfaces are configured with a default gateway, which is used to route requests from the NAS server interface to external services.

Use the following steps:

- If you must configure more granular routes to external services.
- To add a route to access a server from a specific interface through a specific gateway.

Steps

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Network** > **Routes to External Services**.
2. Click **Add** to enter the route information in the **Add Route** wizard.

Enable NDMP backup

You can configure standard backup for the NAS servers using NDMP. The Network Data Management Protocol (NDMP) provides a standard for backing up file servers on a network. When NDMP is enabled, a third-party Data Management Application (DMA), such as Dell Networker, can detect the PowerStore NDMP using the NAS server IP address.

About this task

Enabling NDMP is performed after the NAS server is created.

PowerStore supports:

- Three-way NDMP - The data is transferred through the DMA over a local area network (LAN) or Wide Area Network (WAN).
- Full and incremental backups

Steps

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Protection** .
2. Under **NDMP Backup**, if **Disabled** is on, slide the button to change to **Enabled**.
3. Enter a password for the **New Password**.
   The username is always `ndmp`.
4. Reenter the same password as the new password in **Verify Password**.
5. Click **Apply**.

Next steps

Leave the NDMP page, and return back to the NDMP page to validate that NDMP is enabled.

Configure NAS server security

You can configure the NAS server with **Kerberos** or **anti-virus** security.

Configuring NAS server security includes the following options:

- Kerberos
- Antivirus

Configure Kerberos security for the NAS server

You can configure the NAS server with Kerberos security.

About this task

Be sure to add the SMB server to the AD domain before configuring Kerberos.

If you are configuring the NAS server for SMB-only, you do not need a Keytab file. The Keytab file is only required for Secure NFS configuration.

Steps

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Security** > **Kerberos**.
2. If Disabled is on, slide the button to change to **Enabled**.
3. Enter the name of the **Realm**.
4. Enter the Kerberos IP Address and click **Add**.
5. Enter the TCP Port to use for Kerberos. 88 is the default port.
6. Click **Apply**.

Understanding Common Anti-Virus Agent (CAVA)

Common AntiVirus Agent (CAVA) provides an antivirus solution to clients using a NAS server. It uses an industry-standard SMB protocol in a Microsoft Windows Server environment. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the storage system.

Antivirus software is important because the storage system is resistant to the invasion of viruses because of its architecture. The NAS server runs data access in real-time using an embedded operating system. Third parties are unable to run programs containing viruses on this operating system. Although the operating system software is resistant to viruses, Windows clients that access the storage system require virus protection. Virus protection on clients reduces the chance that they will store an infected file on the server, and protects them if they open an infected file. This antivirus solution consists of a combination of the operating system software, CAVA agent, and a third-party antivirus engine. The CAVA software and a third-party antivirus engine must be installed on a Windows Server in the domain.

For the CEE CAVA versions required by PowerStore see the *Common Event Enabler Release Notes* on the Dell Technologies Support site. For additional information about CAVA, which is part of Common Event Enabler (CEE), see *Using the Common Event Enabler on Windows Platforms* on the Dell Technologies Support site.

Enable a common Anti-Virus Agent (CAVA)

You can enable and configure CAVA when you want to add anti-virus protection to your SMB shares.

Prerequisites

- A Windows server running with a compatible A/V product. For details, see the eLab CEE_CAVA Support Matrix.
- Install the EMC_CEE_Pack_8_x_x_x 32 or 64-bit CAVA application on the Windows A/V server.

  NOTE: After installing the application, go to the EMC CAVA service, Log On section, and assign a Domain administrative user account as the anti-virus user. Then restart the service.

- Create a user in Active Directory.
- Verify that the NAS server has SMB enabled.

About this task

As of PowerStore Manager 4.x, you can configure CAVA, assign virus checking privileges, view CAVA configuration and status, and perform on-demand file system scans using the PowerStore Manager.

NOTE: It is also possible to perform these actions using CLI and REST API.

Steps

1. From PowerStore Manager go to the **Storage** > **NAS Servers** > **[nas server]** > **Security & Events** > **Antivirus** tab.
2. Select **Configure** to open the **Configure Antivirus Settings** dialog.
3. Set the following parameters: the IP address, file extensions you want to be scanned, and file extensions you want to be excluded.
   - IP address - Set the Windows A/V server IP address or FQDN.
   - File extensions to be scanned - Use the following format: *.txt, *.docx, *.exe.
   - File extensions to be excluded - Use the same format as for scanned file types.
4. Select **Advanced Options** to set the following parameters:
   - Maximum File Size
   - Survey Time
   - Shutdown Action
   - High Watermark
   - Low Watermark
   - MSRPC User
   - HTTP Port
   - RPC Retry Timeout
   - RPC Request Timeout
5. Select **Create**.
   The anti-virus service is marked as active.

6. Select the Edit icon to open the **Properties** dialog.
7. Select **Enable** to enable anti-virus scanning and then select **Apply**.
8. To provide the NAS server with the EMC Virus Checking rights, select the **Account Privileges** tab and add the Domain anti-virus user account. Use the Domain\username format (for example, Lab\anti-virus).

   NOTE: This account is the same user account that is selected in the EMC CAVA service on the Windows server.

9. To view details of the anti-virus software and online status, select the **Audit Info** tab.
10. From the **File Systems to be Scanned** tab, select the file systems that you want to scan and then select **Start** to start the scan.
11. If you want the scan to include offline files, select the option in the displayed message and select **Start Scan**.
12. To monitor the scan progress, select the **Status** tab.
13. When the scan is completed, a message indicating the status is displayed.
14. To stop a scan for a file system, select the file system and then select **Stop Scan** and then confirm in the displayed message.
15. If you want to configure CAVA using a configuration file (viruschecker.conf), you can download and modify the current file or upload a new configuration file by selecting **Upload/Retrieve Configuration** from the **Properties** dialog.

    NOTE: For details on the parameters in the viruschecker.conf file, see Configurable anti-virus parameters.

Configurable anti-virus parameters

The table below details the parameters that can be configured in the `viruschecker.conf` CAVA configuration file. You can create the configuration file and then upload it to PowerStore.

Table 3. Anti-virus parameters

Parameter	Description	Mandatory	Example
`addr=`	Sets the IP addresses of the CAVA server or servers.	Yes	`addr=10.205.20.130`
`masks=`	Configures the file extensions that are scanned.	Yes	`masks=*.exe:*.docx:*.com`
`excl=`	Lists file extensions that are excluded during the scan.	No	`excl=pagefile.sys`
`maxsize=<n>`	Integer. Sets the maximum file size for files that are checked. Files that exceed this size are not checked.	No	`maxsize=4294967290`
`surveyTime=<n>`	Sets the time interval (in seconds) used to scan all AV servers to see if they are online or offline. If no AV server answers, the shutdown process begins, using the configured shutdown parameter (see next row).	No	`surveyTime=600`
`shutdown=`	Specifies the shutdown action to take when no server is available. The default value is `Allow Access`.	No	`Allow Access`, `Stop_SMB_Access`, `Disable_Virus_Checker`
`highWaterMark=<n>`	Alerts the system when the number of requests in progress exceeds `highWaterMark`.	No	`highWaterMark=200`
`lowWaterMark=<n>`	Alerts the system when the number of requests in process is lower than `lowWaterMark`.	No	`lowWaterMark=50`
`msrcpuser=`	Specifies the name that is assigned to either a simple user account or a user	No	User account: `msrpcuser=user1`

Table 3. Anti-virus parameters (continued)

Parameter	Description	Mandatory	Example
	account that is part of a domain that the CAVA service is running under on the CEE machine.		Domain/user account: `msrpcuser=CEE1/user1`
`httpport=`	Specifies the HTTP port number on the CEE machine that the system uses.	No	`httpport=12228`
`RPCRetryTimeout`	Sets the timeout (in milliseconds) of the RPC retry.	No	`RPCRetryTimeout=4000 milliseconds`
`RPCRequestTimeout`	Sets the timeout (in milliseconds) of the RPC request. When an RPC is sent to the CAVA server, if the server answers after the RPCRetryTimeout, The NAS server retries until RPCRequestTimeout is reached and then moves to the next available CAVA server.	No	`RPCRequestTimeout=20000 milliseconds`
`reference time`	Enables a scan on the first read. If the last access time of a file is earlier than `reference time`, on access, the file is sent to the Virus Checker before the client is granted access.	No	`reference_time=2022-10-27T 18:30:00`

4

Create file systems and SMB shares

This chapter contains the following information:

Topics:

Create a file system

A file system must be created on the NAS server before you can create an SMB share.

Prerequisites

Ensure that there is a NAS server that is configured to support the SMB protocol as described in Configuring NAS servers.

Steps

1. Select **Storage** > **File Systems** and click **Create**.
2. Continue to work through the **Create File System** wizard.

Option	Description
Select Type	Select **General** file system type
Select NAS Server	Select a NAS server enabled for SMB.
Advanced SMB Settings	Optionally choose from the following: • **Sync Writes Enabled** • **Oplocks Enabled** • **Notify on Write Enabled** • **Notify on Access Enabled** • **Enable SMB Events Publishing** For details see File system advanced settings for SMB shares.
File System Details	Provide the file system name, and the size of the file system. The file system size can be from 3 GB to 256 TB. **NOTE:** All thin file systems, regardless of size, have 1.5 GB reserved for metadata upon creation. For example, after creating a 100GB thin file system, PowerStore T model and PowerStore Q model immediately show 1.5 GB used. When the file system is mounted to a host, it shows 98.5 GB of usable capacity. This is because the metadata space is reserved from the usable file system capacity.
File-Level Retention	Optionally, select file-retention type: • Enterprise (FLR-E) - Protects content from changes that users make through CIFS and FTP. An administrator can delete an FLR-E file system that contains protected files. • Compliance (FLR-C) - Protects content from changes that users and administrators make and complies with SEC rule 17a-4(f) requirements. FLR-C file system can be deleted only when it does not contain any protected files. **NOTE:** FLR state and file-retention type are set at file system creation and cannot be modified.

Option	Description
	Set the retention periods: ● Minimum - Specifies the shortest period for which files can be locked (default value is 1 day). ● Default - Used when a file is locked and no retention period is specified. ● Maximum - Specifies the longest period for which files can be locked.
SMB Share	Optionally, configure the initial SMB Share. You can add shares to the file system after the initial file system configuration. For details about the SMB Share options, see: Create an SMB share.
Protection Policy	Optionally, provide a protection policy for the file system. PowerStore supports both snapshots and replication for file storage protection.
File QoS Policy	Optionally, select a file QoS policy for the file system. **NOTE:** If the selected policy sets a bandwidth that exceeds the maximum bandwidth set for the NAS server, then the effective bandwidth is the maximum bandwidth of the server.
Summary	Review the summary. Go back to make the necessary updates.

3. Click **Create File System**.
   The file system is displayed in the File System list, and if you created an SMB Share, it is displayed in the SMB Share list.

File system advanced settings for SMB

You can add advanced settings to SMB-enabled file systems while creating a file system.

Table 4. File system advanced settings for SMB

Setting	Description
Sync Writes Enabled	When you enable the synchronous writes option for a Windows (SMB) or multiprotocol file system, the storage system performs immediate synchronous writes for storage operations, regardless of how the SMB protocol performs write operations. Enabling synchronous write operations enables you to store and access database files (for example, MySQL) on storage system SMB shares. This option guarantees that any write to the share is done synchronously and reduces the chances of data loss or file corruption in various failure scenarios, for example, loss of power. This option is disabled by default. **NOTE:** The synchronous writes option can have a significant impact on performance. It is not recommended unless you intend to use Windows file systems to provide storage for database applications.
Oplocks Enabled	(Enabled by default) Opportunistic file locks (oplocks, also known as Level 1 opslock) enable SMB clients to buffer file data locally before sending it to a server. SMB clients can then work with files locally and periodically communicate changes to the storage system rather than having to communicate every operation over the network to the storage system. This feature is enabled by default for Windows (SMB) and multiprotocol file systems. Unless your application handles critical data or has specific requirements that make this mode or operation unfeasible, leaving the oplocks enabled is recommended. The following oplocks implementations are supported: ● Level II oplocks, which informs a client that multiple clients are accessing a file, but no client has yet modified it. A level II oplock lets the client perform read operations, and file attribute fetches by using cached or read-ahead local information. All other file access requests must be sent to the server. ● Exclusive oplocks, which informs a client that it is the only client opening the file. An exclusive oplock lets a client perform all file operations by using cached or read-ahead information until it closes the file, at which time the server must be updated with any changes that are made to the state of the file (contents and attributes). ● Batch oplocks, which informs a client that it is the only client opening the file. A batch oplock lets a client perform all file operations by using cached or read-ahead information (including opens and closes). The server can keep a file opened for

Table 4. File system advanced settings for SMB (continued)

Setting	Description
	a client even though the local process on the client machine has closed the file. This mechanism curtails the amount of network traffic by letting clients skip the extraneous close and open requests.
Notify on Write Enabled	Enable notification when a file system is written to. This option is disabled by default.
Notify on Access Enabled	Enable notification when a file system is accessed. This option is disabled by default.
Enable SMB Events publishing	Enable the processing of SMB events for this file system.

Create an SMB share

You can create an SMB share on a file system that has been created with an SMB-enabled NAS server.

Steps

1. Select **Storage** > **File System** > **SMB Share**.
2. Click **Create** and continue to work through the **Create SMB Share** wizard.

Option	Description
Select File System	Select a file system that has been enabled for SMB.
Select a snapshot of the file system	Optionally, select one of the file system snapshots on which to create the share. Only snapshots are supported for file system protection policies. Replication is not supported for file systems.
SMB Share Details	Enter a name, and local path for the share. When entering the local path: ● You can create multiple shares with the same local path on a single SMB file system. In these cases, you can specify different host-side access controls for different users, but the shares within the file system have access to common content. ● A directory must exist before you can create shares on it. If you want the SMB shares within the same file system to access different content, you must first create a directory on the Windows host that is mapped to the file system. Then, you can create corresponding shares using PowerStore. You can also create and manage SMB shares from the Microsoft Management Console. PowerStore also created the SMB Share path, which uses the host to connect to the share. The export path is the IP address of the file system, and the name of the share. Hosts use either the file name or the share path to mount or map to the share from a network host.
Advanced SMB Properties	Enable one or more of the Advanced SMB Settings. ● Continuous Availability ● Protocol Encryption ● Access-based Enumeration ● Branch Cache Enabled Decide which objects are available when the share is offline. For details see Advanced SMB properties.

Next steps

Once you create a share, you can modify the share from PowerStore or using the Microsoft Management Console.

To modify the share from PowerStore, select the share from the list on the **SMB Share** page, and click **Modify**.

Advanced SMB share properties

You can configure the following advanced SMB share properties when you create an SMB share or change its properties:

Table 5. Advanced SMB Properties

Option	Description
Continuous Availability	Gives host applications transparent, continuous access to a share following a failover of the NAS server on the system (with the NAS server internal state saved or restored during the failover process). **NOTE:** Enable continuous availability for a share only when you want to use Microsoft Server Message Block (SMB) 3.0 protocol clients with the specific share.
Protocol Encryption	Enables SMB encryption of the network traffic through the share. SMB encryption is supported by SMB 3.0 clients and above. By default, access is denied if an SMB 2 client attempts to access a share with protocol encryption enabled. You can control this by configuring the RejectUnencryptedAccess registry key on the NAS nonencrypted Server (key path is HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\RejectUnencryptedAccess). 1 (default) rejects access and 0 allows clients that do not support encryption to access the file system without encryption.
Access-Based Enumeration	Filters the list of available files and directories on the share to include only those to which the requesting user has read access. **NOTE:** Administrators can always list all files.
Branch Cache Enabled	Copies content from the share and caches it at branch offices. This allows client computers at branch offices to access the content locally rather than over the WAN. BranchCache is managed from Microsoft hosts.
Offline Availability	Configures the client-side caching of offline files: • **None**: Client-side caching of offline files is not configured (default). • **Manual**: Files are cached and available offline only when caching is explicitly requested. • **Programs**: All files that clients open from the share are automatically available offline. Executable files that were previously cached locally are run from the cached copy even when the share is available. • **Documents**: All files that clients open from the share are automatically available offline. When a user accesses a file from a share the content is automatically cached to be available to the user in offline mode. All files that are opened continue to be cached and available for offline access until the cache is full. Cached content continues to be synchronized with the version on the server. Files that were not opened are not available offline.

Manage ACLs

The Windows client sets and modifies Access permissions of SMB shares (known as Access Control Lists or ACLs) using the MMC console. You can now manage ACLs of SMB shares on the SDNAS cluster directly from PowerStore, using UI or REST API.

NOTE: For details on using the REST API to set ACLs, see *Dell PowerStore REST API Reference Guide* at dell.com/powerstoredocs.

NOTE: Access permissions of files and directories in the SMB shares can be managed only using the Windows client.

To open the Access Control List screen using the PowerStore Manager, select **Storage** > **File Systems** > **SMB Shares** > **[SMB share]** > **More Actions** > **Access Control List**.

The Access Control List screen displays the list of Access Control Entries (ACEs) that are defined for the selected SMB. For each ACE, the trustee name or ID, access level, and access type are listed. You can filter the list by either of the attributes.

NOTE: The default ACE grants full permission to everyone.

From the Access Control List dialog you can:

- Add ACE - For details, see Add an Access Control Entry.
- Modify ACE - Edit any of the selected ACE fields.
- Delete the selected ACE.
- Refresh ACL (under **More Actions**) - Use this option if you modified the ACL using Windows MMC console or REST API. The Refresh option updates the ACL with the changes.

Add an Access Control Entry

About this task

An ACE consists of the following attributes:

- Trustee Type - User, Group, Security Identifier (SID), or WellKnown
- Trustee Name/ID - The format of this field is determined according to the trustee type:
  - User Name - domain/username
  - Group Name - domain/groupname
  - SID - SID format (for example, S-1-2-34-567890123-456789012-3456789012-34)
  - WellKnown - For example, "Everyone"
- Access Level - Read, Change, or Full
- Access Type - Allow, or Deny

Steps

1. Select **Storage** > **File Systems** > **SMB Shares** > **[SMB share]** > **More Actions** > **Access Control List**.
2. On the **Access Control List** window, select **Add ACE**.
3. Set the ACE fields and click **Save**.
   The new ACE is added to the ACL.
4. Click **Apply** to save the changes.

5

More file system features

This chapter contains the following information:

Topics:

File-level retention

File-level retention (FLR) enables you to prevent modifications or deletion of locked for a specified retention period. Protecting a file system using FLR enables you to create a permanent, and unalterable set of files and directories. FLR ensures data integrity and accessibility, simplifies archiving procedures for administrators and improves storage management flexibility.

There are two levels of file-level retention:

- Enterprise (FLR-E) - Protects data from changes that are made by users and storage administrators using SMB, NFS, and FTP. An administrator can delete an FLR-E file system which includes locked files.
- Compliance (FLR-C) - Protects data from changes that are made by users and storage administrators using SMB, NFS, and FTP. An administrator cannot delete an FLR-C file system which includes locked files. FLR-C complies with SEC rule 17a-4(f).

The following restrictions apply:

- File-level retention is available on unified PowerStore system 3.0 or later.
- FLR is not supported in VMware file systems.
- Enabling a file-level retention for a file system and the level of FLR are set at file system creation time and cannot be modified.
- FLR-C does not support restoring from a snapshot.
- When refreshing using a snapshot, both file systems must be of the same FLR level.
- When replicating a file system, source and destination file systems must be of the same FLR level.
- A cloned file system has the same FLR level as the source (cannot be modified).

The FLR mode is displayed in the **File Systems** screen.

Configure DHSM server

Prerequisites

File-level retention requires DHSM server credentials.

DHSM server is also required for Window hosts that want to use FLR and are required to install FLR toolkit that enables managing FLR-enabled file systems.

Steps

1. Select **Storage** > **NAS Servers** > **[NAS server]** > **Protection** > **DHSM**.
2. If disabled, slide the button to **Enabled**.
3. Enter the user name and password for the DHSM server and verify the password.
4. Select **Apply**.

Configure file-level retention

File-level retention is configured at file system creation. For details, see Create a file system.

NOTE: Retention period parameters can be modified later.

Modify file-level retention

About this task

Retention period parameters can be set at file system creation or later and can be modified. Modifying retention period parameter does not affect files that are already locked.

Steps

1. Select **Storage** > **File Systems** > **[file system]** > **Security & Events** > **File-Level Retention**.
2. Set the retention period parameters:
   - Minimum retention period - Specifies the shortest period for which an FLR-enabled file system can be protected (default value is one day).
   - Default retention period - Used when a file is locked and a retention period is not specified (default value is one year).
   - Maximum retention period - Specifies the longest period for which an FLR-enabled file system can be protected (default value is infinite).
3. Optionally, set the advanced settings:
   - Automatic file locking - You can specify whether to automatically lock files in an FLR-enabled file system and set a policy interval that determines the time period between file modification and automatic lock (policy interval default value is one hour).
   - Automatic file deletion - You can specify whether to automatically delete locked files after their retention period is expired. The first scan for locating files for deletion is seven days after the feature is enabled.
4. Select **Apply**.

File system quotas

You can track and limit drive space consumption by configuring quotas for file systems at the file system or directory level. You can enable or disable quotas at any time, but it is recommended that you enable or disable them during non-peak production hours to avoid impacting file system operations.

NOTE: You cannot enable quotas for read-only file systems.

NOTE: Quotas are not supported in VMware file systems.

NOTE: When you create a replication session, quotas are not visible on the destination system even if they are enabled on the source system.

Types of quotas

There are three types of quotas that you can put on a file system.

Table 6. Quota types

Type	Description
User Quotas	Limits the amount of storage that an individual user consumes by storing data on the file system.
Tree Quota	Tree quotas limit the total amount of storage that is consumed on a specific directory tree. You can use tree quotas to: • Set storage limits on a project basis. For example, you can establish tree quotas for a project directory that has multiple users sharing and creating files in it.

Table 6. Quota types (continued)

Type	Description
	• Track directory usage by setting the tree quota hard and soft limits to 0 (zero). **NOTE:** If you change the limits for a tree quota, the changes take effect immediately without disrupting file system operations.
User quota on a quota tree	Limits the amount of storage that an individual user consumes by storing data on the quota tree.

Quota limits

Table 7. Hard and soft limits

Type	Descriptions
Hard	A hard limit is an absolute limit on storage usage. If a hard limit is reached for a user quota on a file system or quota tree, the user cannot write data to the file system or tree until more space becomes available. If a hard limit is reached for a quota tree, no user can write data to the tree until more space becomes available.
Soft limit	A soft limit is a preferred limit on storage usage. The user is allowed to use space until a grace period has been reached. The user is alerted when the soft limit is reached, until the grace period is over. After that, an out of space condition is reached until the user gets back under the soft limit.

Quota grace period

The Quota grace period enables you to set a specific grace period to each tree quota on a file system. The grace period counts down the time between the soft and hard limit, and alerts the user about the time remaining before the hard limit is met. If the grace period expires you cannot write to the file system until more space has been added, even if the hard limit has not been met.

You can set an expiration date for the grace period. The default is 7 days, alternatively you can set the grace period expiration date to an infinite amount of time (the grace period never expires), or for a specified number of days, hours or minutes. Once the grace period expiration date is met, the grace period no longer applies to the file system directory.

Additional information

For more information about quotas, see the *Dell PowerStore File Capabilities White Paper*.

Enable user quotas

You must enable quotas and set the user quota defaults before you can add a user quota to a file system.

Steps

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas**.
2. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Properties**.
3. Slide the **Disabled** button to **Enabled**.
4. Enter the default **Grace Period** for the user quota on the file system which will count down the time after the soft limit is met until the hard limit is met.
5. Enter a default **Soft Limit**, and a default **Hard Limit** and click **Update**.

Add a user quota onto a file system

Create a user quota on a file system to limit or track the amount of storage space that individual users consume on that file system. When you create or modify user quotas, you can use default hard and soft limits that are set at the file-system level.

Prerequisites

You must enable Quotas and set the User Quota defaults before you can add a User Quota to a files system. See Enable User Quotas.

NOTE: You cannot create quotas for read-only file systems.

Steps

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **User**.
2. Select **Add** on the **User Quota** page.
3. In the **Add User Quota** wizard, provide the requested information. To track space consumption without setting limits, set **Soft Limit** and **Hard Limit** to 0, which indicates no limit.
4. Select **Add**.

Add a quota tree onto a file system

About this task

Create a quota tree at the directory level of a file system to limit or track the total storage space that is consumed for that directory.

Steps

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Select **Add**.
3. Slide the **Enforce User Quota** to the right to enabled User Quota defaults on the Tree Quota.
4. Provide the requested information.
   - Enter a **Grace Period** to count down the time between the soft and hard limit. You will begin to receive alerts once the grace period is reached.
   - To track space consumption without setting limits, set the **Soft Limit** and **Hard Limit** fields to 0, which indicates no limit.
5. Select **Add**.

Add a user quota onto a quota tree

Create a user quota on a quota tree to limit or track the amount of storage space that individual users consume on that tree. When you create user quotas on a tree, you can to use the default grace period and default hard and soft limits that are set at the tree-quota level.

Steps

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Select a path, and click **Add User Quota**.
3. On the **Add User Quota** screen, provide the requested information. To track space consumption without setting limits, set the **Soft Limit** and **Hard Limit** fields to 0, which indicates no limit.

File Quality of Service (QoS)

In a system that is running varying workloads with unpredictable demands, Quality of Service ensures that critical applications can get priority and provides predictable performance for each application.

You can apply Quality of Service (QoS) policies to set maximum bandwidth for NAS servers and file systems.

When you assign a QoS policy to a NAS server or file system, SDNAS enforces the policy on NFS/SMB services.

Bandwidth limits are applied based on NFS/SMB, and SFTP/FTP protocols.

If the set bandwidth exceeds the maximum bandwidth set for the NAS server, then the effective bandwidth is the maximum bandwidth of the server.

NOTE: It may take some time for a QoS policy to take effect.

NOTE: QoS is not supported with NAS server clones, file system clones, snapshots, snapshot clones, and snapshot refresh.

NOTE: Bandwidth applied to NAS servers and file systems as part of an assigned QoS policy can deviate within a margin of 10 percent.

File QoS limits:

- A QoS policy can include one I/O limit rule.
- Up to 100 file QoS policies can be defined.
- Up to 100 file QoS rules can be defined.
- Only one QoS policy can be applied to a NAS server or file system.
- The same QoS policy can be assigned to multiple NAS servers and file systems.

QoS and file replication:

- When the NAS server has a replication rule, the assigned QoS policy is replicated to the destination server.
- When you modify QoS policies that are assigned to the NAS server, the changes are replicated to the destination server.
- It is not possible to modify the replicated QoS policy configuration on the destination server.
- It is not possible to assign a QoS policy to a NAS server or file system on the destination server.
- After assigning a QoS policy to a NAS server or file system on the source server, it is not possible to unassign the policy from the destination server.
- After you unassign a QoS policy from a NAS server, the policy should be unassigned at the destination as well.
- After failover, you can assign, unassign, and modify replicated QoS policies.

File QoS limits

You can create I/O limit rules for NAS servers and file systems. An I/O limit rule defines the allowed maximum bandwidth.

- Each NAS server or file system can be associated with only one limit rule.
- Each policy can include only one rule.
- You can define up to 100 rules.

I/O limit rules apply only to I/O from external hosts, and not to internal asynchronous or synchronous replication operations or migration I/O.

I/O limit rules are not applied to objects that are created internally, such as NDMP backups served by an NDMP server in SDNAS.

Specific alerts for file QoS limits are not supported. To learn if the set limits require an adjustment, you can monitor the Latency, IOPS, and Bandwidth charts for each NAS server and file system.

Create a Quality of Service (QoS) bandwidth limit rule and policy

About this task

You can create a bandwidth limit rule and add it to a QoS policy.

Steps

1. Select **Storage** > **Quality of Service (QoS)** > **File I/O Limit Rules**.
2. Select **Create**.
3. On the **Create File I/O Limit Rule** slide-out, set the rule name and max bandwidth (MB/s).
4. Select **Create**.
   The rule is added to the File I/O Limit Rules table.

5. Select **File QoS Policies**.
6. Select **Create**.
7. On the **Create File QoS Policy** slide-out, set the policy name. You can also add a description.
8. From the rule list, select the rule that you want to add to the policy.
9. Select **Create**.
   The policy is added to the File QoS Policies table.

Assign a file QoS policy

About this task

After you define an I/O limit rule as part of a file QoS policy, you can assign it to a NAS server or a file system. You can also modify the assigned QoS policy.

NOTE: It is also possible to assign a QoS policy as part of the procedure for creating a NAS server or a file system.

Steps

1. Select **Storage** > **NAS Servers** or **Storage** > **File Systems**.
2. Select the checkbox next to the relevant NAS server or file system.
3. Select **More Actions** > **Change QoS Policy**.
4. On the **Change QoS Policy** slide-out, select a file QoS policy, and then select **Apply**.
   The policy is assigned. You can view the assigned policy name on the **QoS Policy** column in the NAS Server and File Systems tables. You can view the impact of the assigned policy on performance by selecting **Storage** > **NAS Servers** > **[NAS server]** > **Performance** or **Storage** > **File Systems** > **[file system]** > **Performance**.

   NOTE: You can also set the QoS policy by selecting the relevant NAS server or file system and then selecting **Modify**.

Modify a file QoS policy

You can modify a QoS policy by selecting a different I/O limit rule.

Prerequisites

You cannot modify a policy that is assigned to a NAS server or file system.

Steps

1. Select **Storage** > **Quality of Service (QoS)**.
2. From the **File QoS Policies** table, select the checkbox next to the QoS policy that you want to modify.
3. Select **Modify**.
4. In the **Modify QoS Policy** window, you can modify the name and description of the policy, and select a different I/O limit rule.
5. Select **Apply**.

   NOTE: You can also modify a QoS policy from the storage resource **Properties** screen.

Delete a file QoS policy

Prerequisites

Ensure that the QoS policy that you want to delete is not assigned to a NAS server or file system.

Steps

1. Select **Storage** > **Quality of Service (QoS)**.
2. From the **File QoS Policies** table, select the QoS policy that you want to delete.
3. Select **More Actions** > **Delete**.

4. Select **Delete** to confirm.

6

NAS server replication

This chapter contains the following information:

Topics:

Overview

To enable enhanced redundancy and recovery if data loss occurs, PowerStore enables you to replicate NAS servers from a local system to a remote system.

By default, replication occurs at a NAS server level - all the file systems within the replicated NAS server are replicated to the remote system. You can select to add file systems or delete file systems from the NAS server when it is a part of a replication session.

You can select asynchronous replication, where the systems are synchronized based on a defined RPO, or synchronous replication, where changes are replicated from the source system to the destination system immediately when they occur.

The following pre-requisites are required to enable file replication:

- A file remote system
- A File Mobility network must be configured and mapped (see *PowerStore T and Q Networking Guide for Storage Services* on the PowerStore Documentation page).
- A protection policy that includes a replication rule.

Consider the following for NAS server replication:

- It is not required to define separate protection policies for NAS servers. The same protection policies can be applied to both block and file replication.
- You can delete file systems from the source system of a replication session. After deletion, only the remaining file systems are replicated to the destination. The status of the destination system is not impacted following the file system deletion. If you delete file systems from a replicating source NAS server and then fail over to the destination system, the file systems that were deleted from the old source are not replicated by the new source. If you want to replicate these file systems, generate clones that can be replicated and delete the file systems.
- You can fail over a replication session to the remote system. Failover occurs for all the file systems within the failed over NAS server.
- When you create a replication session, quotas are not visible on the destination system even if they are enabled on the source system.
- For asynchronous replication, RPO is configured at the NAS server level and is identical across all associated file systems.
- For synchronous replication, increasing the size of a file system that is under replication requires pausing the replication session first. Reducing the size of a file system does not require pausing the replication session.
- For synchronous replication, it is not possible to change the network latency of the replication system pair to a higher value than five milliseconds when synchronous replication sessions are defined.
- Switching between synchronous and asynchronous replication is not supported for file replication.

For detailed information about NAS server replication procedures, see *Protecting your Data* on the PowerStore Documentation page.

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.
- Perform a planned failover.

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 NAS server 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.

In PowerStoreoperating system 3.6 and later, 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.

Perform a planned failover

You can use planned failover to test disaster recovery. When you perform a planned failover, the NAS server replication session is manually failed over from the source system to the destination system. Before the failing over, the destination system is synchronized with the source system, to prevent any data loss.

NOTE: Failing over the production NAS server to the destination system may impact production.

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

When operation is normal, changes made to the NAS server and file systems during the DR test are preserved and replicated back to the original source when reprotect is initiated (either manually or automatically). However, if you do not want to save

the changes made during DR testing (either data or configuration), you can select to discard the changes, using REST API or PSTCLI commands:

- REST API - `POST /replication_session/{id}/reprotect discard_changes_after_failover`
- PSTCLI - `replication_session -id <value> reprotect [-discard_changes_after_failover]`

The changes that are discarded:

- For NAS Servers:
  - Configuration changes
- For file systems:
  - Configuration changes
  - File system data changes
  - Snapshot resources
  - File system size changes
  - Quota changes
- For exports and shares:
  - NFS export changes
  - SMB share changes

NOTE: This option is only supported for asynchronous replication.

For details on using the REST API and CLI to discard changes after failover, see *Dell PowerStore REST API Reference Guide* and *Dell PowerStore CLI Reference Guide* at dell.com/powerstoredocs.

After the NAS server is reprotected, you can initiate a planned failover again to bring the resources online on the original source system.

NOTE: Do not perform unplanned failover for disaster recovery purposes. Unplanned failover should be used only when the source system is inaccessible.

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.

NOTE: After failover, user quotas are not visible on the destination system (which has become the new source). To view the user quotas, manually refresh the quotas by selecting **Storage** > **File Systems**, checking the checkbox next to the relevant file system, and then selecting **More Actions** > **Refresh Quotas**.

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...).

7

Using CEPA with PowerStore

This chapter contains the following information:

Topics:

Events publishing

CEE enables third-party applications to receive event information from the storage system upon accessing file systems.

The Common Event Enabler (CEE) provides an event publishing solution for PowerStore clients that allow third-party applications to register and receive event notification and context from the storage system when accessing file systems. Receiving event notification enables you to take event-driven actions on the storage to prevent security threats such as ransomware or unauthorized access.

The CEE Common Events Publishing Agent (CEPA) consists of applications that are designed to process SMB and NFS files and directory event notifications. The CEPA delivers both event notification and associated context to the application in one message. Context can consist of file metadata or directory metadata that is needed for business policy decisions.

To enable CEE CEPA support, you must enable CEE CEPA and create an Event Publishing Pool on the NAS server.

An Event Publishing Pool defines the CEPA servers and the specific events that trigger notifications.

After configuring the NAS server, you can enable events publishing on the file system from which you want to receive events. When a host generates an event on the file system over SMB or NFS, the information is forwarded to the CEPA server over an HTTP connection. The CEE CEPA software on the server receives the event and publishes it, thus enabling the third-party software to process it.

To use the Events Publishing Agent, it is required to have a PowerStore system with at least one NAS server configured on the network.

For additional information about CEPA, which is part of the Common Event Enabler (CEE), see *Using the Common Event Enabler on Windows Platforms* on the Dell Technologies Support site.

Create a publishing pool

Prerequisites

To create an event publishing pool, you must have an Events Publishing (CEPA) server FQDN.

About this task

An Event Publishing Pool defines the CEPA server and the specific events that trigger notifications. Define at least one of the following event options:

- Pre Events - Events that are sent to the CEPA server for approval before processing.
- Post Events - Events that are sent to the CEPA server after they occur for logging or auditing purposes.
- Post Error Events - Error events that are sent to the CEPA server after they occur for logging or auditing purposes.

Steps

1. Select **Storage** > **NAS Servers**.
2. Select **NAS Settings**.

3. In the **Event Publishing** window, select **Publishing Pools** and then select **Create**.
4. Enter a **Pool Name**.
5. Enter the CEPA server FQDN.
6. In the Event Configuration section, click the event types and select the events that you want to add to the pool.
7. Click **Apply** to create the Events Publishing Pool.

Create an event publisher

About this task

After configuring publishing pools, create an event publisher to set the response to the different event types.

NOTE: Event publishers are created at the system level and one event publisher can be associated with multiple NAS servers.

Steps

1. Select **Storage** > **NAS Servers**.
2. Select **NAS Settings**.
3. Select **Event Publishers** and then select **Create**.
4. Continue to work through the **Create Event Publisher** wizard.

Wizard Screen	Description
Select Publishing Pools	• Enter a name. • Select up to 3 Publishing Pools. To create a new Publishing Pool, click **Create**.

Configure Event Publisher	• Pre-Events Failure Policy - Select the wanted behavior when all CEPA servers are offline for pre-events:
	  ○ Ignore (default) - Assume that all events are acknowledged.
	  ○ Deny - Deny events that require approval until CEPA servers are online.
	• Post-Events Failure Policy - Select the wanted behavior when all CEPA servers are offline for post-events:
	  ○ Ignore (default) - Continue operating. Events that occurred while the CEPA servers are down, will be lost.
	  ○ Accumulate - Continue operating and save events to a local buffer (up to 500 MB).
	  ○ Guarantee - Continue operating and save events to a local buffer (up to 500 MB). Deny access when buffer is full.
	  ○ Deny - Deny access to file systems when the CEPA servers are offline.
	• HTTP/Microsoft RPC
	• HTTP Port

5. Select **Apply** to create the Event Publisher.

Enabling an event publisher for a NAS server

About this task

After configuring the event publisher, enable it for the NAS server and all the file systems that are defined on it.

Steps

1. Select **Storage** > **NAS Servers** > **[nas server]**.
2. On the **Security & Events** page, select **Events Publishing**.
3. Select an Event Publisher from the list and enable it.
4. Select whether to enable the event publisher for all the file systems that are defined on the NAS server.

   Alternatively, you can select to enable the event publisher for specific file systems. For details, see Enable event publisher for file system.

5. Click **Apply**.

Enable event publisher for a file system

About this task

You can enable the event publisher for selected file systems.

Steps

1. Select **Storage** > **File Systems** > **[file system]**.
2. On the **Protection** page, select **Events Publishing**.
3. Enable the event publisher for the file system and select the protocol.
4. Click **Apply**.