DELL EMC PowerStore Configuring SMB User Guide

Home » Dell » DELL EMC PowerStore Configuring SMB User Guide

Contents

Dell EMC PowerStore

Configuring SMB

3.x

October 2022
Rev. A03

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.**

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.

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 Overview

This chapter contains the following information:

Topics:

- SMB support
- Planning considerations

SMB support

PowerStore T model supports 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.

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 appliances. File storage is not supported with PowerStore X 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 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 Networking Guide for PowerStore T Models for details.

Deployment requirements

NAS services are only available on PowerStore T model appliances. If you are running PowerStore X model appliances, this service is not available.

You must have chosen **Unified** during initial configuration of your PowerStore T model appliance. If you chose **Block Optimized** while running the Initial Configuration Wizard, NAS services were not installed. To install NAS services, you will need to have your system reinitialized by a customer support representative. 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 an LACP bond for NAS traffic

You can combine several network interfaces into a network bond for redundancy and high availability purposes.

About this task

Network bonding is a process in which two or more network interfaces are combined to a single interface. Using network bonding provides performance improvements and redundancy by increasing the network throughput and bandwidth. If one of the combined interfaces is down the other interfaces allow to maintain a stable connection.

You can use network bonding by creating a Link Aggregate Group (LAG) for NAS traffic.

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 wish 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 will need to select the bond name when you create the NAS server.

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

Refer to the following for additional information:

Table 2. Documentation resources

Document	Description	Location
PowerStore Networking Guide for PowerStore T Models	Provides network planning and configuration information .	https://www.dell.com/powerstoredocs
PowerStore Configuring NFS Guide	Provides information necessary to configure SMB shares with PowerStore Manager.	
Dell EMC PowerStore File Capabilities White Paper	Discusses the features, functionality, and protocols supported by Dell EMC 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
- Create NAS server for SMB (Windows-only) file systems
- Change NAS server settings

Overview of configuring NAS servers

Before you can provision file storage on the PowerStore T model appliance, 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 (Windows-only) 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 computer 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 – If you created an LACP bond, select it from the list (see Create an LACP bond for NAS traffic). • 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	Select a protection 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 will use.
  ⓘ**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 & Events** page, enable or disable NDMP.
For details see Enable NDMP Protection and Events.
6. On the **Security** 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
Additional NAS Server Features

This chapter contains the following information:

Topics:

- Configure FTP or SFTP sharing protocol
- Configure NAS server networks
- Enable NDMP backup
- Configure NAS server Security

Configure 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 domainuser, SMB authentication is used. SMB authentication uses the Windows Domain Controller.

Steps

1. Select **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:** You cannot 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. Click:

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 need to 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 EMC 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 user name is always ndmp.
4. Re-enter 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 **Antivirus** 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. 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 AntiVirus 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 PowerStore Release Notes. For additional information about CAVA, which is part of Common Event Enabler (CEE), see Using the Common Event Enabler on Windows Platforms on **https://www.dell.com/support**.

Enable Common AntiVirus Agent (CAVA)

You enable CAVA, and upload the CAVA configuration file when you want to add anti-virus protection to your SMB shares.

Prerequisites

To enable Antivirus scanning, you need to create a user in the Active Directory, and then give it permissions on the CAVA server to perform scans.

Steps

1. From PowerStore Manager go to the **Storage** > **NAS Servers** > **[nas server]** > **Security & Events** > **Antivirus** tab.
2. If Disabled is on, slide the button to change to Enabled.
3. If you do not have a current CAVA configuration file available:

> **a.** Click **Retrieve Current Configuration**.
> **b.** Complete the CAVA configuration file template.
> **c.** Upload the updated CAVA configuration file.

4. Click **Enabled** and **Apply** to enable Antivirus scanning.

Configurable AntiVirus 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. Antivirus 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 will be scanned.	Yes	masks=*.exe:*.docx:*.com
excl=	Lists file extensions that will be excluded during the scan.	No	excl=pagefile.sys
maxsize=<n>	Integer. Sets the maximum file size for files that will be 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. 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 assigned to either a simple user account or user account that is part of a domain that the CAVA service is running under on the CEE machine.	No	User account: msrpcuser=user1 Domain/user account: msrpcuser=CEE1/user1
httpport=	Specifies the HTTP port number on the CEE machine that the system will use.	No	httpport=12228
RPC Retry Timeout	Sets the timeout (in milliseconds) of the RPC retry.	No	RPCRetryTimeout=4000 milliseconds
RPC RequestTimeout	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
- Create an SMB share

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 immediately shows 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 are made by users 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 are made by users and administrators 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. 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.
Summary	Review the summary. Go back to make 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 writes 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 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 Server. 1 (default) rejects non-encrypted 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.
BranchCache 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: • **Manual**: Files are cached and available offline only when caching is explicitly requested. • **Programs and files opened by users**: All files that clients open from the share are automatically cached and available offline. Clients open these files from the share when they are connected to it. This option is recommended for files with shared work. • **Programs and files opened by users, optimize for performance**: All files that clients open from the share are automatically cached and available offline. Clients open these files from the share’s local cache, if possible, even when they are connected to the network. This option is recommended for executable programs. • **None**: Client-side caching of offline files is not configured.

5 More file system features

This chapter contains the following information:

Topics:

- File-level retention
- File system quotas

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 at a later time.

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.

Types of quotas

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

Table 6. Quota types

Type	Description
User Quotas	Limits the amount of storage that is consumed by an individual user 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. • 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 is consumed by an individual user 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, provides the ability 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 can not 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 and the Grace Period will never expire, or for specified number of days, hours or minutes. Once the Grace Period expiration date is met, the Grace Period will no longer apply to the File System directory.

Additional information

For more information on quotas, see the Dell EMC 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 files 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 the right until it is **Enabled**.
4. Enter the default **Grace Period** for the user quota on the file system which will count down time after the soft limit is met until the hard limit will be 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.

6
NAS Server replication

This chapter contains the following information:

Topics:

- Overview

Overview

PowerStore enables you to replicate NAS servers asynchronously between a local system and a remote system. Replication occurs at a NAS server level – all the file systems within the replicated NAS server are replicated to the remote system. RPO is configured at the NAS server level and is identical across all associated file systems.

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 fail over a replication session to the remote system. Failover occurs for all the file systems within the failed over NAS server.

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

- A file remote system
- A File Moblility network must be configured and mapped (see Networking Guide for PowerStore T models on

the PowerStore Documentation page at **https://www.dell.com/powerstoredocs**).

- A protection policy that includes a replication rule.

For detailed information about NAS server replication procedures, see Protecting your Data on the PowerStore Documentation page at **https://www.dell.com/powerstoredocs**.

7
Using CEPA with PowerStore

This chapter contains the following information:

Topics:

- Events publishing
- Create a publishing pool
- Create an event publisher
- Enabling an event publisher for a NAS server
- Enable event publisher for a file system

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 **https://www.dell.com/support**.

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**.

Documents / Resources

 Dell EMC PowerStore Configuring SMB 3.x October 2022 Rev. A06	**DELL EMC PowerStore Configuring SMB** [pdf] User Guide EMC PowerStore Configuring SMB, EMC, PowerStore Configuring SMB, Configuring SMB