Dell PowerStore

Configuring Multiprotocol File Sharing

4.1

February 2025
Rev. A01

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.

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.

Contents

1

Overview

This chapter contains the following information:

Topics:

About multiprotocol file sharing in PowerStore

To access a datafile shared by a NAS server over the network, host clients mainly use two file protocols: SMB and NFS. Windows clients user the SMB protocol, and UNIX clients use the NFS protocol. The NFS and SMB protocols have many differences, some of which are described in the following table:

Table 1. Main differences between NFS and SMB protocols

Feature	NFS	SMB
User Identification	Uses a User Identifier (UID) and Group Identifier (GID).	Uses a security Identifier (SID).
Lock policy	NFSv3 range locks are advisory, and NFSv4 range locks are advisory or mandatory (default).	SMB range locks are mandatory.
User authentication	Authentication is handled by one of the following: ● A previous local login to another UNIX system ● A UNIX Directory Service (NIS or LDAP), which looks up a UID/GID of the user. ● Local password and group files, which look up a UID/GID of the user.	Authentication is handled by Active Directory, which looks up the SID of a user. This requires NTP and DNS.
Security rules	Uses the UNIX credential that is associated with the authenticated user to check mode bits (NFSv3) or to check access rights in the NFSv4 ACL.	Uses the Windows credential that is associated with the authenticated user to check the SMB Access ACL.
Rename policy	Renaming a component of an open file is allowed.	Renaming a component of an open file is not allowed.

PowerStore supports a mixed NFS and SMB environment by providing simultaneous access to the same data for both NFS (v3 and v4) and SMB. The NAS server functionality is determined by the server sharing protocol configuration. To enable multiprotocol, select both SMB and NFS sharing protocol as part of the NAS server configuration. Then, create a file system off this NAS server, and finally, create both NFS and SMB shares on that file system.

To configure multiprotocol functionality, you must add the NAS server to a Windows Active Directory domain and configure a UNIX Directory Service (LDAP or NIS) or a local password and group files for the NAS server, or both. To use LDAP, it must adhere to the IDMU, RFC2307, or RFC2307bis schemas. Some examples include AD LDAP with IDMU, iPlanet, OpenLDAP. The LDAP server must be configured properly to provide UIDs for each user. For example, on IDMU, the administrator must go in to the properties of each user and add a UID to the UNIX Attributes tab.

The usernames in an NFS environment and in an SMB environment must match character for character. If there are discrepancies in the usernames, you can configure a user-mapping file (`ntxmap`) to map each NFS name to the corresponding SMB name, and each SMB name to the corresponding NFS name. You can also configure default UNIX and Windows account

names. The system uses the default Windows account name when it cannot find a match for an SMB name on NFS, and the default UNIX account name when it cannot find a match for an NFS name on SMB.

NOTE: When multiple users use the default accounts, quotas may be impacted.

When you configure a file system that supports multiprotocol access, you must also select an access policy to manage user access control for the file system. For detailed information about how security and file access works in a multiprotocol environment, see Deep dive: File system security and access in a multiprotocol environment.

The following figures show the high-level steps that are required for configuring multiprotocol file sharing.

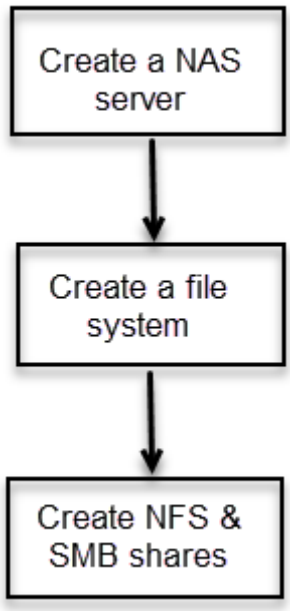

Figure 1. High-level steps for configuring multiprotocol file sharing

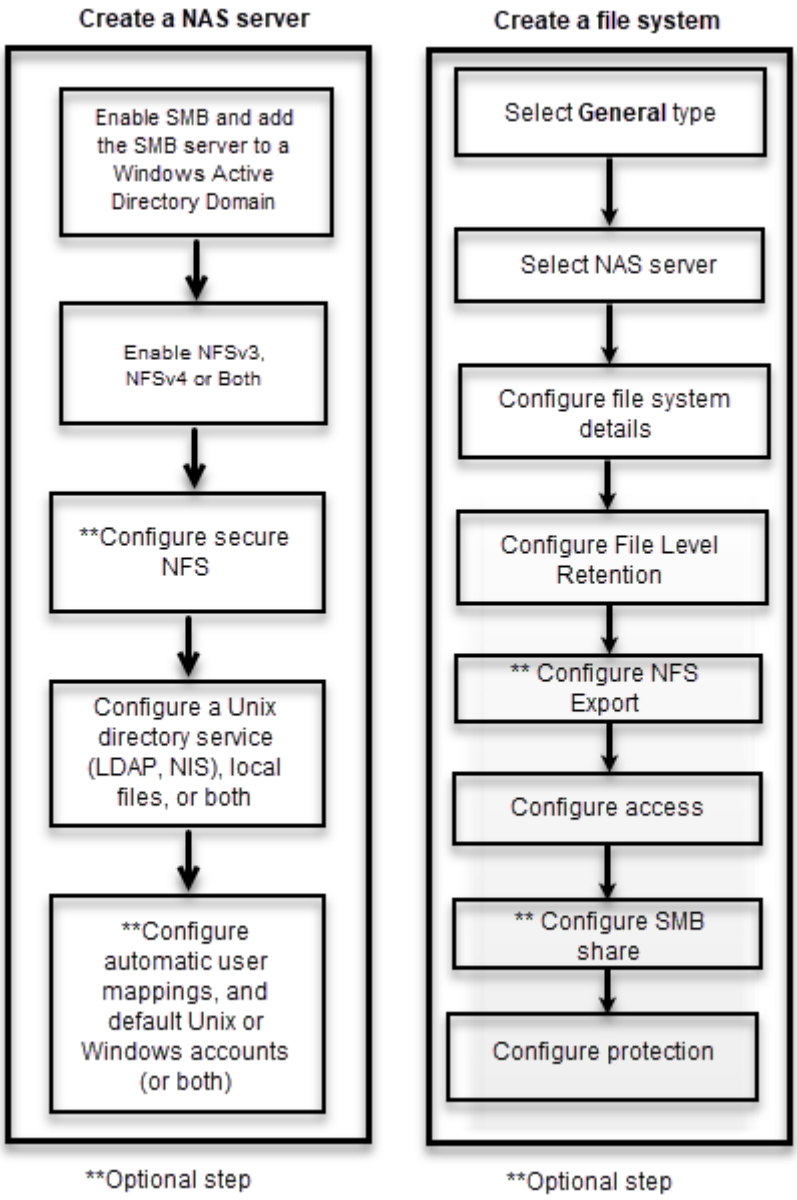

Figure 2. High-level steps for configuring multiprotocol file sharing (continued)

2

Deep dive: File system security and access in a multiprotocol environment

This chapter contains the following information:

Topics:

Security on file system objects

In a multiprotocol environment, security policy is set at the file system level, and is independent for each file system. Each file system uses its access policy to determine how to reconcile the differences between NFS and SMB access control semantics. Selecting an access policy determines which mechanism is used to enforce file security on the particular file system.

The default setting of native security maintains two separate sets of permissions for each file and the protocol that is used to access the file determines which permission set is checked. If the SMB protocol is used, ACLs are checked. If the NFS protocol is used, NFSv3 mode bits or NFSv4 ACL are checked.

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.

Native security model

The native security model is the default setting. This model manages access for each protocol separately using its own native security:

- Security for NFS shares uses the UNIX mode bits or NFSv4 ACL.
- Security for SMB shares uses the SMB Access Control List (ACL).

The two sets of permissions are independent and not synchronized. NFSv3 UNIX mode bits or NFSv4 ACL permission changes are synchronized without changing the SMB ACL. SMB ACL changes do not affect NFSv3 UNIX mode bits or NFSv4 ACL.

The permission set that is enforced depends on the access protocol that is being used.

UNIX security model

When the UNIX policy is selected, any attempt to change file level security from the SMB protocol, such as changes to Access Control Lists (ACLs), is ignored. UNIX access rights are named NFSv3 UNIX mode bits or NFSv4 ACL of a file system object. A bit string represents mode bits. Each bit represents an access mode or privilege that is granted to the user owning the file, the group associated with the file system object, and all other users. UNIX mode bits are represented as three sets of concatenated rwx (read, write, and execute) triplets for each category of users (user, group, or other). An ACL is a list of users and groups of users by which access to, and denial of, services is controlled.

The UNIX security model uses the NFSv3 UNIX mode bits or NFSv4 ACL for both protocols. When there is a request for SMB access, the UNIX credential that is built from the UDS/local files is used to check the NFSv3 mode bits or NVSv4 ACL for permissions. When NFSv3 UNIX mode bits or NFSv4 ACLs are changed, SMB ACL permissions are updated.

SMB ACL permission changes are allowed to avoid disruption, but are not maintained.

Windows security model

The Windows security model is based primarily on object rights, which involve the use of a Security Descriptor (SD) and its ACL. When an SMB policy is selected, changes to the mode bits from the NFS protocol are ignored.

Access to a file system object is based on whether permissions have been set to Allow or Deny using an SD. The SD describes the owner of the object and group SIDs for the object along with its ACLs. An ACL is part of the security descriptor for each object. Each ACL contains access control entries (ACEs). Each ACE in turn contains a single SID that identifies a user, group, or system unit and a list of rights that are denied or allowed for that SID.

The Windows security model uses the SMB ACL for both protocols. When there is a request for NFS access, the Windows credential that is built from the DC/LGDB is used to check the ACL for permissions. When SMB ACL permissions are changed, NFSv3 UNIX mode bits or NFSv4 ACLs are updated. NFSv3 UNIX mode bits or NFSv4 ACL permission changes are denied.

File system access

File access is provided through NAS servers, which contain file systems where data is stored. The NAS server provides access to this data for NFS and SMB file protocols by sharing file systems through SMB shares and NFS shares. The NAS server allows the sharing of the same data between SMB and NFS and provides simultaneous SMB and NFS access to a file system. Mapping of Windows users to UNIX users and defining of security rules (mode bits, ACLs, and user credentials) must be considered and configured for multiprotocol sharing.

User mapping

In a multiprotocol context, a Windows user must be matched with a UNIX user. However, a UNIX user has to be mapped to a Windows user only when the access policy is Windows. This matching is necessary so that file system security can be enforced, even if it is not native to the protocol.

The following components are involved in user mapping:

- UNIX Directory Services, local files, or both
- Windows resolvers
- Secure mapping (secmap) - a cache that contains all mappings between SIDs, and UID or GIDs used by a NAS server.
- ntxmap

NOTE: User mapping does not affect the users or groups that are local to the SMB server.

UNIX Directory Services and local files

UNIX Directory Services (UDSs) and local files are used to do the following:

- Return the corresponding UNIX account name for a particular User Identifier (UID).
- Return the corresponding UID and primary Group Identifier (GID) for a particular UNIX account name.

The supported services are:

- LDAP
- NIS
- Local files
- None (the only possible mapping is through the default user).

There must be a UDS enabled or local files enabled, or both local files and a UDS enabled for the NAS server when multiprotocol sharing is enabled. The UDS search order determines which is used for user mapping.

Windows resolvers

Windows resolvers are used to do the following for user mapping:

- Return the corresponding Windows account name for a particular Security Identifier (SID).
- Return the corresponding SID for a particular Windows account name.

The Windows resolvers are:

- The domain controller (DC) of the domain
- The Local Group Database (LGDB) of the SMB server

Secure mapping cache

A secure mapping cache (secmap) is a cache that stores mappings of users that connected to the NAS server. For each user the SID, username, and UID are stored. secmap only stores mappings that the standard mapping mechanism generates.

Storing SID-to-UID and primary GID and UID-to-SID mappings in a local cache ensures coherency across all file systems of the NAS server.

Storing user mappings in secmap reduces network traffic and increases efficiency. When a user mapping is stored in secmap, the NAS server leverages the local cache for future mapping lookups.

ntxmap

ntxmap is an optional local file that is used to provide name translations between protocols. When there is inconsistency between usernames, ntxmap is used to associate a Windows account to a UNIX account. For example, if there is a user who has an account titled Gerald on Windows and an account titled Gerry on UNIX, ntxmap makes the correlation between the two accounts.

ntxmap can also be used for advanced name translations, such as converting multiple usernames to a single username, and providing name conversions.

NOTE: ntxmap only provides username translations between protocols and does not provide any ID to username mappings.

SID to UID and primary GID mapping

The following sequence is the process that is used to resolve an SID to a UID, primary GID mapping:

1. secmap is searched for the SID. If the SID is found, the UID and primary GID mappings are resolved.
2. If the SID is not found in secmap, the Windows username that is related to the SID must be found.
   a. The local group database (LGDB) is searched for the SID to determine if the user is local. If the SID is found, the related Windows name is `SMB_SERVER\USER`. Since it is a local user for SMB-only access, no UNIX mapping is required.
   b. If the SID is not found in the LGDB, the DC of the domain is searched. If the SID is found in the domain, the related Windows name is `DOMAIN\USER`.
   c. If the SID cannot be resolved, access is denied. The failed mapping is added to the persistent secmap database.
3. If the default UNIX account is not used, the Windows name is translated to the UNIX name using ntxmap.
   a. If the Windows name is found in ntxmap, the entry is used as the UNIX name.
   b. If the Windows name is not found in ntxmap, or if ntxmap is disabled, the Windows name is used as the UNIX name.
4. The local files or UDS is searched using the UNIX name to find the UID and primary GID.
   a. If the UNIX username is found, the UID and primary GID mapping is resolved. The successful mapping is added to the persistent secmap database.
   b. If the UNIX username is not found, but the automatic mapping for unmapped Windows accounts feature is enabled, the UID is automatically assigned. The successful mapping is added to the persistent secmap database.
   c. If the UNIX username is not found, but a default UNIX account, the UID and primary GID mapping are mapped to that of the default UNIX account. The failed mapping is added to the persistent secmap database.
   d. If the UNIX username cannot be resolved, access is denied. The failed mapping is added to the persistent secmap database.

If the mapping is found, it is added in the persistent secmap database. If the mapping is not found, the failed mapping is added to the persistent secmap database.

The following diagram illustrates the process that is used to resolve an SID to a UID, primary GID mapping:

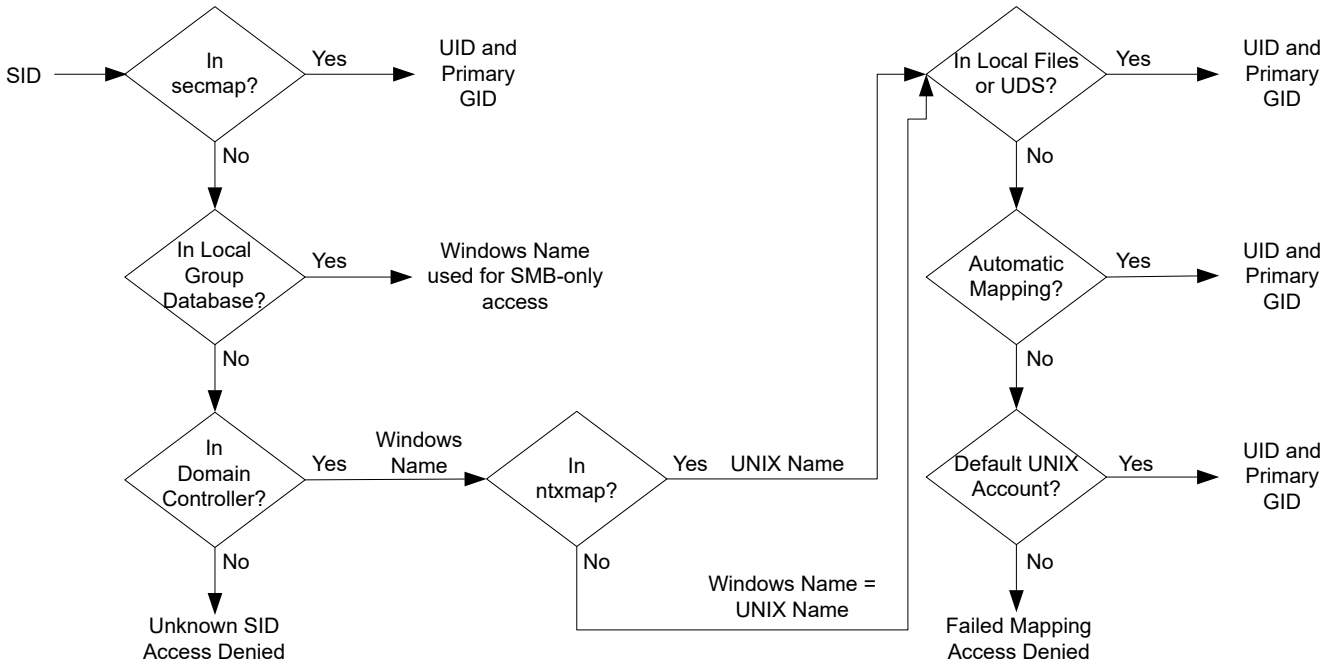

Figure 3. Process for resolving an SID to a UID, primary GID mapping

UID to SID mapping

The following sequence is the process that is used to resolve a UID to an SID mapping:

1. secmap is searched for the UID. If the UID is found, the SID mapping is resolved.
2. If the UID is not found in secmap, the UNIX name that is related to the UID must be found.
   a. Local files or the UDS is searched for the UID. If the UID is found, the related UNIX name is the username.
   b. If the UID is not found in the UDS but there is a default Windows account, the UID is mapped to the default Windows account. If it does not exist, the default Windows user is added to the persistent secmap database.
   c. If the UID is not resolved, access is denied.
3. If the default Windows account is not used, the UNIX name is translated into a Windows name, using ntxmap.
   a. If the UNIX name is found in ntxmap, the entry is used as the Windows name.
   b. If the UNIX name is not found in ntxmap, or if ntxmap is disabled, the UNIX name is used as the Windows name.
4. The DC or LGDB is searched for the Windows name to find the SID.
   a. The Windows name is searched for the DC. If the Windows name is found, the SID mapping is resolved.
   b. If the Windows name contains a period (.), and the part of the name following the last period matches an SMB server name, the LGDB of that SMB server is searched to resolve the SID mapping. If the Windows name is found, the SID mapping is resolved.
   c. If the Windows name is not found but there is a default Windows account, the SID is mapped to that of the default Windows account. If it does not exist, the default Windows user is added to the persistent secmap database.
   d. If the Windows name cannot be resolved, access is denied.

If the mapping is found, it is added in the persistent secmap database. If the mapping is not found, the failed mapping is added to the persistent secmap database.

The following diagram illustrates the process that is used to resolve a UID to an SID mapping:

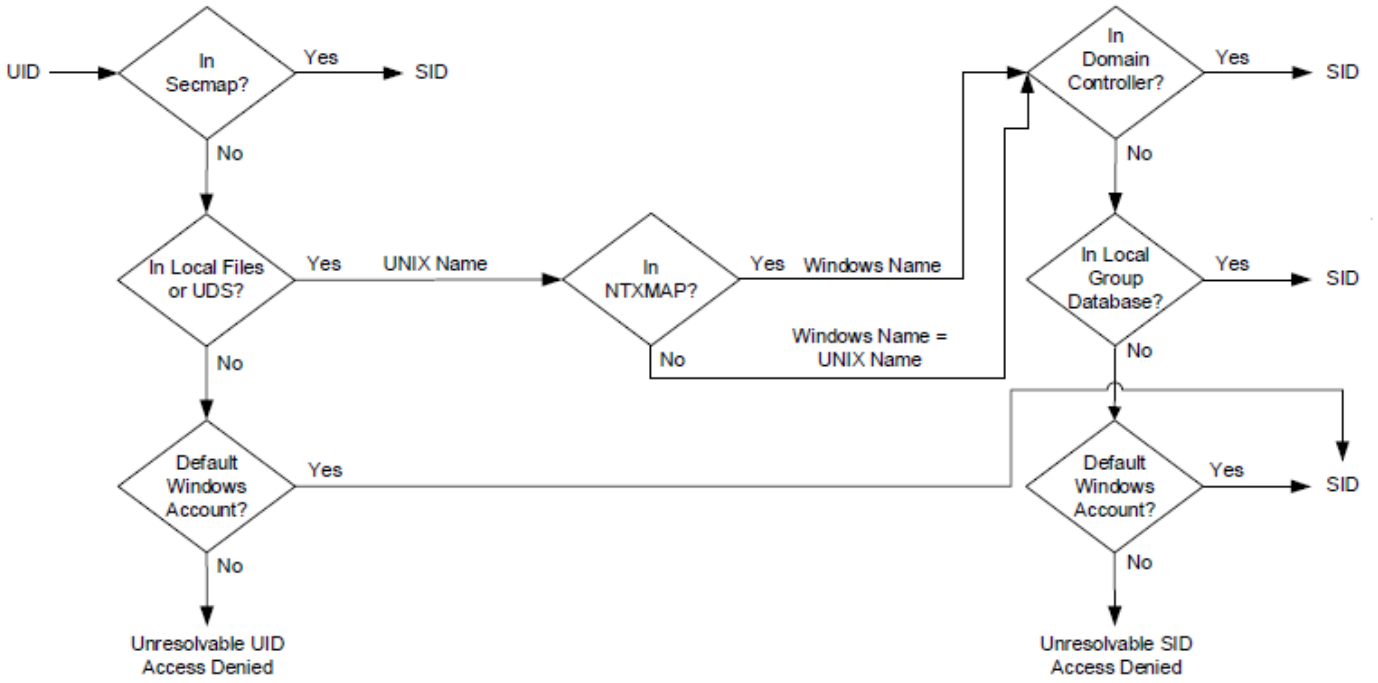

Figure 4. Process for resolving a UID to an SID mapping

Access policies for NFS, SMB, and FTP

In a multiprotocol environment, the storage system uses file system access policies to manage user access control of its file systems. There are two kinds of security, UNIX and Windows.

For UNIX security authentication, the credential is built from the UNIX Directory Services (UDS) except for nonsecure NFS access, where the credentials are provided by the host client. User rights are determined from the mode bits and NFSv4 ACL. The user and group identifiers (UID and GID, respectively) are used for identification. There are no privileges that are associated with UNIX security.

For Windows security authentication, the credentials are built from the Windows domain controller (DC) and Local Group Database (LGDB) of the SMB server. User rights are determined from the SMB ACLs. The Security Identifier (SID) is used for identification. Privileges that are associated with Windows security, such as TakeOwnership, Backup, and Restore, are granted by the LGDB or group policy object (GPO) of the SMB server.

The following table describes the access policies that define what security is used by which protocols:

Table 2. Access policies

Access policy	Description
Native (default)	• Each protocol manages access with its native security. • Security for NFS shares uses the UNIX credential that is associated with the request to check the NFSv3 UNIX mode bits or NFSv4 ACL. The access is then granted or denied. • Security for SMB shares uses the Windows credential that is associated with the request to check the SMB ACL. The access is then granted or denied. • NFSv3 UNIX mode bits and NFSv4 ACL permission changes are synchronized to each other. • There is no synchronization between the UNIX and Windows permissions.
Windows	• Secures file level access for Windows and UNIX using Windows security. • Uses a Windows credential to check the SMB ACL. • An SMB ACL conversion determines permissions for newly created files. SMB ACL permission changes are synchronized to the NFSv3 UNIX mode bits or NFSv4 ACL. • NFSv3 mode bits and NFSv4 ACL permission changes are denied.
UNIX	• Secures file level access for Windows and UNIX using UNIX security.

Table 2. Access policies (continued)

Access policy	Description
	• Upon request for SMB access, the UNIX credential that is built from the local files or UDS is used to check the NFSv3 mode bits or NFSv4 ACL for permissions. • The UMASK determines permissions for newly created files. • NFSv3 UNIX mode bits or NFSv4 ACL permission changes are synchronized to the SMB ACL. • SMB ACL permission changes are allowed in order to avoid causing disruption, but these permissions are not maintained.

For FTP, authentication with Windows or UNIX depends on the username format that is used when authenticating to the NAS server. If Windows authentication is used, FTP access control is similar to that for SMB; otherwise, authentication is similar to authentication for NFS. FTP and SFTP clients are authenticated when they connect to the NAS server. It could be an SMB authentication (when the format of the username is `domain\user` or `user@domain`) or a UNIX authentication (for the other formats of a single username). The Windows DC of the domain that is defined in the NAS server ensures the SMB authentication. The NAS server ensures the UNIX authentication according to the encrypted password stored in either a remote LDAP server, a remote NIS server, or in the local passwd file of the NAS server.

Credentials for file level security

The storage system must build a credential that is associated with the SMB or NFS request being handled to enforce file-level security. There are two kinds of credentials, Windows and UNIX. The NAS server creates UNIX and Windows credentials for the following use cases:

- Building a UNIX credential with more than 16 groups for an NFS request. The extended credential property of the NAS server must be set to provide this ability.
- Building a UNIX credential for an SMB request when the access policy for the file system is UNIX.
- Building a Windows credential for an SMB request.
- Building a Windows credential for an NFS request when the access policy for the file system is Windows.

NOTE: For an NFS request, when the extended credential property is not set, the UNIX credential from the NFS request is used. When using Kerberos authentication for an SMB request, the Windows credential of the domain user is in the Kerberos ticket of the session setup request.

A persistent credential cache is used for the following:

- Windows credentials built for access to a file system having a Windows access policy.
- UNIX credential for access through NFS if the extended credential option is enabled.

There is one cache instance for each NAS server.

Granting access to unmapped users

Multiprotocol requires the following:

- A Windows user must be mapped to a UNIX user.
- A UNIX user must be mapped to a Windows user in order to build the Windows credential when the user is accessing a file system that has a Windows access policy.

Two properties are associated to the NAS server regarding unmapped users:

- The default UNIX user
- The default Windows user

When an unmapped Windows user attempts to connect to a multiprotocol file system and the default UNIX user account is configured for the NAS server, the user identifier (UID) and primary group identifier (GID) of the default UNIX user are used in the Windows credential. Similarly, when an unmapped UNIX user attempts to connect to a multiprotocol file system and the default Windows user account is configured for the NAS server, the Windows credential of the default Windows user is used.

NOTE: If the default UNIX user is not set in the UNIX Directory Services (UDS), SMB access is denied for unmapped users. If the default Windows user is not found in the Windows DC or the LGDB, NFS access on a file system that has a Windows access policy is denied for unmapped users.

NOTE: The default UNIX user can be a valid existing UNIX account name or follow the new format `@uid=xxxx,gid=yyyy@`, where *xxxx* and *yyyy* are the decimal numerical values of the UID and the primary GID, respectively, and can be configured on the system using CLI.

Since the PowerStore file system is UNIX-based, all data that is written must be associated with a valid UID and primary GID. NFS users have a UID and primary GID natively available. However, SMB users must have a mapping that converts their native SID to a UID and primary GID. A reverse mapping from UID to SID is only required if Windows permissions are enforced (Windows access policy).

The automatic mapping feature enables the ability to automatically generate and assign a unique UID to Windows users that do not have a UID mapping. This feature enables access to the share for unmapped users, instead of denying access. Since each user has a unique UID, UID-based features such as user quotas can still properly track the consumption of each individual user.

Automatic mapping is enabled by default on SMB-only and multiprotocol NAS servers. If the feature is enabled, the ability to configure default accounts is disabled. Because the system automatically assigns each UID, use this feature only in environments where the UID of these users is not critical. In environments where administrators want to control UID assignments, disable the feature. If automatic mapping is disabled and there are no other mapping methods available for unmapped users, the unmapped users are denied access to the share.

UNIX credential for NFS requests

A UNIX credential must be used to handle NFS requests for an NFS-only or multiprotocol file system with a UNIX or native access policy. The UNIX credential is always embedded in each request; however, the credential is limited to 16 extra groups.

To enable the Extended Credentials property, select **Storage** > **NAS Servers** > **[NAS server]** > **Sharing Protocols** > **NFS Server** and toggle the **Extended Credentials** option. By enabling UNIX extended credentials, it is possible to build a credential with more than 16 groups. If this option is set, the active UDS is queried with the UID to get the primary GID and all the group GIDs to which it belongs. If the UID is not found in the UDS, the UNIX credential that is embedded in the request is used.

NOTE: For NFS secure access, the credential is always built using the UDS.

UNIX credential for SMB requests

When the session is set up, a Windows credential must be built for the SMB user. Building the credential enables handling SMB requests for a multiprotocol file system with a UNIX access policy. The SID of the Windows user is used to find the name from the AD. That name is then used (optionally using ntxmap) to find a UNIX UID and GID from the UDS or local file (passwd file). The owner UID of the user is a part of the Windows credential. When accessing a file system with a UNIX access policy, the UID of the user is used to query the UDS to build the UNIX credential, similar to building an extended credential for NFS. The UID is required for quota management.

Windows credential for SMB requests

A Windows credential must be used to handle SMB requests for an SMB-only or a multiprotocol file system with a Windows or native access policy. The Windows credential for SMB is built only once at the session setup request time when the user connects.

With Kerberos authentication, the credential of the user is a part of the Kerberos ticket of the session setup request, unlike when using NT LAN Manager (NTLM). Other information is queried from the Windows DC or the LGDB. For Kerberos, the list of extra group SIDs is taken from the Kerberos ticket and the list of extra local group SIDs. The list of privileges are taken from the LGDB. For NTLM, the list of extra group SIDs is taken from the Windows DC and the list of extra local group SIDs. The list of privileges is taken from the LGDB.

The corresponding UID and primary GID are also retrieved from the user-mapping component. Since the primary group SID is not used for access checking, the UNIX primary GID is used instead.

NOTE: NTLM is an older suite of proprietary security protocols that provides authentication, integrity, and confidentiality to users. Kerberos is an open standard protocol that provides faster authentication by using a ticketing system. Kerberos adds greater security than NTLM to systems on a network.

Windows credential for NFS requests

The Windows credential is only built or retrieved when a user, using an NFS request, attempts to access a file system that has a Windows access policy. The UID is extracted from the NFS request. There is a global Windows credential cache to help avoid building the credential on each NFS request with an associated retention time. If the Windows credential is found in this cache, no other action is required. If the Windows credential is not found, the UDS or local file is queried to find the name for the UID. The name is then used (optionally, with ntxmap) to find a Windows user, and the credential is retrieved from the Windows DC or LGDB. If the mapping is not found, the Windows credential of the default Windows user is used instead, or the access is denied.

Multiprotocol file system security settings

PowerStore offers access customization, renaming, and locking policies for a multiprotocol file system.

File system access policies

You can select one of the following access policies for a multiprotocol file system:

- Native Security
- UNIX Security
- Windows Security

For information about these access policies, see Access policies for NFS, SMB, and FTP.

File system renaming policies

You can select one of the following rename policies for a multiprotocol file system. A rename policy controls the circumstances under which NFS and SMB clients can rename a directory. The setting can be one of the following:

Table 3. Rename policies for a multiprotocol file system

Setting	Description
All Allowed	All NFS and SMB clients can rename directories without any restrictions.
SMB Forbidden	Only NFS clients can rename directories without any restrictions. If at least one file is opened in a directory or in one of its subdirectories, an SMB client cannot rename the directory. For example, if the path to a file is C:\Dir1\Dir2\Dir3\File1.txt, and an SMB client opens File1, Dir1, Dir2 , and Dir3 cannot be renamed.
All Forbidden	(Default) If at least one file is opened in a directory or in one of its subdirectories, then NFS and SMB clients cannot rename the directory.

File system locking policies

SMB and NFS have their own locking semantics. Protocol specifications define lock ranges as mandatory for SMB but may be advisory for NFS. NFSv3 uses a separate protocol (NLM) that is always advisory. NFSv4 has a lock management that is integrated in the protocol itself, but may also be advisory or mandatory, depending on the implementation.

A locking policy property is used to define the behavior. You can select one of the following locking policies for a multiprotocol file system:

Table 4. Locking policies for file systems

Setting	Description
Mandatory	This policy uses the SMB and NFSv4 protocols to manage range locks for a file that is in use by another user. If there is concurrent access to the same locked data, a mandatory locking policy prevents data corruption.

Table 4. Locking policies for file systems (continued)

Setting	Description
Advisory	(Default) In response to lock requests, this policy reports that there is a range lock conflict, but does not prevent access to the file. This policy allows NFSv3 applications that are not range-lock compliant to continue working, but risks data corruption if there are concurrent writes.

3

Configure a NAS server for multiprotocol file sharing

This chapter contains the following information:

Topics:

Configuring NAS servers for multiprotocol file sharing

Configuring a multiprotocol NAS server in the UI requires specifying the following information:

- Networking information for the NAS server (IP interfaces, netmask, gateway, VLAN, and so on.)
- The DNS server IP address and DNS domain for contacting AD.
- The credential of an Active Directory (AD) user with privileges for joining AD.
- The UNIX Directory Service (UDS) information. For NIS, this information includes the domain name and the IP address the NIS servers. For LDAP, this information includes the IP address of the LDAP servers, baseDN, and authentication information. For local files, this information includes passwd and group files.

The following table describes the available NAS server configurations for multiprotocol NAS servers:

Table 5. NAS server configurations for multiprotocol NAS servers

Operating Environment	NAS server function	Recommended configuration options
Balanced UNIX and Windows environment; that is, when your system requires a 1:1 mapping of all or most users.	Enable SMB and NFS access to the same file systems data.	1. Do the following in the Create a NAS Server wizard: • On the **Sharing Protocols** tab, select **SMB** along with **NFSv3** and/or **NFSv4**. • Join the NAS server to a Windows AD domain. • Configure a UDS (LDAP or NIS), local files, or both local files and a UDS to manage user identities. • Configure DNS. • Optionally, configure automatic user mapping or default accounts. • Configure UDS search order. 2. Optionally customize the mappings between Windows user accounts and UNIX user accounts by modifying and uploading a user-mapping file with advanced naming rules (ntxmap). You should choose this option when the names of the same users follow different naming rules in Windows and UNIX.
UNIX environment with the ability to access file system data through SMB	Enable NFS access to file system data and optionally enable SMB access to the same file system data for some Windows accounts.	1. Follow the steps in the Balanced UNIX and Windows environment row for creating a NAS server, configuring a UNIX directory service or local files, and optionally customizing the mappings between Windows user accounts and UNIX user accounts.

Table 5. NAS server configurations for multiprotocol NAS servers (continued)

Operating Environment	NAS server function	Recommended configuration options
		2. Optionally, configure a default UNIX user account. All unmapped Windows accounts are mapped to this user account. If you choose to use automatic user mappings, you cannot control what UID each user has, but can use quotas. **NOTE:** If you use a default UNIX account for SMB users, these users are mapped to one UID. Therefore, only one user quota applies to all these users. 3. After you create file systems for the NAS server, It is recommended that you specify a file system access policy of UNIX.
Windows environment with the ability to access file system data through NFS	Enable SMB access to file system data and optionally enable NFS access to the same file system data for some UNIX accounts.	1. Follow the steps in the Balanced UNIX and Windows environment row for creating a NAS server and optionally use ntxmap to customize the mappings between Windows user accounts and UNIX user accounts. 2. Optionally, configure a default Windows user account. All unmapped UNIX accounts are mapped to this user account. **NOTE:** If you use a default Windows account for UNIX users, these users are mapped to one SID. Therefore, only one user quota applies to all these users. 3. After you create file systems for the NAS server, It is recommended to specify a file system access policy of Windows.

Create a NAS server for multiprotocol file sharing (SMB and NFS)

Prerequisites

Obtain the following information:

- Networking information for the NAS server (IP interfaces, netmask, gateway, VLAN, and so on.)
- VLAN ID, if the switch port supports VLAN tagging.
- AD information, including the SMB system name (used to access SMB shares), and either the credentials of the domain administrator or of a user of the domain who has privileges for joining the AD. Optionally, you can specify the NetBIOS name and organizational unit. The NetBIOS name defaults to the first 15 characters of the SMB server name. The organizational unit defaults to CN=Computers.
- UNIX Directory Service (UDS) information for NIS, LDAP, or other local files. The UDS provides the UNIX UID and GID for AD users.

  NOTE: You can configure mappings for some users in the UDS and let the others be mapped through the default account, or use automatic mapping.

- DNS server and domain information.
- Protection policy (optional).

About this task

It is recommended to balance the number of NAS servers on both nodes.

In a multiprotocol configuration, it is recommended to join the SMB server to an Active Directory domain for resolving SIDs to and from Windows usernames. When connecting to a multiprotocol file system, domain users perform user mapping to create a mapping from the Windows SID to the UNIX UID and primary GID.

Standalone SMB servers only support local users (which are intended for SMB-only access and are not mapped), and would not have the necessary mappings for a proper multiprotocol configuration.

Because the UID of the local user on the file system is unlikely to match the UID configured on the UNIX client, the two UIDs are seen as two different users from the point of view of the NAS server. As a result, the same user has inconsistent permissions across different protocols.

You can use one of the following workarounds:

- Manually configure UIDs to ensure that they are consistent with the local SMB server - Create all the local users on an SMB server, determine the UIDs of the local users, and then configure the UNIX clients to use those UIDs.
- If security is not a concern, you can use open permissions.
- If the files are accessible to everyone, then it is not required to maintain consistent permissions across protocols.

Steps

1. Select **Storage** > **NAS Servers**.
2. On the **NAS Servers** tab, click **Create**.
3. On the **Details** page, specify the NAS server name, network interface, IP address, subnet mask, and VLAN ID.
4. Select **Next** to open the **Sharing Protocol** page.
5. On the **Select Sharing Protocol** page, select **SMB** and **NFSv3** and/or **NFSv4**, and select **Next**.
6. On the **Windows Server Settings** tab, in the Windows Server Type field, select **Join to the Active Directory Domain**, and fill the required AD information.
7. Optionally, select **Advanced** to change the default NetBIOS name and organizational unit. Select **Save** and then select **Next**.
8. On the **UNIX Directory Services** tab, configure one of the following directory services:
   - Local files
   - NIS
   - LDAP
   - Local files and NIS or LDAP
9. Optionally, select **Secure NFS** and then switch the **Secure NFS Settings** to enable secure NFS.
10. On the **DNS** page, select **Enable DNS Server** option, and provide the following information:
    - DNS Transport Protocol - UDP (default), TCP
    - Domain
    - IP address of the DNS servers
11. On the **Protection Policy** page, optionally select a protection policy for the NAS server.
12. On the **File QoS Policy** page, optionally select a file QoS policy for the NAS server.
13. Select **Finish** to create the NAS server.

Configure a NAS server UNIX Directory Service

When you configure a NAS server that supports multiprotocol file sharing, you must configure a way to look up identity information, such as UIDs, GIDs, netgroups, and so on.

There are three ways to configure identity lookups:

- Use local files, alone or with a UDS.
- Configure a UNIX Directory Service (UDS) using NIS.
- Configure a UDS using LDAP.

If you are creating a NAS server, use the **Configure UNIX Directory Service** window in the **Create NAS server** wizard to configure identity lookups.

If you are configuring a UDS for an existing NAS server, access the **Naming Services** tab to access the identity lookup options:

1. In the PowerStore Manager, select **Storage** > **NAS Servers**.
2. Click a NAS server to select it.
3. Select the **Naming Services** tab.

To specify the search order for an existing NAS server, select the **User Mapping** tab and configure the search order. The directory services that you configured earlier are selectable in the drop-down menu. Possible options are:

- LDAP
- NIS

- Local Files
- Local then NIS
- Local then LDAP

Using local files

Local password and group files can be used to resolve IDs and usernames. The passwd file uses the same format and syntax as UNIX-based operating systems, so an existing file from a host could also be leveraged for the NAS server.

The relevant items for the NAS server are the username, hashed password (used for FTP authentication), UID, and primary GID. The rest of the items in the passwd file can remain empty.

To troubleshoot issues with configuring local files, ensure that:

- The file is created with the proper syntax (six colons are required for each line). See the template for more details.
- Each user has a unique name and UID.

Enabling local files for a new NAS server

Prerequisites

You can download the current version of the local files from the NAS server, which also provides syntax, examples and additional details. After you edit the file with the user details, upload it back to the NAS server.

About this task

Perform the following steps to enable the use of local files for directory services when you are creating a NAS server:

Steps

1. From the **UNIX Directory Services** window in the **Create NAS Server** wizard, select **Use Local Files**.
2. Create the passwd file for the UDS. To view the template for the passwd file, select **Passwd file template**.
3. To upload the password file to the NAS server, select **Select Passwd File**.

Enabling local files for an existing NAS server

Steps

1. In the PowerStore Manager, select **Storage** > **NAS Servers**.
2. Select the NAS server and then select the **Naming Services** tab.
3. Select the **Local Files** tab.
4. Click the downward arrow of the relevant file to retrieve it, and make the necessary changes.
5. To upload the files, select **Upload Local Files**.
6. Select the file type and click **Select File**.
7. Select the file and then select **Upload**.

Configure a UNIX Directory Service using NIS

You can use NIS for UDS. To configure NIS, you must provide the following information:

- NIS domain
- IP addresses for NIS server

If you provide addresses of multiple NIS servers, they can be moved up or down in the priority list.

Configuring a UDS using NIS for a new NAS server

Steps

1. From the **UNIX Directory Services** window in the **Create NAS Server** wizard, select **Enable a UNIX Directory using NIS or LDAP**.
2. In the **UNIX Directory Services** window select **NIS**.
3. Enter the NIS domain and add up to three IP addresses for the NIS servers.

Configuring a UDS using NIS for an existing NAS server

Steps

1. In the PowerStore Manager, select **Storage** > **NAS Servers**.
2. Select the NAS server and then select the **Naming Services** tab.
3. Select the **UDS** tab.
4. In the **Unix Directory Service** field, select **NIS**.
5. Enter the NIS domain, and add up to three IP addresses for the NIS servers.
6. Select **Apply**.

Configure a UNIX Directory Service using LDAP

LDAP must adhere to the IDMU, RFC2307, or RFC2307bis schemas. Some examples include AD LDAP with IDMU, iPlanet, and OpenLDAP. The LDAP server must be configured properly to provide UIDs for each user. For example, on IDMU, the administrator must go into the properties of each user and add a UID to the UNIX Attributes tab.

To troubleshoot issues with configuring UDS using LDAP, ensure that:

- The LDAP configuration adheres to one of the supported schemas.
- All the containers that are specified in the `ldap.conf` file are for valid and existing containers.
- Each LDAP user is configured with a unique UID.

You can also use the `-ldap` option of the `svc_nas_tools` service command to troubleshoot LDAP issues. This command can display advanced diagnostics for the connection to the LDAP server and can run a username resolution to ensure that the LDAP settings are correct.

Configuring a UDS using LDAP for a new NAS server

Steps

1. From the **UNIX Directory Services** window in the **Create NAS Server** wizard, select **Enable a UNIX Directory using NIS or LDAP**.
2. In the **UNIX Directory Services** window select **LDAP**.
3. Enter the port number.

   NOTE: By default, LDAP uses port 389, and LDAP over SSL (LDAPS) uses port 636.

4. Enter IP addresses (a single address, multiple addresses that are separated by commas, or a range of addresses) and select **Add**.
5. Configure the LDAP authentication as described in LDAP Authentication.
6. Enter the Base DN in X.509 format.
7. For an iPlanet LDAP server, enter the Profile DN (optional).
8. If you want to use secure LDAP, select the option.
9. Select **Confirm**.

Configuring a UDS using LDAP for an existing NAS server

Steps

1. In the PowerStore Manager, select **Storage** > **NAS Servers**.
2. Select the NAS server and then select the **Naming Services** tab.
3. Select the **UDS** tab.
4. In the **Unix Directory Service** field, select **LDAP**.
5. Enter the port number.

   NOTE: By default, LDAP uses port 389, and LDAP over SSL (LDAPS) uses port 636.

6. Enter IP addresses (a single address, multiple addresses that are separated by commas, or a range of addresses) and select **Add**.
7. Configure the LDAP authentication as described in LDAP Authentication.
8. Enter the Base DN in X.509 format.
9. For an iPlanet LDAP server, enter the Profile DN (optional).
10. To upload an LDAP schema, select **Upload New Schema** and then **Select File**.
11. If you want to use secure LDAP, select the option.
12. Select **Confirm**.

LDAP authentication

The following table summarizes the possible LDAP authentication options:

Table 6. LDAP authentication

Option	Considerations
LDAP with Anonymous or Simple authentication	For Anonymous authentication, add the LDAP servers and specify the port number that the LDAP servers use, the Base DN, and the profile DN for the iPlanet/OpenLDAP server. For Simple authentication, add the LDAP servers and specify the following: ● If you are using AD, LDAP/IDMU: ○ The port number used by the LDAP servers ○ User account in LDAP notation format; for example, cn=administrator,cn=users,dc=svt,dc=lab,dc=com ○ User account password ○ Base DN, which is the same as the Fully Qualified Domain Name (for example, svt.lab.com). ● If you are using the iPlanet/OpenLDAP server: ○ User account in LDAP notation format; for example, cn=administrator,cn=users,dc=svt,dc=lab,dc=com ○ Password ○ Base DN. For example, if using svt.lab.com, the Base DN would be DC=svt,DC=lab,DC=com ○ Profile DN for the iPlanet/OpenLDAP server
LDAP with Kerberos authentication	There are two methods for configuring Kerberos: ● Authenticate to the SMB domain. With this option, you can either authenticate using the SMB server account or authenticate with other credentials. ● Configure a custom realm to lead to any type of Kerberos realm (Windows, MIT, Heimdal). With this option, the NAS server uses the custom Kerberos realm that is defined in the Kerberos subsection under the **Security** tab for the NAS server. AD authentication of the SMB server is not used when you choose this option. **NOTE:** If you use NFS secure with a custom realm, you have to upload a keytab file.

Edit OpenLDAP schema for Linux

It may be necessary to change the OpenLDAP schema for Linux when exporting some NFS file systems to netgroups.

When downloading OpenLDAP from the OpenLDAP organization, the LDAP server comes with a schema that complies strictly with RFC 2307:

```
( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )
```

The LDAP server schema can also comply with RFC 2307bis:

```
( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

With PowerStore, both RFC 2307 and RFC 2307bis are supported.

RFC 2307 defines the syntax of the netgroup triple as case-sensitive even though the common usage is that host names in netgroup triples should not be case-sensitive. If you want to match host names with different cases (for example, the host names are uppercase in DNS and lowercase in netgroup triples as defined in the LDAP directory), the LDAP schema must be changed.

Because RFC 2037bis is a draft and the OpenLDAP organization does not recognize it, the OpenLDAP schema for Linux has to be changed to be compatible with PowerStore. Therefore, it is necessary to change the OpenLDAP schema for PowerStore as follows:

In the `/etc/openldap/schema/nis.schema` file on your OpenLDAP server, find the following entry:

```
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Edit the entry to appear as follows (adding the EQUALITY directive):

```
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Upload or view an LDAPS CA certificate for a NAS server

About this task

NOTE: This procedure is required only if you are using LDAPS.

Steps

1. Select **Storage** > **NAS Servers**.
2. Select the NAS server and then select the **Naming Services** tab.
3. Select the **LDAP Secure (Use SSL)** option, and then Select the **Enforce Certification Authority (CA) Certificate** option.

   NOTE: These options are available for Anonymous and Simple authentication.

4. If a CA certificate is already uploaded, select **Retrieve CA Certificate** to view it.
5. Select **Upload CA Certificate**, locate the certificate to upload, and select **Start Upload**.

Change NAS server UNIX credential settings

Steps

1. Select **Storage** > **NAS Servers**.
2. Select the NAS server from the list and then select the **Sharing Protocols** tab.
3. Select the **NFS Server** tab.
4. Make the necessary changes, as described in the following table.

Table 7. NAS server UNIX credential settings

Task	Description
Extend the UNIX credential to enable the storage system to obtain more than 16 group GIDs. **NOTE:** This is required only if you have users with more than 16 GIDs. **NOTE:** With secure NFS, the NAS server always builds the UNIX credential, so this option does not apply.	Enable or disable **Extended Credentials**. • If this option is enabled, the NAS server uses the User ID (UID) to obtain the primary Group ID (GID) and all group GIDs to which it belongs. The NAS server obtains the GIDs from the local password file or UDS. • If this option is disabled, the UNIX credential of the NFS request is directly extracted from the network information that is contained in the frame. This method has better performance, but it is limited to including up to only 16 group GIDs.
Specify a UNIX credential cache retention period. This option can improve performance, because it reuses the UNIX credential from the cache instead of building it for each request.	In the **Credential cache retention** field, enter a time period (in minutes) for which access credentials are retained in the cache. Range is 1 - 35791394, default value is 15 minutes.

Configuring user mappings for multiprotocol NAS servers

A multiprotocol environment requires the following types of user mappings:

- To access a file system configured with a UNIX access policy, a Windows username must map to a corresponding UNIX username. In addition, the storage system must be able to resolve that UNIX username to a UID.
- A UNIX username must map to a corresponding Windows username when using NFS to access a file system configured with a Windows access policy.
- A UNIX user does not have to map to a corresponding Windows user when using NFS to access a file system that is configured with a UNIX or native access policy.

The system automatically creates a mapping between a Windows and a UNIX user when the same username is defined in the UNIX Directory Service (UDS) or local password file, and Windows Active Directory (AD). UNIX usernames are case-sensitive. For example, Windows User1 automatically maps to UNIX User1. If the usernames are different, you can upload a customized user-mapping file (ntxmap) to create custom mapping rules. These rules can be bi-directional, or they can map Windows users to UNIX users or UNIX users to Windows users. The rules support wildcards and substitutions.

To allow users with unmapped usernames to access a file system, you can set automatic user mapping (which enables quotas). Another option is to set default UNIX and default Windows accounts for the NAS server.

Automatic user-mapping process

The automatic user-mapping process maps the UNIX UID to the Windows SID. Mapping is done by matching the username from the UDS or local files to the username from the AD.

Automatic mapping for Windows users

When you modify NAS server sharing protocols, you can optionally direct the system to automatically generate a UNIX UID for each Windows user that is not already mapped to a UNIX account through a directory service (LDAP or NIS) or local files.

NOTE: Use automatic mapping only when it is not important which UID is assigned to which user.

This option is available when a default UNIX user is not configured, and it is intended for multiprotocol configurations where most users are Windows users. Using this option allows for the retention of file system quotas for each unmapped Windows user (file system quotas are based on the UNIX UID). The automatically generated UNIX UIDs are in the reserved range of 0x80000001 to 0x803FFFFF.

NOTE: If a default UNIX user is configured, you cannot enable automatic mapping for Windows users.

Default usernames

When you modify the NAS server sharing protocols, you can optionally configure default user accounts for a NAS server:

- The default UNIX user account specifies the UNIX account to use for file system access from an unmapped Windows account. If you do not specify a default UNIX account, unmapped Windows users are unable to access the system. The default UNIX user can be a valid existing UNIX account name or follow the format `@uid=xxxx, gid=yyyy@`, where xxxx and yyyy are the decimal numerical values of the UID and the primary GID, respectively. When you configure a default UNIX user, consider the following:
  - If you use a default UNIX account for Windows users, these users are mapped to one UID. Therefore, only one user quota applies to all the users.
  - Setting the default user to a UID of zero or to a user that is resolved to a zero UID grants full root access to that user, which can be dangerous from a security point of view.
- If the file system access policy is Windows, the default Windows account specifies the Windows account to use for file system access from an unmapped UNIX account. For Windows security authorization, the credential is built from the Windows domain controller (DC) and Local Group Database (LGDB) of the SMB server. If you do not specify a default Windows account and if the default Windows user is not found in the Windows DC or the LGDB, an unmapped UNIX user is unable to access a file system that has a Windows access policy. The default Windows user account must be an existing user account in the AD in which the SMB server of the NAS server is joined. It is case insensitive.

Customizing the user-mapping file

After you create a NAS server, you can optionally use a customized user-mapping file (ntxmap) to map one or more Windows user accounts to one or more UNIX user accounts, or one or more UNIX user accounts to one or more Windows user accounts (both directions are valid). Customizing the user-mapping file allows you to provide file system access when:

- A Windows user account does not have a corresponding UNIX user account.
- The file system access policy is Windows, and a UNIX user account does not have a corresponding Windows user account.
- A Windows user account and a UNIX user account exist, but use different naming rules. UNIX user accounts are case-sensitive.

The user-mapping file supports the use of wildcards and substitution sequences.

To use a customized user-mapping file, select **Storage** > **NAS Servers** > **[NAS server]** > **Naming Services** > **Local Files** and download the Ntxmap file template. After downloading, customize the file, and upload it to the system.

NOTE: The syntax for the mapping file is displayed in the file template.

Change NAS server user mappings

About this task

You can change the user mappings for multiprotocol NAS servers.

Steps

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

2. Select the NAS server and then select the **Naming Services** tab.
3. Make the necessary changes as described in the following table:

Table 8. NAS server user mappings

Task	Description
Map together UNIX accounts and Windows accounts that have different usernames.	The ntxmap configuration file lets you map together UNIX accounts and Windows accounts that have different usernames. The syntax for ntxmap is displayed in the template that you retrieve by following these steps: a. Select **Local Files**. b. On the local files list, select the download icon next to Ntxmap to retrieve it. **NOTE:** If there is no custom mapping file, the NAS server retrieves a template for configuration. c. Use a text editor to add or change user account mappings in the file. d. Select **Upload Local Files** and then select **ntxmap** from the File Type options. e. Use the browser to select the updated file and select **Upload**.
Automatically generate a UNIX UID for each Windows user that is not mapped to a UNIX account.	a. Select **User Mapping**. b. Select **Enable automatic mappping for unmapped Windows accounts/users**. This option is for multiprotocol environments in which most users are Windows users. When you select this option, the system generates UNIX UIDs for Windows users that are not already mapped to UNIX accounts through a directory service (LDAP or NIS) or local files. This functionality allows for the retention of file system quotas for unmapped Windows users.
Enable or disable default accounts for unmapped users.	a. Select **User Mapping**. b. Select or clear the **Enable default account for unmapped users** option. c. If you enabled this option, set the default UNIX user (name or UID/GID) and the default Windows username. If you enable default accounts for unmapped users, you can enter default UNIX and Windows accounts that the system uses to grant file system access to unmapped users. The default UNIX user can be a valid existing UNIX account name or follow the format `@uid=xxxx,gid=yyyy@`, where xxxx and yyyy are the decimal numerical values of the UID and the primary GID, respectively. **NOTE:** If you are using default accounts, the users are mapped to one UID, and only one user quota applies to all users.

4

Configure a file system for multiprotocol file sharing

This chapter contains the following information:

Topics:

Create a file system

Prerequisites

- A NAS server configured to support SMB and NFS protocols

Steps

1. Select **Storage** > **File Systems**.
2. Select **Create** to open the **Create File System** wizard.
3. Configure the file system according to the wizard steps:

Option	Description
Select Type	Select the **General** file system type.
Select NAS Server.	Select a NAS server that is enabled for SMB and NFS. Optionally you can set Advanced SMB Settings. For details, see File system advanced settings for SMB.
File System Details	Provide the file system name, description (optional), and size. 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. The displayed capacity reflects the metadata space that is reserved from the usable file system capacity.
File-Level Retention	Select a file-level retention type: • Off - No file-level retention is set. • Enterprise (FLR-E) - Protects content from changes that users make through SMB, NFS, 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-level 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. Value is unlimited. • Maximum - Specifies the longest period for which files can be locked. Value is unlimited.

Option	Description
NFS Export (Optional)	Configure a name and description of the initial export for the file system. You can add the exports to the file system after the initial file system configuration.
Configure Access	Add hosts.

SMB Share (Optional)	Configure the initial SMB Share:
	NOTE: You can add shares to the file system after the initial file system configuration.
	• Name
	• Description (optional)
	• Offline availability - Sets the client-side caching of offline files:
	  ○ None - Client-side caching of offline files is not configured.
	  ○ Manual - Files are cached and available offline only when caching is explicitly requested.
	  ○ Programs - Executable files that have been previously cached locally are run from the cached copy instead of the copy on the share.
	  ○ Documents - When a user accesses a file or program from a share, the content is automatically cached to be available offline. Cached content is continuously synchronized with the version on the server.
	Optionally, configure advanced SMB settings for SMB shares. For details, see Advanced SMB share properties.
	• **Continous Availability**
	• **Protocol Encryption**
	• **Access-Based Enumeration**
	• **Branch Cache Enabled**

Protection Policy (Optional)	Provide a protection policy for the file system. PowerStore supports both snapshots and replication for file storage protection.
File QoS Policy (Optional)	Provide a 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. If necessary, go back to make changes.

4. Click **Create File System**.
   The file system is displayed in the File System list. If you created an NFS Export or an SMB Share, they are displayed in the respective lists.

File system advanced settings for SMB

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

Table 9. 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. The synchronous writes 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.

Table 9. File system advanced settings for SMB (continued)

Setting	Description
Oplocks Enabled	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.
Enable Notify on Access Enabled	Enable notification when a file system is accessed. This option is disabled by default.

5

Configure shares

This chapter contains the following information:

Topics:

Share and export local paths and export paths

The following table describes the path settings for shares and exports:

Table 10. Path settings for shares and exports

Setting	Description
Local path	A local path is the path to the file system storage resource on the storage system. This path specifies the unique location of the share or export on the storage system. ● SMB shares ○ In an SMB file system, you can create multiple shares with the same local path. In these cases, you can specify different host-side access controls for different users, but the shares within the file system all access 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. ● NFS exports ○ Each NFS export must have a unique local path. PowerStore automatically assigns this path to the initial share created within a new file system. The local path name is based on the file system name. ○ Before you can create additional shares within an NFS file system, you must create a directory to share from a Linux/UNIX host that is connected to the file system. Then, you can create an export from PowerStore and set access permissions accordingly.
Export path	The path used by the host to connect to the share or export. PowerStore creates the export path based on the name of the share or export and the name of the file system where it resides. Hosts use either the export name or the export path to mount or map to the share or export from the network host. This behavior is enabled by using NFS aliases for shares.

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 Shares**.
2. Click **Create** and complete the steps of the **Create SMB Share** wizard.

Page	Description
Select File System	Select a file system that has been enabled for SMB.
Select Snapshot (Optional)	Select one of the file system snapshots on which to create the share.
SMB Share Details	Enter a name, description, 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 displays the SMB Share path, which the host uses to connect to the share. The share path is the IP address or the name of the NAS server, and the name of the share. Hosts use the share path to mount or map to the share from a network host.
Advanced SMB Share Settings	Enable one or more of the advanced SMB share settings: ● Continuous Availability ● Protocol Encryption ● Access-based Enumeration ● Branch Cache Enabled ● Offline Availability (default - None) ● Umask (default - 022)

Next steps

When 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 11. 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)

Table 11. Advanced SMB Properties (continued)

Option	Description
	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.
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.
Distributed File System (DFS)	(Read only) Lets you group files that are on different shares by transparently connecting them to one or more DFS namespaces. This simplifies the process of moving data from one share to another. This option is read-only in Unisphere because you manage DFS from Microsoft hosts. For information, see the Microsoft Distributed File System documentation.
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.
UMASK	(Applies to SMB shares of a file system that supports multiprotocol access with a UNIX access policy or a Native access policy.) A Bitmask that shows which UNIX permissions are excluded for files that are created on the share. The default permissions are: • 666 for files, which allow read and write permissions for all. • 777 for directories, which allow read, write, and execute permissions for all. If UMASK is set to 022, following permissions are granted: • 644 for files, which allow read and write permissions for the file owner, and read permission for everyone else. • 755 for directories, which allow read, write and execute permissions for directory owners, and read and execute permissions for everyone else. **NOTE:** If NFSv4 ACL inheritance is present, it takes precedence over the UMASK setting, • To change the excluded permissions, click **Modify**, and then select or clear permissions. • To set the bitmask to the default value (022), click **Set default**. A value of 022 allows only you to write data, but lets anyone read data. For more information, see the UNIX documentation.

Create an NFS export

You can create an NFS export on a file system.

Steps

1. Select the **Storage** > **File Systems** > **NFS Export** tab.
2. Click **Create**.
   The **Create NFS Export** wizard launches.

3. Enter the requested information while noting the following:
   - If you want to create an export based on a snapshot, then the snapshots must be created before creating the NFS export.
   - **Local Path** must correspond to an existing folder name within the file system that was created from the host-side.
   - The value specified in the **NFS Export Details**, **Name** field, along with the NAS server IP, constitutes the export path.

     NOTE: You can also mount the export using the NAS server IP and local path.

   - NFS export names must be unique at the NAS server level per protocol. However, you can specify the same name for an SMB share, and NFS exports.
4. Once you approve the settings, click **Create NFS Export**.
   The NFS Export displays on the **NFS Export** page.

6

Enable multiprotocol file sharing on an existing NAS server

This chapter contains the following information:

Topics:

Enable multiprotocol file sharing on an existing NFS-enabled NAS server

About this task

When you configure multiprotocol, all existing file systems are enabled with the native security access policy.

Steps

1. Select **Storage** > **NAS Servers**.
2. Select the relevant NAS server and then select the **Naming Services** tab.
3. Configure one of the following directory services if no UNIX Directory Service (UDS) is already configured for the NAS server or if local files are not configured:
   - NIS
   - LDAP
   - Local files
   - Local files and NIS or LDAP

   You can configure LDAP to use anonymous, simple, and Kerberos authentication. You can also configure LDAP with SSL (LDAP Secure) and can enforce the use of a Certificate Authority certificate for authentication.
4. Select the **User Mapping** tab and configure the search order. The directory services that you configured earlier are selectable in the drop-down menu.
5. Select the **User Mapping** tab and enable automatic mapping or default account for unmapped users. If you selected to enable default account, specify default Windows and UNIX accounts. You can also use **`ntxmap`** (located in the **Local files** tab) to map Windows and UNIX users.
6. Select the **Sharing Protocols** page, and then select **SMB Server**.
7. On the **SMB Server** tab, perform the following:
   - Enable the SMB server.
   - Join the NAS server to the Active Directory (AD) domain.
   - Optionally, Select **Advanced** to specify the NetBIOS name and organizational unit. The NetBIOS name defaults to the first 15 characters of the SMB server name. The organizational unit defaults to CN=Computers.

Enable multiprotocol file sharing on an existing SMB-enabled NAS server

About this task

The following considerations apply to enabling multiprotocol file sharing on an existing SMB-enabled NAS server:

- When you configure multiprotocol, all existing file systems are enabled with the native security access policy. With this policy, Windows security is used for both NFS and SMB access to the files. This policy uses a Native Windows credential for all protocols and enforces only the SMB ACL for all protocols. Also, the system automatically updates the ownership of all files with UNIX UID information. The update process can take time, but data remains accessible. If required, you can change this access policy.
- Clients with incorrect mappings receive an Access denied message until the mapping configuration is correct.

Steps

1. Select **Storage** > **NAS Servers**.
2. Select the relevant NAS server and then select the **Naming Services** tab.
3. Configure one of the following directory services:
   - NIS
   - LDAP
   - Local files
   - Local files and NIS or LDAP

   You can configure LDAP to use anonymous, simple, and Kerberos authentication. You can also configure LDAP with SSL (LDAP Secure) and can enforce the use of a Certificate Authority certificate for authentication.
4. Select the **User Mapping** tab and configure the search order. The directory services that you configured earlier are selectable in the drop-down menu.
5. In the **User Mapping** tab, set the mapping mode for unmapped users. If you want automatic UID assignments, enable the **Enable automatic mapping for unmapped Windows accounts/users**. Another option is to enable **Enable default account for unmapped users**, in which case specify default Windows and Unix accounts.

7

Configure distributed file system and widelinks

This chapter contains the following information:

Topics:

About distributed file system

Microsoft Distributed File System (DFS) allows you to group file systems (shared folders) that reside on different servers into a logical DFS namespace. A DFS namespace is a virtual view of these file systems that is shown in a directory tree structure. By using DFS, you can group file systems into a logical DFS namespace and make folders that are distributed across multiple servers appear to users as if they reside in one place on the network. Users can navigate through the namespace without having to know server names or the file systems hosting the data.

Each DFS tree structure has a root target, which is the host server running the DFS service and hosting the namespace. A DFS root contains DFS links that lead to the file systems (a share and any directory below it on the network). The file systems are seen as DFS targets. Microsoft offers stand-alone and domain-based DFS root servers. The domain-based DFS server stores the DFS hierarchy in the AD. The stand-alone DFS root server stores the DFS hierarchy locally. PowerStore provides the same functionality as a Windows 2000 or Windows Server 2003 stand-alone DFS root server.

Configuring DFS roots

You can configure Distributed Filesystem Support (DFS) roots on an SMB share in PowerStore. Complete the following tasks before configuring a DFS root on an SMB share:

1. Configure a NAS server that supports SMB.
2. On the newly created NAS server, configure a file system on which to create the DFS root.

> **NOTE:** Do not establish a DFS root on a file system object with an access-checking policy of UNIX, because none of the DFS link components are created with UNIX rights.

There are two ways to create a DFS root on an SMB share:

- Create a DFS root using dfsutil.exe.
- Create a stand-alone DFS root using DFS MMC.

For more information about configuring DFS, see the Microsoft documentation.

About widelinks

Widelinks make traditional UNIX symbolic links in user file systems useful to SMB clients. When an NFS client encounters a symbolic link in a file system, it resolves the target of the link itself. The challenge is that while the target path of the symbolic link is meaningful to NFS clients, it is most likely of no use to SMB clients. This challenge is addressed by configuring a Microsoft Windows Local DFS root on the NAS server that hosts the user file systems, which include UNIX symbolic links that must be translated for SMB clients. Entries are added to the DFS root so that the NAS server can translate the UNIX paths.

For example, assume that widelink1 looks as follows to an NFS client:

```
$ ls -l widelink1
lrwxr-xr-x 1 cstacey ENG\Domain Users 30 23 JUS 17:33
widelink1 -> /net/nfsserver42/export1/target1
```

$ ls -l widelink1

Then the entry in the DFS root should be:

```
net/nfsserver42/export1/target1 ->
\\nfsserver42\<share-name>\<path-to-target1>
```

8

Troubleshooting a multiprotocol configuration

This chapter contains the following information:

Topics:

Service commands for troubleshooting a multiprotocol configuration

The following service commands are useful for troubleshooting access issues in a multiprotocol configuration. For detailed information about the service commands, see the *Service Commands Technical Notes*.

Table 12. Service commands for troubleshooting a multiprotocol configuration

Use case	Service command
Obtain information about network connectivity to domain controllers, access rights, credentials, access logs, and so forth.	`svc_nas_cifssupport --server <NAS_Server_Name>`
Audit the current connection between the SMB client and domain controller.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-builtinclient"`
Run an internal test to help find the root cause of potential configuration or environmental errors.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-checkup"`
Troubleshoot user access control by listing user credentials as seen from the SMB server cache.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-cred"`
Obtain information about the global policy objects that are applied to the SMB server.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-gpo"`
Enable a log of user or machine log-in attempts.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-logontrace"`
Check the authentication of a given user to an SMB server.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-lsarpc"`
Test the network log-in to an SMB server.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-nltest"`
Display domain controller information for a given SMB server.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-pdcdump"`
Attempt to connect to the SMB domain controller from a given SMB server.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-pingdc"`
Obtain the group membership of a given user from the SMB domain controller.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-samr"`
Access the Secure Mapping database, which acts as a cache mechanism to relate Windows SIDs to UNIX UIDs.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-secmap"`