Dell EMC PowerStore

Security Configuration Guide

Version 2.x

June 2021
Rev. A06

Notes, cautions, and warnings

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

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

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

Contents

Additional Resources....................5

Chapter 1: Authentication and access....................6

Hardware root of trust....................6

Authenticating and Managing User Accounts, Roles, and Privileges....................6

Factory default management....................7

Session rules....................7

Username and password usage....................7

ESXi passwords....................8

Roles and privileges....................8

User account management based on role privileges....................12

Reset admin and service account passwords....................12

Certificates....................14

Viewing certificates....................14

Secure communication between PowerStore appliances within a cluster....................15

Secure communication for replication and data import....................15

vSphere Storage API for Storage Awareness support....................15

CHAP authentication....................17

Configuring CHAP....................17

External SSH access....................18

Configuring external SSH access....................18

SSH sessions....................18

Service account password....................19

SSH authorization....................19

Appliance service scripts....................19

Appliance node Ethernet service port and IPMItool....................19

NFS secure....................19

Security on file system objects....................21

File systems access in a multiprotocol environment....................21

User mapping....................21

Access policies for NFS, SMB, and FTP....................24

Credentials for file level security....................25

Understanding Common AntiVirus Agent (CAVA)....................26

Code signing....................27

Chapter 2: Communication security settings....................28

Port Usage....................28

Appliance network ports....................28

Appliance network ports related to file....................30

Network ports related to PowerStore X model appliances....................33

Transport Layer Security....................34

Configuring Transport Layer Security....................35

Chapter 3: Auditing....................36

Auditing....36
Remote logging....36
Add Remote Syslog Server....37
Import a certificate for remote logging....38
Generate a Certificate Signing Request....38
Manage remote logging settings....39

Chapter 4: Data security settings....40
Data at Rest Encryption....40
Encryption activation....40
Encryption status....40
Key management....41
Keystore backup file....41
Repurpose a drive in an appliance with encryption enabled....42
Replacing a base enclosure and nodes from a system with encryption enabled....42
Resetting an appliance to factory settings....42

Chapter 5: Secure serviceability settings.... 43
Operational description of SupportAssist....43
SupportAssist and security....43
SupportAssist management....43
SupportAssist communication....44
SupportAssist remote support....44
SupportAssist options....44
SupportAssist Connect via Gateway option....45
SupportAssist Connect Directly option....45
Requirements for SupportAssist Connect via Gateway....45
Requirements for SupportAssist Connect Directly....46
Configuring SupportAssist....46
Configure SupportAssist....46
CloudIQ....47
Cybersecurity....47

Chapter 6: Security Alert Settings.... 48
Alert settings....48
Configure email notifications....49
Configure SNMP....49

Appendix A: TLS cipher suites....51
Supported TLS cipher suites....51

Appendix B: Directory Services.... 52
Configuring Directory Services....52
Configure LDAP server....52
Verify LDAP configuration....54
Configure Secure LDAP....55
Verify LDAPS configuration....56
Configure LDAP account....56

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

Authentication and access

This chapter contains the following information:

Topics:

- Hardware root of trust
- Authenticating and Managing User Accounts, Roles, and Privileges
- Certificates
- Secure communication between PowerStore appliances within a cluster
- Secure communication for replication and data import
- vSphere Storage API for Storage Awareness support
- CHAP authentication
- Configuring CHAP
- External SSH access
- Configuring external SSH access
- NFS secure
- Security on file system objects
- File systems access in a multiprotocol environment
- Understanding Common AntiVirus Agent (CAVA)
- Code signing

Hardware root of trust

The PowerStore hardware provides the following security features for firmware images and the operating system through the Secure Boot and x86 Secure Boot technologies that are provided through the enclosure management software on the system:

- Authentication and root of trust provides the capability to authenticate boot loader and firmware, and immutable hardware root of trust.
- Ensure a verified and measured boot.
- Authenticate firmware images and operating system boot loader at boot time.
- Digitally signed firmware upgrades ensure that root of trust authenticates all signed upgrade firmware images.

Authenticating and Managing User Accounts, Roles, and Privileges

Authentication for access to the cluster is performed based on the credentials of a user (local or LDAP) account. User accounts are created and subsequently managed from the **Users** page, which is accessible in PowerStore Manager through **Settings** > **Users** > **Users**. The authorizations that apply depend on the role associated with the user account. When the user specifies the network address of the cluster as the URL in a web browser, the user will be presented with a login page from which the user can authenticate as either a local user or through an LDAP directory server. The credentials that the user provides will be authenticated and a session will be created on the system. Subsequently, the user can monitor and manage the cluster within the capabilities of the role assigned to the user. The cluster authenticates its users by validating user names and passwords through a secure connection with the management server.

NOTE: When users attempt to perform an action in PowerStore Manager for which they are not authorized, a notification appears stating that the action is not authorized.

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory services running on TCP/IP networks. LDAP provides central management of authentication and identity and group information used for authorization on the cluster. Integrating the system into an existing LDAP environment provides a way to control user and user group access to the system through PowerStore Manager, RESTful API or CLI.

After you configure LDAP settings for the system, you can manage users and user groups, within the context of an established LDAP directory structure. For instance, you can assign access roles (Administrator, Storage Administrator, Security Administrator, Operator, VM administrator) to the LDAP user or groups. The role applied will determine the level of authorization the user or group will have in administering the storage system. The system uses the LDAP settings only for facilitating control of access to PowerStore Manager, RESTful API or CLI, not for access to storage resources.

Factory default management

Your appliance comes with factory default user account settings to use when initially accessing and configuring the appliance. During initial configuration, the default passwords must be changed so that the system can become fully operational. The password change is set before the cluster is created.

ⓘ **NOTE:** With releases 1.0.x, it is recommended that you initially configure PowerStore using PowerStore Manager rather than using the API, CLI, or Service Scripts interfaces. It ensures that all the default passwords are changed. With releases 2.x, the default passwords must be changed during initial configuration, however, the API, CLI, or Service Scripts interfaces can be used as well as PowerStore Manager.

Table 1. Factory default user account settings

Account type	Username	Password	Privileges
System management	`admin`	`Password123#`	Administrator privileges used to reset default passwords, configuring appliance settings, and managing user accounts.
Service	`service`	`service`	Used to perform service operations. ⓘ **NOTE:** The service user exists for secure shell (SSH) access. However, you cannot log in to PowerStore Manager using the service user.

Session rules

Sessions on the cluster have the following characteristics:

- Expiration term of one hour.

  ⓘ **NOTE:** User is automatically logged off the cluster after session inactivity of one hour.
- The session timeout is not configurable.

Username and password usage

ⓘ **NOTE:** The appliance does not manage LDAP user passwords. LDAP user password management can only be done by the LDAP directory server.

System account usernames must meet the following requirements:

Restriction	Username requirement
Structure	Must start and end with an alphanumeric character.
Case	All usernames are case-insensitive
Minimum number of alphanumeric characters	1
Maximum number of alphanumeric characters	64
Supported special characters	. (dot)

System account passwords must meet the following requirements:

Restriction	Password requirement
Minimum number of characters	8
Minimum number of uppercase characters	1
Minimum number of lowercase characters	1
Minimum number of numeric characters	1
Minimum number of special characters - Supported characters: ! @ # $ % ^ * _ ~ ? **NOTE:** The password cannot include single quote ('), ampersand (&), or space characters.	1
Maximum number of characters	40

NOTE: The last five passwords are blocked from being reused. A previous password can be reused after the fifth time in sequence.

ESXi passwords

The default root password for ESXi on a PowerStore X model appliance is in the following format: ***<Service_Tag>_123!***, where *<Service_Tag>* is the seven-character Dell Service Tag for the appliance.

Do not change the default ESXi password until the initial cluster configuration is complete. For more information about changing an ESXi password, see the VMware ESXi documentation.

CAUTION: It is critical that you do not lose the ESXi password. If ESXi goes down and you do not have the password, the appliance must be reinitialized. This behavior is normal for ESXi, however reinitializing due to a lost password can result in data loss.

CAUTION: The default ESXi password is uniquely configured for each PowerStore X model appliance. The password is used to authenticate with the ESXi host when the nodes in the appliance are added to a vCenter cluster. If you change the default password before the cluster is fully configured, you will have to reinitialize the appliance.

Roles and privileges

Role-based access controls allow for users to have different privileges. This provides a means to segregate administration roles to better align with skill sets and responsibilities.

The following table lists the roles and privileges related to block that the system supports:

NOTE: A ✓ in a box denotes a supported privilege for that role while a blank box denotes the privilege is not supported for that role.

Table 2. Roles and privileges related to block

Task	Operator	VM Administrator	Security Administrator	Storage Administrator	Administrator	Storage Operator
Change your system local password	✓	✓	✓	✓	✓	✓
View system settings, status, and performance information	✓		✓	✓	✓	✓
Modify system settings					✓	
Create, modify, delete protection policies				✓	✓	

Table 2. Roles and privileges related to block (continued)

Task	Operator	VM Administrator	Security Administrator	Storage Administrator	Administrator	Storage Operator
Enable/disable SSH				✓	✓	
Create, modify, delete volumes, and attach, detach, snapshot, restore, refresh, clone				✓	✓	✓
Create, modify, delete volume groups, add and remove members, snapshot, restore, refresh, clone				✓	✓	✓
Create, modify, delete vVols					✓	
Create, modify, delete storage containers, and mount, unmount, and create directory				✓	✓	
Create, modify, delete vCenter				✓	✓	✓
View a list of local accounts			✓		✓	
Add, delete, or modify a local account			✓		✓	
View system storage information through a vCenter server that is connected to the VASA provider	✓		✓	✓	✓	✓
View and modify metro node application IP address				✓	✓	✓

Roles and privileges related to file

The following table lists the roles and privileges related to file that the system supports:

NOTE: A ✓ in a box denotes a supported privilege for that role while a blank box denotes the privilege is not supported for that role.

Table 3. Roles and privileges related to file

Task	Operator	VM Administrator	Security Administrator	Storage Administrator	Administrator	Storage Operator
View the following: ● File system alerts ● NAS server list ● File system list ● File user quota list ● File interface route list ● File interface list ● SMB share list ● NFS export list	✓		✓	✓	✓	✓

Table 3. Roles and privileges related to file (continued)

Task	Operator	VM Administrator	Security Administrator	Storage Administrator	Administrator	Storage Operator
View the following: ● List of file DNS servers or a specified DNS server ● List of file FTP servers or a specified FTP server ● List of file interfaces or specified file interface ● List of file interface routes or a specified interface route ● List of file Kerberos servers or a specified Kerberos server ● List of file LDAP servers or a specified LDAP server ● List of file NDMP servers or a specified NDMP server ● List of file NIS servers or a specified NIS server ● List of file systems or a specified file system ● List of file tree quotas or a specified file tree quota ● List of file user quotas or a specified user quota ● List of file virus checkers or a specified file virus checker ● List of NAS servers or a specified NAS server ● List of NFS exports or a specified NFS export ● List of NFS servers or a specified NFS server ● List of SMB servers or a specified SMB server ● List of SMB shares or a specified SMB share	✓		✓	✓	✓	✓
Add, modify, delete, or ping, a specified NAS server, or upload password, hosts, or groups to a specified NAS server				✓	✓	
View password of a specified NAS server			✓	✓	✓	✓
View hosts of a specified NAS server	✓		✓	✓	✓	✓

Table 3. Roles and privileges related to file (continued)

Task	Operator	VM Administrator	Security Administrator	Storage Administrator	Administrator	Storage Operator
Add a file system, or modify or delete a specified file system on an existing NAS server				✓	✓	✓
Add a clone or snapshot to a specified file system, or refresh or restore a specified file system, or refresh the quota of a specified file system				✓	✓	✓
Add a file tree quota, or modify, delete, or refresh a specified file tree quota				✓	✓	✓
Add a file user quota, or modify, delete, or refresh a specified file user quota				✓	✓	✓
Add a file virus checker, or modify or delete a specified file virus checker, or upload a specified file virus checker configuration				✓	✓	
Download a specified file virus checker configuration	✓		✓	✓	✓	
Add an SMB or NFS server, or modify, delete, join or unjoin a specified SMB or NFS server				✓	✓	
Add an SMB share, or modify or delete a specified SMB share				✓	✓	✓
Add an NFS export, or modify or delete a specified NFS export				✓	✓	✓
Add a file interface, or modify or delete a specified file interface				✓	✓	
Add a file interface route, or modify or delete a specified file interface route				✓	✓	
Add a file DNS, file FTP, file Kerberos, file LDAP, file NDMP, or file NIS server, or modify or delete a specified file DNS, file FTP, file Kerberos, file LDAP, file NDMP, or file NIS server				✓	✓	
Upload a file Kerberos keytab				✓	✓	
Download a file Kerberos keytab			✓		✓	

Table 3. Roles and privileges related to file (continued)

Task	Operator	VM Administrator	Security Administrator	Storage Administrator	Administrator	Storage Operator
Upload a file LDAP configuration or LDAP certificate				✓	✓	
Download of a file LDAP certificate	✓		✓	✓	✓	

User account management based on role privileges

A user with either an Administrator or Security Administrator role can do the following with regards to user account management:

- Create a new user account.
- Delete any user account except the built-in Administrator account.

  NOTE: The built-in Administrator account cannot be deleted.
- Change another user to any role.
- Reset another user's password.
- Lock or unlock another user account.

  NOTE: Logged-in users with either an Administrator or Security Administrator role cannot lock their own account.

Logged-in users cannot delete their own user account. Also, with the exception of users with either the Security Administrator or Administrator role, Logged-in users can only change their own password. Users must provide their old password to change their password. Logged-in users cannot reset their own password, change their own role, or lock or unlock their own accounts.

The built-in Administrator account profile (with Administrator role) cannot be edited and cannot be locked.

When either a user's role or lock status is changed, the user is deleted, or its password is changed by a Security Administrator or an Administrator, all sessions tied to that user are invalidated.

NOTE: If a users update their own passwords in-session, the session remains alive.

Reset admin and service account passwords

The appliance ships with a default admin user account that lets you perform the initial configuration. It also ships with a default service user account that lets you perform specialized service functions. It is recommended that you initially configure PowerStore using the PowerStore Manager UI rather than another method such as the REST API or the CLI. Using the PowerStore Manager UI ensures that all the default passwords are changed. If you forget the new passwords, you can reset the passwords back to their default values.

The method to reset these passwords depends on whether your appliance is a PowerStore T model or a PowerStore X model. Use the method that corresponds to your appliance to reset the admin or service, or both passwords.

Reset admin and service account passwords to their default values in a PowerStore T model appliance

About this task

For a PowerStore T model appliance, the primary method to reset the admin or service user passwords is to use a USB drive. Supported file systems include FAT32 and ISO 9660.

NOTE: To reset the password if both nodes on the appliance are in Service Mode, use the following steps with one difference. Apply the USB reset process to each node. This action ensures that when the system is returned to Normal Mode and upon PowerStore Manager login, you are prompted to provide a new password for both the admin and service users.

Steps

1. If the USB drive is formatted, go to the next step; otherwise, use a command prompt such as: `format <d:> /FS:FAT32` to format the drive.

   Where `d:` is the drive letter for the USB drive you have inserted into your laptop or PC.

2. Set the label with the command:

   ```
   label d:
   RSTPWD
   ```

   NOTE: The appliance will not mount the USB drive without the `RSTPWD` label. After labeling the USB drive, insert an empty file for the account passwords that you would like to reset. You can reset the admin or service account password, or both.

3. To create an empty file on the drive, use one or both of the following commands as needed:

   ```
   copy NUL d:\admin
   copy NUL d:\service
   ```

4. Insert the USB drive into the USB port of either node of the appliance, wait 10 seconds, and then remove it.
   The password for each account you reset is now the default value.
5. Connect to the cluster through a browser using the cluster IP address and log in as admin with the default initial password, which is **`Password123#`**.
   A prompt to reset the admin or service passwords, or both should appear. If you prefer to reset the service password using secure shell (SSH), the initial default password for the service account is **`service`**.
6. Change the admin password from the default to a user specified password.
7. If you wish to set the service account password to be different from the admin password, clear the related check box.

Results

If you are still not prompted to reset the password on login attempt after executing this procedure, contact your service provider.

Reset admin and service account passwords to their default values in a PowerStore X model appliance

Prerequisites

Know the primary node name of your primary appliance (for example, PSTX-44W1BW2-A and PowerStore D6013). If necessary, generate the `reset.iso` file.

About this task

For a PowerStore X model appliance, use an ISO image and mount it from vSphere. Pre-created image files can be downloaded from https://www.dell.com/support. You can also create your own image from a Linux system using one or both of the following touch commands depending on which passwords must be reset:

```
mkdir iso
touch iso/admin
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

NOTE: The ISO image, `reset.iso`, must reside on a datastore before it can be mounted as a virtual CD from vSphere.

NOTE: To reset the password if both nodes of the appliance are in Service Mode, use the following steps with two differences. First, you must upload the ISO image to the PRIVATE-C9P42W2.A.INTERNAL datastore of the controller virtual machine (VM) itself because the public datastore is not available. Second, upload and apply the `reset.iso` file to both controller VM nodes A and B. This action ensures that when the system is back in Normal Mode and PowerStore Manager access is available, you are prompted to provide a new password for both the admin and service users.

Steps

1. In vSphere under**Storage**, select your PowerStore X model appliance.

   For example, **DataCenter-WX-D6013** > **PowerStore D6013**

2. Under **Files**, select **ISOs**.
3. Select **Upload** and upload the `reset.iso` file, either the pre-created image file from https://www.dell.com/support or your own image file that you created on a Linux system.
   The `reset.iso` file appears in the **ISOs** folder.
4. In vSphere under **Host and Clusters**, select the primary node of the primary PowerStore X model appliance in the cluster.

   For example, **DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. Under **Summary**, click **CD/DVD drive 1** and select **Connect to datastore ISO file**.
   The **Choose an ISO image to mount** window appears.
6. Under **Datastores**, click the primary PowerStore X model appliance in the cluster and select the **ISOs** folder.
   The `reset.iso` file should appear under **Contents**.
7. Select the `reset.iso` file and click **OK**.
   Under **Summary**, **CD/DVD drive 1** should appear as **Connected** for about 10 seconds, and then change to **Disconnected**.
   The cluster admin password, or service password, or both, are now reset to their default.
8. Connect to the cluster through a browser using the cluster IP address and log in as admin with the default initial password, which is **`Password123#`**.
   A prompt to reset the admin or service passwords, or both should appear. If you prefer to reset the service password using SSH, the initial default password for the service account is **`service`**.
9. Change the admin password from the default to a user specified password.
10. If you wish to set the service account password to be different from the admin password, clear the related check box.

Results

If you are still not prompted to reset the password on login attempt after executing this procedure, contact your service provider.

Certificates

Data in the certificate store of PowerStore is persistent. The certificate store stores the following types of certificates:

- Certificate Authority (CA) certificates
- Client certificates
- Server certificates

Viewing certificates

About this task

The following information appears in PowerStore Manager for each certificate that is stored on the appliance:

- `Service`
- `Type`
- `Scope`
- `Issued by`
- `Valid`
- `Valid to`
- `Issued to`

ⓘ **NOTE:** Use the REST API or CLI to view additional certificate information.

To view the certificate information, do the following:

Steps

1. Launch the PowerStore Manager.
2. Click **Settings** and under **Security** click **Certificates**.
   Information about the certificates stored on the appliance appears.
3. To view the chain of certificates that comprise a certificate and associated information for a service, click the specific service.
   View Certificate Chain appears and lists information about the chain of certificates that comprise the certificate.

Secure communication between PowerStore appliances within a cluster

During cluster creation, the primary node of the cluster master appliance creates a certificate authority (CA) certificate, also known as the cluster CA. The master appliance passes the cluster CA certificate to the appliances joining the cluster.

Each PowerStore appliance in a cluster generates its own unique IPsec certificate which is signed by the cluster CA certificate. The sensitive data that PowerStore appliances transmit over their cluster network are protected by IPsec and TLS so that the security and integrity of the data is preserved.

Secure communication for replication and data import

PowerStore's certificate and credential infrastructure allows the exchange of server and client certificates, and user credentials. This process includes:

- Retrieving and validating server certificate during TLS handshake
- Adding the trusted CA certificate from the remote system to the credential store
- Adding the trusted server/client certificate to the credential store
- Assisting in establishing secure connections once the trust is established

PowerStore supports the following certificate management functionality:

- For replication, a certificate exchange between two PowerStore clusters to establish trusted management communication. To facilitate replication between PowerStore clusters, bi-directional trust must be established between the clusters to allow for mutual TLS authentication when issuing replication REST control requests.
- For data import, a certificate and credentials exchange with persistence, to establish a secure connection between a Dell EMC storage system (a VNX, Unity, Storage Center (SC), or a Peer Storage (PS) system) and a PowerStore cluster.

vSphere Storage API for Storage Awareness support

vSphere Storage API for Storage Awareness (VASA) is a VMware-defined, vendor-neutral API for storage awareness. A VASA Provider consists of multiple components working in cooperation to service incoming VASA API requests. The VASA API gateway, which receives all incoming VASA APIs, is deployed on the primary appliance (the appliance that owns the floating management IP) in a PowerStore cluster. ESXi hosts and vCenter Server connect to the VASA Provider and obtain information about available storage topology, capabilities, and status. After the vCenter Server provides this information to vSphere clients. VMware clients use VASA rather than PowerStore Manager clients.

The vSphere user must configure the VASA Provider instance as the provider of VASA information for the cluster. If the lead appliance goes down, the related process will restart on the appliance that becomes the next primary, along with the VASA Provider. The IP address fails over automatically. Internally, the protocol sees a fault when obtaining configuration change events from the newly active VASA Provider, but this fault causes an automatic resynchronization of the VASA objects without user intervention.

The PowerStore provides VASA 3.0 interfaces for vSphere 6.5 and 6.7.

VASA 3.0 supports Virtual Volumes (vVols). VASA 3.0 supports interfaces to query storage abstractions such as vVols and Storage Containers. This information helps storage policy-based management (SPBM) determine virtual drive placement and compliance. VASA 3.0 also supports interfaces to provision and manage the life cycle of vVols used to back up virtual drives. ESXi hosts directly invoke these interfaces.

For more information related to VASA, vSphere, and vVols, see the VMware documentation and the PowerStore Manager online help.

Authentication related to VASA

During the initial configuration of a PowerStore X model cluster, a vCenter Server is automatically established and a PowerStore VASA provider is automatically registered. The vCenter Server connection on a PowerStore X model cluster cannot be modified after the initial configuration is complete.

However, during the initial configuration of a PowerStore T model cluster, a connection to a vCenter Server and PowerStore VASA provider are optional. Establishing a connection to a vCenter Server and registering a VASA provider can be performed after the initial configuration of a PowerStore T model cluster is complete.

NOTE: PowerStore T model clusters can host traditional (VMFS) datastores without being registered as a VASA provider or connecting to a vCenter Server. However, registering a PowerStore VASA provider in vCenter Server is required to use vVols.

To manually establish an initial connection to a vCenter server and to register a PowerStore VASA provider in a vCenter Server, use the vSphere client to enter the following information to configure a connection to the PowerStore T model cluster:

- Name (can be any name that you choose)
- URL of the VASA Provider, using the following format for VASA 3.0: https://<Management IP address>:8443/version.xml
- Username of a PowerStore user (the role of this user must be either VM Administrator or Administrator)

  NOTE: A PowerStore user with the VM Administrator role is strictly used as a means to register certificates. A PowerStore user with an Administrator role can perform additional tasks. See Roles and privileges on page 8 for more details.

  - For local users use the syntax: local/<username>
  - For LDAP users use the syntax: <domain>/<username>
- Password associated with the PowerStore user.

NOTE: The PowerStore user credentials that are used here are only used during this initial step of the connection. If the PowerStore user credentials are valid for the target cluster, the certificate of the vCenter Server is automatically registered with the cluster. This certificate is used to authenticate all subsequent requests from the vCenter. No manual steps are required to install or upload this certificate to the VASA Provider. If the certificate has expired, the vCenter must register a new certificate to support a new session. If the user revokes the certificate, the session is invalidated and the connection is severed.

On the PowerStore T model cluster, use the PowerStore Manager to enter the following information:

- IP address of the vCenter
- Username of the vCenter
- Password associated with the vCenter.
- Username of a PowerStore user (the role must be either VM Administrator or Administrator)
- Password associated with the PowerStore user

vCenter session, secure connection, and credentials

A vCenter session begins when a vSphere administrator uses the vSphere Client to supply the vCenter Server with the VASA Provider URL and login credentials. The vCenter Server uses the URL, credentials, and the SSL certificate of the VASA Provider to establish a secure connection with the VASA Provider. A vCenter session ends when one of the following events occurs:

- An administrator uses the vSphere Client to remove the VASA Provider from the vCenter configuration, and the vCenter Server terminates the connection.
- The vCenter Server fails or a vCenter Server service fails, terminating the connection. If vCenter or the vCenter Server service cannot reestablish the SSL connection, it starts a new session.
- The VASA Provider fails, terminating the connection. When the VASA Provider starts up, it can respond to communication from the vCenter Server to reestablish the SSL connection and VASA session.

A vCenter session is based on secure HTTPS communication between a vCenter Server and a VASA Provider. In VASA 3.0, the vCenter Server acts as the VMware certificate authority (VMCA). The VASA Provider transmits a self-signed certificate on request, after authorizing the request. It adds the VMCA certificate to its truststore, then issues a certificate signing request, and replaces its self-signed certificate with the VMCA signed certificate. Future connections will be authenticated by the VASA

Provider using the client Storage Monitoring Service(SMS) certificate validated against the previously registered root signing certificate. A VASA Provider generates unique identifiers for storage entity objects, and the vCenter Server uses the identifier to request data for a specific entity.

A VASA Provider uses SSL certificates and the VASA session identifier to validate VASA sessions. After the session is established, a VASA Provider must validate both the SSL certificate and the VASA session identifier associated with each function call from the vCenter Server. The VASA Provider uses the VMCA certificate stored in its truststore to validate the certificate associated with function calls from the vCenter SMS. A VASA session persists across multiple SSL connections. If an SSL connection is dropped, the vCenter Server will perform an SSL handshake with the VASA Provider to re-establish the SSL connection within the context of the same VASA session. If an SSL certificate expires, the vSphere administrator must generate a new certificate. The vCenter Server will establish a new SSL connection and register the new certificate with the VASA Provider.

CAUTION: SMS does not call the `unregisterVASACertificate` function against a 3.0 VASA Provider. Therefore, even after unregistration, the VASA Provider can continue to use its VMCA signed certificate obtained from SMS.

CHAP authentication

Challenge Handshake Authentication Protocol (CHAP) is a method of authenticating iSCSI initiators (hosts) and targets (volumes and snapshots). CHAP exposes iSCSI storage, and ensures a secure, standard storage protocol. Authentication depends on a secret, similar to a password, that is known to both the authenticator and the peer. There are two variants of CHAP protocol:

- Single CHAP authentication allows for the iSCSI target to authenticate the initiator. When an initiator tries to connect to a target (Normal mode or through Discovery mode), it provides a user name and password to the target.
- Mutual CHAP authentication is applied in addition to single CHAP. Mutual CHAP allows for the iSCSI target and the initiator to authenticate each other. Each iSCSI target presented by the group is authenticated by the iSCSI initiator. When an initiator tries to connect to a target, the target provides a user name and password to the initiator. The initiator compares the supplied user name and password to information it holds. If they match, the initiator can connect to the target.

NOTE: If CHAP will be used in your environment, it is recommended that you set up and enable CHAP authentication before preparing volumes to receive data. If you prepare drives to receive data before you set up and enable CHAP authentication, you could lose access to the volumes.

PowerStore does not support iSCSI CHAP Discovery mode. The following table shows the limitations of PowerStore related to iSCSI CHAP Discovery mode.

Table 4. iSCSI CHAP Discovery mode limitations

CHAP Mode	Single Mode (initiator enabled)	Mutual Mode (initiator and target enabled)
Discovery	PowerStore will not authenticate (challenge) the host. Authentication cannot be used to preclude the discovery of targets. This does not result in unintended access to user data.	PowerStore will not respond to an authentication request (challenge) from a host, and discovery will fail if the host challenges PowerStore.
Normal	Works as expected. Credentials are tested by PowerStore.	Works as expected. Credentials are transferred by PowerStore.

For remote replication between a source and target appliance, the verify and update process detects changes in the local and remote systems and reestablishes data connections, while also taking the CHAP settings into account.

Configuring CHAP

CHAP single (initiator enabled) or mutual (initiator and target) authentication can be enabled on a PowerStore cluster. CHAP can be enabled for a cluster implementation of one appliance or multiple PowerStore appliances and external hosts.

When single authentication is enabled, the username and password for each initiator are required to be entered when external hosts are added. When mutual authentication is enabled, the username and password for the cluster are also required to be entered. When adding a host and adding initiators with CHAP enabled, the initiator password must be unique, you cannot use the same password across the initiators of a host. Specific details on how to configure the CHAP configuration of an external host varies. To utilize this capability, you need to be familiar with the operating system of the host and how to configure it.

ⓘ **NOTE:** Enabling CHAP once hosts are configured on the system is a disruptive action for the external hosts. It causes I/O interruption until configurations are set up on both the external host and appliance. It is recommended that, before adding external hosts to the appliance, you decide what type of CHAP configuration you want to implement, if any.

If you enable CHAP after hosts are added, update each host's initiators. If CHAP is enabled, you cannot add a host to a host group that does not have CHAP credentials. Once CHAP is enabled and you add a host later, manually register the host in the PowerStore Manager, under **Compute** select **Hosts & Host Groups**. You need to enter credentials at the iSCSI level for authentication use. In this case, copy the IQN from the host and then add the related CHAP credentials for each initiator.

Configure CHAP for a cluster through any of the following means:

- **CHAP** - A CHAP settings page that you can access from the PowerStore Manager (click **Settings** and under **Security** select **CHAP**).
- REST API server - Application interface that can receive REST API requests to configure CHAP settings. For more information about the REST API, refer to the *PowerStore REST API Reference Guide*.

To determine the status of CHAP, in the PowerStore Manager, click **Settings** and under **Security** select **CHAP**.

External SSH access

Each appliance can optionally enable external secure shell (SSH) access to the SSH port of the appliance IP address, which takes the user to the service feature on the primary node of an appliance. The appliance IP address floats between the two nodes of the appliance as the primary designation changes. If external SSH is disabled, SSH access is disallowed.

When an appliance first comes up and is not configured, SSH is enabled by default so that the appliance can be serviced if issues are encountered before it is added to a cluster. When a new cluster is created or for a join cluster operation, all appliances should have SSH initially set to disabled.

Configuring external SSH access

Configure external SSH access to appliances within a cluster by using any of the following means:

- **SSH Management** – A SSH settings page that you can access from the PowerStore Manager (click **Settings** and under **Security** select **SSH Management**).
- REST API server – Application interface that can receive REST API requests to configure SSH settings. For more information about the REST API, see the *PowerStore REST API Reference Guide*.
- `svc_service_config` – A service command that you can enter directly as the service user on the appliance. For more information about this command, see the *PowerStore Service Scripts Guide*.

To determine the status of SSH on appliances within a cluster, in the PowerStore Manager, click **Settings** and under **Security** select **SSH Management**. You can also enable or disable SSH on one or more appliances that you select.

Once the SSH service has been successfully enabled, use any SSH client to log in to the appliance IP address. Accessing the appliance requires service user credentials.

The service account enables users to perform the following functions:

- Perform specialized appliance service scripts for monitoring and troubleshooting appliance system settings and operations.
- Operate only a limited set of commands that are assigned as a member of a non-privileged Linux user account in restricted shell mode. This account does not have access to proprietary system files, configuration files, or user or customer data.

For maximum appliance security, it is recommended to always leave the external SSH service interface disabled unless it must be used to perform service operations on the appliance. After performing the necessary service operations, disable the SSH interface to ensure that the appliance remains secure.

SSH sessions

The PowerStore SSH service interface sessions are maintained according to the settings established by the SSH client. Session characteristics are determined by the SSH client configuration settings.

Service account password

The service account is an account that service personnel can use to perform basic Linux commands.

During initial configuration of the appliance, you must change the default service password. The service password restrictions are the same as those that apply to the System management accounts (see Username and password usage on page 7).

SSH authorization

Service account authorization is based on the following:

- Application isolation – PowerStore software uses container technology that provides application isolation. Appliance service access is provided by the service container, only a set of service scripts and a set of Linux commands are available. The service account does not have the ability to access other containers which serve file system and block I/O to users.
- Linux file system permissions – Most Linux tools and utilities that modify system operation in any way are not available for the service user, it requires superuser account privileges. Since the service account does not have such access rights, the service account cannot use Linux tools and utilities to which it does not have execute permissions and cannot edit configuration files that require root access to read or modify, or both.
- Access controls – Besides application isolation provided by container technology, the access control list (ACL) mechanism on the appliance uses a list of very specific rules to explicitly grant or deny access to system resources by the service account. These rules specify service account permissions to other areas of the appliance that are not otherwise defined by standard Linux file system permissions.

Appliance service scripts

A set of problem diagnostic, system configuration, and system recovery scripts are installed on the appliance's software version. These scripts provide an in-depth level of information and a lower level of system control than is available through PowerStore Manager. The *PowerStore Service Scripts Guide* describes these scripts and their common use cases.

Appliance node Ethernet service port and IPMItool

Your appliance provides console access over an Ethernet service port that is on each node. This access requires the use of the IPMItool. The IPMItool is a network tool similar to SSH or Telnet that interfaces with each node over an Ethernet connection by using the IPMI protocol. The IPMItool is a Windows utility that negotiates a secure communication channel to access the node console of an appliance. This utility requires physical access to activate the console.

The node Ethernet service port interface provides the same functions and features as the service SSH interface (Service LAN interface). Also, it is subject to the same restrictions. However, users access the interface through an Ethernet port connection rather than an SSH client. This interface is designed for field service personnel who can connect to the appliance without having to disturb your network. A dedicated management console is not necessary.

This interface provides a direct point-to-point, nonroutable connection. Service personnel can use the Service LAN interface for console output, SSH access to the PowerStore Service Container and PowerStore Manager including the Initial Configuration Wizard (ICW). SSH access to the Service Container through the Service LAN interface is always enabled, and cannot be disabled; however, you manage the service account credential.

For a list of service scripts, see the *PowerStore Service Scripts Guide*.

NFS secure

NFS secure is the use of Kerberos for authenticating users with NFSv3 and NFSv4. Kerberos provides integrity (signing) and privacy (encryption). Integrity and privacy are not required to be enabled, they are NFS export options.

Without Kerberos, the server relies entirely on the client to authenticate users: the server trusts the client. With Kerberos this is not the case, the server trusts the Key Distribution Center (KDC). It is the KDC which handles the authentication and manages accounts (principals) and passwords. Moreover, no password in any form is sent on the wire.

Without Kerberos, the credential of the user is sent on the wire un-encrypted and thus can easily be spoofed. With Kerberos, the identity (principal) of the user is included in the encrypted Kerberos ticket, which can only be read by the target server and KDC. They are the only ones to know the encryption key.

In conjunction with NFS secure, AES128 and AES256 encryption in Kerberos is supported. Along with NFS secure, this also impacts SMB and LDAP. These encryptions are now supported by default by Windows and Linux. These new encryptions are much more secure; however, it is up to the client whether they are used. From that user principal, the server builds the credential of that user by querying the active Unix Directory Service (UDS). Since NIS is not secured, it is not recommended to use it with NFS secure. It is recommended to use Kerberos with LDAP or LDAPS.

NFS secure can be configured through PowerStore Manager.

File protocol relationships

With Kerberos the following is required:

- DNS - You must use DNS name in place of IP addresses.
- NTP - PowerStore must have a configured NTP server.

  NOTE: Kerberos relies on the correct time synchronization between the KDC, servers, and client on the network.
- UDS - To build credentials.
- Hostname - Kerberos works with names and not IP addresses.

NFS secure uses one or two service principal names (SPNs) depending on the value of the hostname. If the hostname is in FQDN format host.domain:

- The short SPN: **`nfs/host@REALM`**
- The long SPN: **`nfs/host.domainFQDN@REALM`**

If the hostname is not in FQDN format, only the short SPN will be used.

Similar to SMB, where an SMB server can be joined to a domain, an NFS server can be joined to a realm (the Kerberos equivalent term for domain). There are two options for this:

- Use the configured Windows domain if any
- Entirely configure a UNIX KDC based Kerberos realm

If the administrator selects to use the configured Windows domain, there is nothing else to do. Every SPN used by the NFS service is automatically added/removed into the KDC when joining/unjoining the SMB server. Note that the SMB server cannot be destroyed if NFS secure is configured to use the SMB configuration.

If the administrator selects to use a UNIX based Kerberos realm, more configuration is needed:

- Realm name: The name of the Kerberos realm, which generally contains all upper-case letters.
- Entirely configure a UNIX KDC based Kerberos realm.

To ensure that a client mounts an NFS export with a specific security, a security parameter, sec, is provided that indicates which minimal security is allowed. There are 4 kinds of security:

- `AUTH_SYS`: Standard legacy security which does not use Kerberos. The server trust the credential provided by the client
- `KRB5`: Authentication using Kerberos v5
- `KRB5i`: Kerberos authentication plus integrity (signing)
- `KRB5p`: Kerberos authentication plus integrity plus privacy (encryption)

If a NFS client tries to mount an export with a security that is lower than the configured minimal security, the access will be denied. For example, if minimal access is `KRB5i`, any mount using `AUTH_SYS` or `KRB5` will be rejected.

Building a credential

When a user connects to the system, it presents only its principal, **`user@REALM`**, which is extracted from the Kerberos ticket. Unlike `AUTH_SYS` security, the credential is not included in the NFS request. From the principal, the user part (before the @) is extracted and used to lookup the UDS for the corresponding uid. From that uid, the credential is built by the system using the active UDS, similar to when the Extended NFS credential is enabled (with the exception that, without Kerberos, the uid is provided directly by the request).

If the principal is not mapped in the UDS, the configured default UNIX user credential is used instead. If the default UNIX user is not set, the credential used will be nobody.

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.

ⓘ **NOTE:** If the older SMB1 protocol needs to be supported in your environment, it can be enabled by using the `svc_nas_cifssupport` service command. For more information about this service command, see the *PowerStore Service Scripts Guide*.

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 referred to as the mode bits or NFSv4 ACL of a file system object. Mode bits are represented by a bit string. 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.

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 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 through the use of a security descriptor. 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 computer and a list of rights that are denied or allowed for that SID.

File systems access in a multiprotocol environment

File access is provided through NAS servers. A NAS server contains a set of 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 mode for multiprotocol sharing allows the sharing of the same data between SMB and NFS. Because the multiprotocol sharing mode provides simultaneous SMB and NFS access to a file system, the mapping of Windows users to UNIX users and defining the security rules to use (mode bits, ACL, and user credentials) must be considered and configured properly for multiprotocol sharing.

ⓘ **NOTE:** For information about configuring and managing NAS servers with regard to multiprotocol sharing, user mapping, access policies, and user credentials, see the PowerStore Manager online help.

User mapping

In a multiprotocol context, a Windows user needs to be matched to 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 should be one UDS enabled or local files enabled, or both local files and a UDS enabled for the NAS server when multiprotocol sharing is enabled. The Unix directory service property of the NAS server 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

secmap

The function of secmap is to store all SID-to-UID and primary GID and UID-to-SID mappings to ensure coherency across all file systems of the NAS server.

ntxmap

ntxmap is used to associate a Windows account to a UNIX account when the name is different. For example, if there is a user who has an account that is called Gerald on Windows but the account on UNIX is called Gerry, ntxmap is used to make the correlation between the two.

SID to UID, primary GID mapping

The following sequence is the process 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 GID mapping is resolved.
2. If the SID is not found in secmap, the Windows name related to the SID must be found.
   a. The local group databases of the SMB servers of the NAS are searched for the SID. If the SID is found, the related Windows name is the local user name along with the SMB server name.
   b. If the SID is not found in the local group database, the DC of the domain is searched. If the SID is found, the related Windows name is the user name. If the SID is not resolvable, access is denied.
3. The Windows name is translated into a UNIX name. The ntxmap is used for this purpose.
   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, the Windows name is used as the UNIX name.
4. The UDS (NIS server, LDAP server, or local files) is searched using the UNIX name.
   a. If the UNIX user name is found in the UDS, the UID and GID mapping is resolved.
   b. If the UNIX name is not found, but the automatic mapping for unmapped Windows accounts feature is enabled, the UID is automatically assigned.
   c. If the UNIX user name is not found in the UDS but there is a default UNIX account, the UID and GID mapping is resolved to that of the default UNIX account.
   d. If the SID is not resolvable, 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 used to resolve an SID to a UID, primary GID mapping:

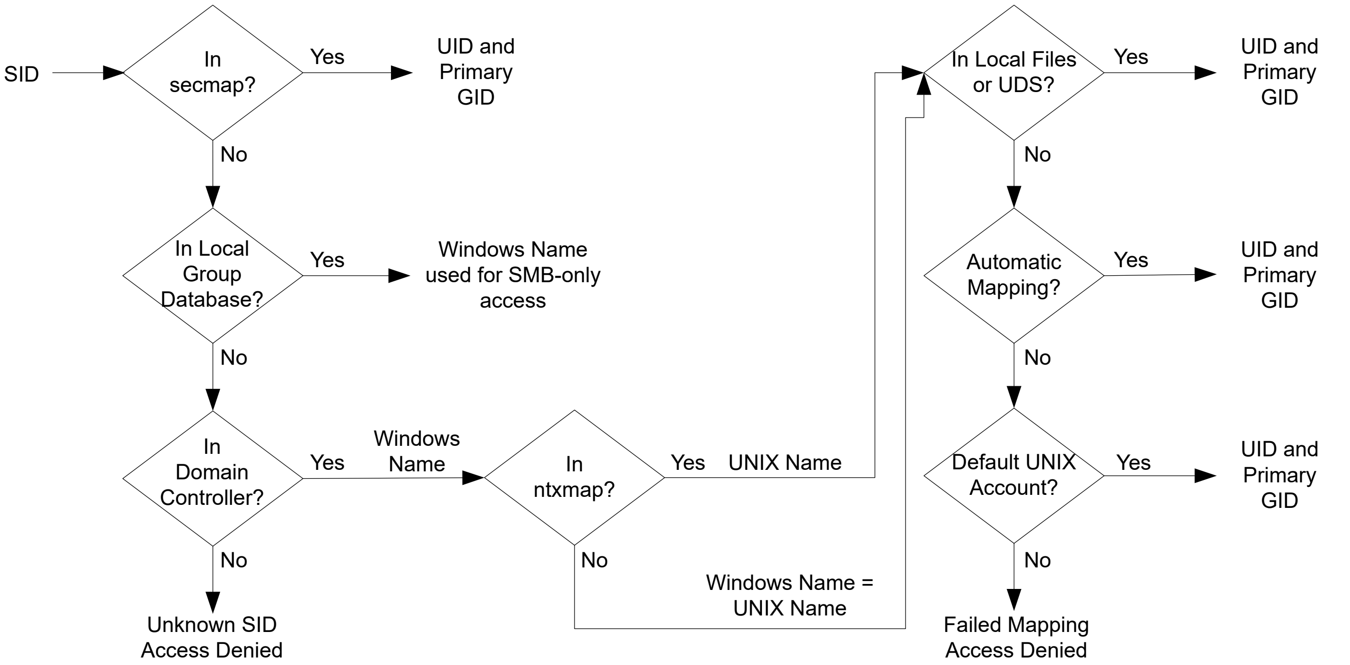

Figure 1. Process for resolving an SID to a UID, primary GID mapping

UID to SID mapping

The following sequence is the process 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 related to the UID must be found.
   a. The UDS (NIS server, LDAP server, or local files) is searched using the UID. If the UID is found, the related UNIX name is the user name.
   b. If the UID is not found in the UDS but there is a default Windows account, the UID is mapped to the SID of the default Windows account.
3. If the default Windows account information is not used, the UNIX name is translated into a Windows name. The ntxmap is used for this purpose.
   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, the UNIX name is used as the Windows name.
4. The Windows DC or the local group database is searched using the Windows name.
   a. 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 local group database of that SMB server is searched to resolve the SID mapping.
   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.
   d. If the SID is not resolvable, 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 used to resolve a UID to an SID mapping:

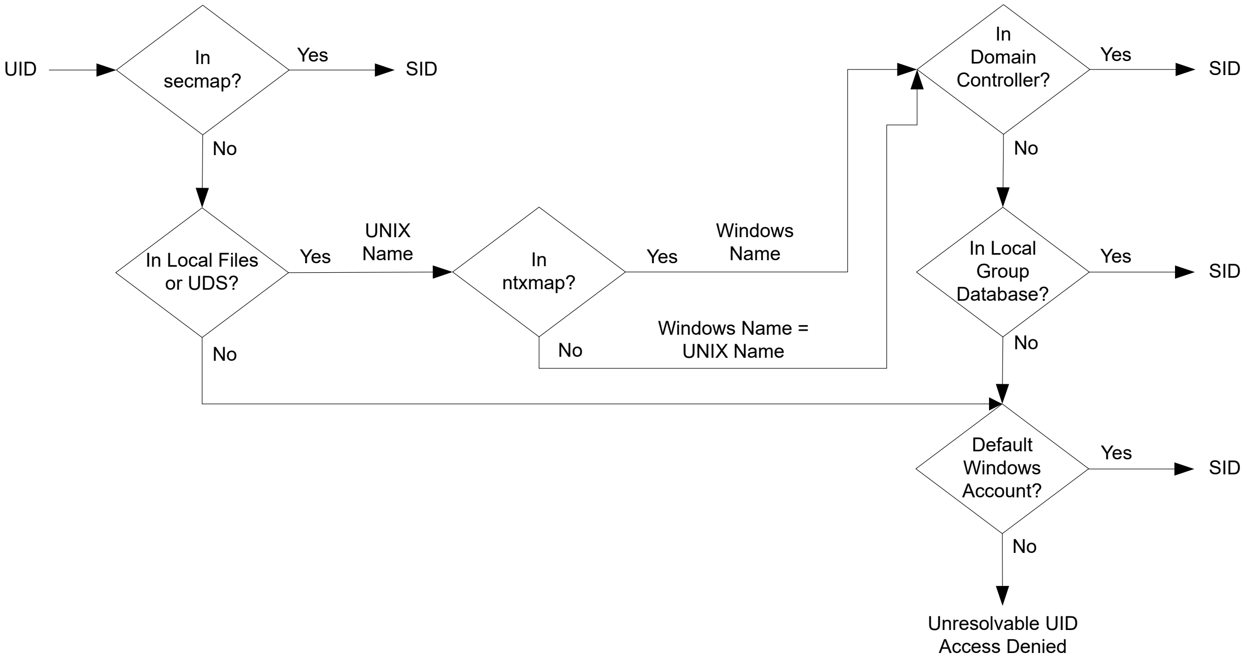

Figure 2. Process used to resolve a UID to an SID mapping

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) with the exception for non-secure NFS access, where the credential is 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 associated with UNIX security.

For Windows security authentication, the credential is 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. There are privileges associated with Windows security, such as TakeOwnership, Backup, and Restore, that 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:

Access policy	Description
Native (default)	• Each protocol manages access with its native security. • Security for NFS shares uses the UNIX credential 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 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. • Permissions for newly created files are determined by an SMB ACL conversion. 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. • Upon request for SMB access, the UNIX credential built from the local files or UDS is used to check the NFSv3 mode bits or NFSv4 ACL for permissions. • Permissions for newly created files are determined by the UMASK. • NFSv3 UNIX mode bits or NFSv4 ACL permission changes are synchronized to the SMB ACL.

Access policy	Description
	● 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 user name 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 that 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 user name is `domain\user` or `user@domain`) or a UNIX authentication (for the other formats of a single user name). The SMB authentication is ensured by the Windows DC of the domain defined in the NAS server. The UNIX authentication is ensured by the NAS server according to the encrypted password stored in either a remote LDAP server, a remote NIS server, or in the local password file of the NAS server.

Credentials for file level security

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

- To build 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.
- To build a UNIX credential for an SMB request when the access policy for the file system is UNIX.
- To build a Windows credential for an SMB request.
- To build 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 included 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 with regards to 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 through PowerStore Manager.

UNIX credential for NFS requests

To handle NFS requests for an NFS only or multi-protocol file system with a UNIX or native access policy, a UNIX credential must be used. The UNIX credential is always embedded in each request; however, the credential is limited to 16 extra groups. The NFS server `extendedUnixCredEnabled` property provides the ability to build a credential with more than 16 groups. If this property 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 embedded in the request is used.

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

UNIX credential for SMB requests

To handle SMB requests for a multi-protocol file system with a UNIX access policy, a Windows credential must first be built for the SMB user at the session setup time. The SID of the Windows user is used to find the name from the AD. That name is then used (optionally through ntxmap) to find a Unix UID and GID from the UDS or local file (passwd file). The owner UID of the user is included in 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

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

When using Kerberos authentication, the credential of the user is included in 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 are taken from the LGDB.

Additionally, 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 through the use of 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 through 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, through 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.

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 Windows Server environment. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the storage system.

Why is antivirus important?

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 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 additional information about CAVA, which is part of Common Event Enabler (CEE), see *Using the Common Event Enabler on Windows Platforms* at https://www.dell.com/powerstoredocs.

Code signing

PowerStore is designed to accept software upgrades for both new releases and patch releases. A master GNU Privacy Guard (GPG) key signs all PowerStore software packages and Dell EMC controls this GPG key. The PowerStore software upgrade process verifies the signature of the software package, and rejects invalid signatures that might indicate possible tampering or corruption. The verification step is built into the upgrade process, and the signature of the software package is automatically verified during the pre-installation phase.

2

Communication security settings

This section contains the following topics:

Topics:

- Port Usage
- Transport Layer Security

Port Usage

The following sections outline the collection of network ports and the corresponding services that may be found on the appliance. The appliance functions as a network client in several circumstances, for example, in communicating with a vCenter Server. In these instances, the appliance initiates communication and the network infrastructure will need to support these connections.

ⓘ **NOTE:** For additional information about ports, see Knowledge Base Article 542240, *PowerStore: Customer Network Firewall Rules - TCP/UDP Ports*. Go to https://www.dell.com/support/kbdoc/en-us/542240. The Customer Network Firewall Rules tool enables you to filter and review the list of firewall rules and ports that are relevant to your PowerStore deployment.

Appliance network ports

The following table outlines the collection of network ports and the corresponding services that may be found on the appliance.

Table 5. Appliance network ports

Port	Service	Protocol	Access Direction	Description
22	SSH client, SupportAssist Connect Home	TCP	Bi-directional	● Allows SSH access (if enabled). ● Required for SupportAssist Connect Home. If closed, management connections using SSH will be unavailable.
25 or 587	SMTP	TCP	Outbound	Allows the appliance to send email. If closed, email notifications will be unavailable.
26	SSH client	TCP	Bi-directional	SSH access to port 22 is redirected to this port. If closed, management connections using SSH will be unavailable.
53	DNS	TCP/UDP	Outbound	Used to transmit DNS queries to the DNS server. If closed, DNS name resolution will not work.
80, 8080, 3128	SupportAssist	TCP	Outbound	Used for SupportAssist Proxy connection.
123	NTP	TCP/UDP	Outbound	NTP time synchronization. If closed, time will not be synchronized among appliances.
162 or between 1024 - 49151	SNMP	UDP	Outbound	SNMP communications. If closed, storage system alert mechanisms which rely on

Table 5. Appliance network ports (continued)

Port	Service	Protocol	Access Direction	Description
				SNMP will not be sent. The default port set for SNMP is 162.
443	HTTPS	TCP	Bi-directional	Secure HTTP traffic to PowerStore Manager. If closed, communication with the appliance will be unavailable.
500	IPsec (IKEv2)	UDP	Bi-directional	To make IPSec work through your firewalls, open UDP port 500 and permit IP protocol numbers 50 and 51 on both inbound and outbound firewall filters. UDP Port 500 should be opened to allow Internet Security Association and Key Management Protocol (ISAKMP) traffic to be forwarded through your firewalls. IP protocol ID 50 should be set to allow IPSec Encapsulating Security Protocol (ESP) traffic to be forwarded. IP protocol ID 51 should be set to allow Authentication Header (AH) traffic to be forwarded. If closed, IPsec connection between PowerStore appliances will be unavailable.
514	Remote Logging	UDP	Outbound	Allows the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.
1468	Remote Logging	TCP	Outbound	Allows the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.
3033	Import	TCP/UDP	Outbound	Required for storage import from legacy EqualLogic Peer Storage and Compellent Storage Center systems.
3260	iSCSI	TCP	● Inbound for Host and ESXi host access ● Bi-directional for replication ● Outbound for storage import	Required to provide the following access to iSCSI services: ● External host iSCSI access ● External or PowerStore embedded ESXi host iSCSI access ● Inter cluster access for replication ● Storage import access from legacy EqualLogic Peer Storage, Compellent Storage Center, Unity, and VNX2 systems If closed, iSCSI services will be unavailable. Used by Data mobility to support reasonable replication performance on low latency connection.
3261	Data mobility	TCP	Bi-directional	Used by Data mobility to support reasonable replication performance on high latency connection.
5353	Multicast DNS (mDNS)	UDP	Bi-directional	Multicast DNS query. If closed, mDNS name resolution will not work.
8443	VASA, SupportAssist	TCP	● Inbound for VASA	● Required for the VASA Vendor Provider for VASA 3.0.

Table 5. Appliance network ports (continued)

Port	Service	Protocol	Access Direction	Description
			- Outbound for SupportAssist	- Required for the related SupportAssist Connect Home functions.
8443, 50443, 55443, or 60443	Windows import host agent, Linux import host agent, or VMware import host agent	TCP	Outbound	One of these ports must be open when importing data storage from legacy storage systems.
9443	SupportAssist	TCP	Outbound	Required for SupportAssist REST API related to Connect Home.

Appliance network ports related to file

The following table outlines the collection of network ports and the corresponding services that may be found on the appliance related to file.

ⓘ **NOTE:** Outbound ports are ephemeral.

Table 6. Appliance network ports related to file

Port	Service	Protocol	Access Direction	Description
20	FTP	TCP	Outbound	Port used for FTP data transfers. This port can be opened by enabling FTP. Authentication is performed on port 21 and defined by the FTP protocol.
21	FTP	TCP	Inbound	Port 21 is the control port on which the FTP service listens for incoming FTP requests.
22	SFTP	TCP	Inbound	Allows alert notifications through SFTP (FTP over SSH). SFTP is a client/server protocol. Users can use SFTP to perform file transfers on an appliance on the local subnet. Also provides outgoing FTP control connection. If closed, FTP will not be available.
53	DNS	TCP/UDP	Outbound	Used to transmit DNS queries to the DNS server. If closed, DNS name resolution will not work. Required for SMB v1.
88	Kerberos	TCP/UDP	Outbound	Required for Kerberos authentication services.
111	RPC bind (for SDNAS namespaces; otherwise, host service)	TCP/UDP	Bi-directional	Opened by the standard portmapper or rpcbind service and is an ancillary appliance network service. It cannot be stopped. By definition, if a client system has network connectivity to the port, it can query it. No authentication is performed.
123	NTP	UDP	Outbound	NTP time synchronization. If closed, time will not be synchronized among appliances.
135	Microsoft RPC	TCP	Inbound	Multiple purposes for Microsoft Client. Also used for NDMP.

Table 6. Appliance network ports related to file (continued)

Port	Service	Protocol	Access Direction	Description
137	Microsoft Netbios WINS	UDP; TCP/UDP	Inbound; Outbound	The NETBIOS Name Service is associated with the appliance SMB file sharing services and is a core component of that feature (Wins). If disabled, this port disables all SMB related services.
138	Microsoft Netbios BROWSE	UDP	Outbound	The NETBIOS Datagram Service is associated with the appliance SMB file sharing services and is a core component of that feature. Only Browse service is used. If disabled, this port disables Browsing capability.
139	Microsoft SMB	TCP	Bi-directional	The NETBIOS Session Service is associated with appliance SMB file sharing services and is a core component of that functionality. If SMB services are enabled, this port is open. It is specifically required for SMB v1.
162 or between 1024 - 49151	SNMP	UDP	Outbound	SNMP communications. If closed, storage system alert mechanisms which rely on SNMP will not be sent. The default port set for SNMP is 162.
389	LDAP	TCP/UDP	Outbound	Unsecure LDAP queries. If closed, Unsecure LDAP authentication queries will be unavailable. Secure LDAP is configurable as an alternative.
445	Microsoft SMB	TCP	Inbound	SMB (on domain controller) and SMB connectivity port for Windows 2000 and later clients. Clients with legitimate access to the appliance SMB services must have network connectivity to the port for continued operation. Disabling this port disables all SMB related services. If port 139 is also disabled, SMB file sharing is disabled.
464	Kerberos	TCP/UDP	Outbound	Required for Kerberos authentication services and SMB.
500	IPsec (IKEv2)	UDP	Bi-directional	To make IPSec work through your firewalls, open UDP port 500 and permit IP protocol numbers 50 and 51 on both inbound and outbound firewall filters. UDP Port 500 should be opened to allow Internet Security Association and Key Management Protocol (ISAKMP) traffic to be forwarded through your firewalls. IP protocol ID 50 should be set to allow IPSec Encapsulating Security Protocol (ESP) traffic to be forwarded. IP protocol ID 51 should be set to allow Authentication Header (AH) traffic to be forwarded. If closed, IPsec connection between PowerStore appliances will be unavailable.
514	Remote Logging	UDP	Outbound	Allows the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.

Table 6. Appliance network ports related to file (continued)

Port	Service	Protocol	Access Direction	Description
636	LDAPS	TCP/UDP	Outbound	Secure LDAP queries. If closed, secure LDAP authentication will be unavailable.
1234	NFS mountd	TCP/UDP	Bi-directional	Used for the mount service, which is a core component of the NFS service (versions 2, 3, and 4).
1468	Remote Logging	TCP	Outbound	Allows the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.
2000	SSHD	TCP	Inbound	SSHD for serviceability (optional)
2049	NFS I/O	TCP/UDP	Bi-directional	Used to provide NFS services.
3268	LDAP	UDP	Outbound	Unsecure LDAP queries. If closed, Unsecure LDAP authentication queries will be unavailable.
3269	LDAPS	UDP	Outbound	Secure LDAP queries. If closed, Secure LDAP authentication queries will be unavailable.
4000	STATD for NFSv3	TCP/UDP	Bi-directional	Used to provide NFS statd services. statd is the NFS file-locking status monitor and works in conjunction with lockd to provide crash and recovery functions for NFS. If closed, NAS statd services will be unavailable.
4001	NLMD for NFSv3	TCP/UDP	Bi-directional	Used to provide NFS lockd services. lockd is the NFS file-locking daemon. It processes lock requests from NFS clients and works in conjunction with the statd daemon. If closed, NAS lockd services will be unavailable.
4002	RQUOTAD for NFSv3	TCP/UDP; UDP	Inbound; Outbound	Used to provide NFS rquotad services. The rquotad daemon provides quota information to NFS clients that have mounted a file system. If closed, NAS rquotad services will be unavailable.
4003	XATTRPD (extended file attribute)	TCP/UDP	Inbound	Required for managing file attributes in a multi-protocol environment.
4658	PAX (NAS server archive)	TCP	Inbound	PAX is an appliance archive protocol that works with standard UNIX tape formats.
8888	RCPD (replication data path)	TCP	Inbound	Used by the replicator (on the secondary side). It is left open by the replicator as soon as some data has to be replicated. After it is started, there is no way to stop the service.
10000	NDMP	TCP	Inbound	● Enables you to control the backup and recovery of a Network Data Management Protocol (NDMP) server through a network backup application, without installing third party software on the server. In an appliance, the NAS Server functions as the NDMP server.

Table 6. Appliance network ports related to file (continued)

Port	Service	Protocol	Access Direction	Description
				- The NDMP service can be disabled if NDMP tape backup is not used. - The NDMP service is authenticated with a username/password pair. The username is configurable. The NDMP documentation describes how to configure the password for a variety of environments.
[10500,10531]	NDMP reserved range for NDMP dynamic ports	TCP	Inbound	For three-way backup/restore sessions, NAS Servers use ports 10500 to 10531.
12228	Antivirus checker service	TCP	Outbound	Required for the Antivirus checker service.

Network ports related to PowerStore X model appliances

The following table outlines the collection of network ports and the corresponding services that may be found on PowerStore X model appliances.

Table 7. Network ports related to PowerStore X model appliances

Port	Service	Protocol	Access Direction	Description
22	SSH server	TCP	Inbound	Allows SSH access (if enabled). If closed, management connections using SSH will be unavailable.
80, 9000	vSphere Web Access	TCP	Inbound	Access for vSphere Update Manager Web Client plug-in for vSphere Web Client.
162 or between 1024 - 49151	SNMP	UDP	Outbound	SNMP communications. If closed, storage system alert mechanisms which rely on SNMP will not be sent. The default port set for SNMP is 162.
427	CIM Service Location Protocol (SLP)	TCP/UDP	Bi-directional	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.
443	vSphere Web Client	TCP	Inbound	Used for client connections.
514	Remote Logging	UDP	Outbound	Allows the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.
902	Network File Copy (NFC), VMware vCenter, vSphere Web Client	TCP	- Bi-directional for NFC - Outbound for VMware vCenter - Inbound for vSphere Web client	- NFC provides a file-type-aware FTP service for vSphere components. ESXi uses NFC for operations such as copying and moving data between datastores by default. - VMware vCenter agent - For vSphere Web client, used for client connections.
1468	Remote Logging	TCP	Outbound	Allows the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.

Table 7. Network ports related to PowerStore X model appliances (continued)

Port	Service	Protocol	Access Direction	Description
5900, 5901, 5902, 5903, 5904	RFB protocol	TCP	Inbound	Remote access to graphical user interfaces such as VNC.
5988	Common Information Model (CIM) Server	TCP	Inbound	Server for CIM.
5989	CIM Secure Server	TCP	Inbound	Server for CIM.
6999	NSX Virtual Distributed Logical Router, rabbitmqproxy	UDP	● Bi-directional for NSX Virtual Distributed Router service ● Outbound for rabbitmqproxy	● For NSX Virtual Distributed Router service, the firewall port associated with this service is opened when NSX VIBs are installed and the VDR module is created. If no VDR instances are associated with the host, the port does not have to be open. ● For rabbitmqproxy, a proxy running on the ESXi host. This proxy allows applications that are running inside virtual machines to communicate with the AMQP brokers that are running in the vCenter network domain. The virtual machine does not have to be on the network, that is, no NIC is required. Ensure that outgoing connection IP addresses include at least the brokers in use or future. You can add brokers later to scale up.
8000	vMotion	TCP	Bi-directional	Required for virtual machine migration with vMotion. ESXi hosts listen on port 8000 for TCP connections from remote ESXi hosts for vMotion traffic.
8100, 8200, 8300	Fault Tolerance	TCP/UDP	Bi-directional	Used for traffic between hosts for vSphere Fault Tolerance (FT).
8301, 8302	DVSSync	UDP	Bi-directional	DVSSync ports are used for synchronizing states of distributed virtual ports between hosts that have VMware FT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT, these ports do not have to be open.
9080	I/O filter	TCP	Outbound	Used by the I/O Filters storage feature.
31031	vSphere Replication, VMware Site Recovery Manager	TCP	Outbound	Used for ongoing replication traffic by vSphere Replication and VMware Site Recovery Manager.
44046	vSphere Replication, VMware Site Recovery Manager	TCP	Outbound	Used for ongoing replication traffic by vSphere Replication and VMware Site Recovery Manager.

Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol that allows for secure communication over a network. PowerStore supports TLS 1.2 by default. PowerStore uses the TLS 1.2 protocol as both a server (for management traffic) and as a client (for example, when importing external data from older systems). For some operations, an earlier version of the TLS protocol may be required. For example, importing external storage from a different storage system that does not support TLS 1.2 but does support TLS 1.1. TLS 1.1 is disabled by default on PowerStore and is not considered a secure protocol. TLS 1.1 can be enabled on PowerStore and allows users to import data from older systems that do not support TLS 1.2. When TLS 1.1 is enabled, both TLS 1.1 and TLS 1.2 are supported and considered as valid protocols.

ⓘ **NOTE:** For enhanced security, disable TLS 1.1 and revert to the TLS 1.2 default once the operation that requires the earlier TLS version has completed.

Configuring Transport Layer Security

Configure Transport Layer Security (TLS) for a PowerStore cluster through any of the following means:

- **Transport Layer Security** - A Transport Layer Security settings page that you can access from the PowerStore Manager (click **Settings** and, under **Security**, select **Transport Layer Security**).
- REST API server - Application interface that can receive REST API requests to configure Transport Layer Security settings. For more information about the REST API, see the *PowerStore REST API Reference Guide*.

Use either of these methods to enable or disable TLS 1.1 protocol support. To determine the status of Transport Layer Security in PowerStore Manager, click **Settings** and, under **Security**, select **Transport Layer Security**.

3

Auditing

This chapter contains the following information:

Topics:

- Auditing
- Remote logging

Auditing

Auditing provides a historical view of users activity on the system. A user with the role of Administrator, Security Administrator, or Storage Administrator can use the REST API to search for and view configuration change events on the system. These events that are audited are not just security related, all set operations (that is, POST/PATCH/DELETE) are audit logged.

Other interfaces such as the PowerStore Manager UI and the CLI can be used to search and view audit events.

Remote logging

The storage system supports sending audit log messages to a maximum of two hosts. The hosts must be accessible from the storage system. Audit log message transfers can use a one-way authentication (Server CA Certificates) or an optional two-way authentication (Mutual Authentication Certificate). An imported certificate applies to each remote syslog server that is configured to use TLS Encryption.

To review or update remote logging settings, log in to PowerStore Manager and click **Settings**, and under **Security** select **Remote Logging**.

The following information appears on the **Remote Logging** page for Remote Syslog Servers:

- Disabled or Enabled - Status of the sending log information to a remote host.
- Host IP address - Where the storage system sends remote log information.
- Port number and protocol (UDP or TCP) - The storage system transfers audit log information through port 514 using the UDP protocol or port 1468 using the TCP protocol.
- Use certificate - A Server CA Certificate for one-way authentication with your remote syslog server is required to be imported for remote syslog servers that are configured to use TLS Encryption.
- Audit Types - Types of audit events to send to the remote syslog server. The following types of audit events can be selected to be sent to the remote syslog server:
  - Authentication
  - Authorization
  - Config (Configuration)
  - Logout
  - System

The following information appears on the **Remote Logging** page for certificates:

- Service - Remote Logging
- Type - Server CA Certificate or Mutual Authentication Certificate
- Scope - Remote Logging
- Issued by - Authority issuing the certificate
- Valid - Indicates whether the certificate is valid for use
- Valid to - Expiry date of the certificate
- Issued to - Entity receiving the certificate

Configuring a remote syslog server to receive storage system log messages

Before configuring remote logging for a storage system, you must configure each remote system to receive logging messages from the storage system. A root or administrator on the receiving system can configure the remote syslog server or rsyslog server to receive log information by editing the syslog server or rsyslog server configuration file (syslogng.conf or rsyslog.conf) on the remote system.

ⓘ **NOTE:** For more information about setting up and running a remote syslog server, see the documentation for the operating system running on the remote system.

Add Remote Syslog Server

Prerequisites

Before adding a remote syslog server, ensure that you have obtained the following remote syslog server details:

- Host/IP address
- Protocol to use
- Whether TLS encryption is used
- Audit types to send

If log message transfers use TLS encryption and a Server Certificate Authority (CA) Certificate has not been imported, import the Server CA Certificate to PowerStore. The Server CA Certificate is required for TLS encryption.

If log message transfers use optional two-way authentication and a signed Mutual Authentication Certificate (Client CA Certificate) has not been imported, import the signed Mutual Authentication Certificate to PowerStore.

ⓘ **NOTE:** To acquire a signed Mutual Authentication Certificate for import, a Certificate Signing Request (CSR) must be generated for it and signed by your certificate authority before it can be imported to PowerStore.

About this task

To add a Remote Syslog Server using the PowerStore Manager, do the following:

Steps

1. Click **Settings** and under **Security** select **Remote Logging**.
   The **Remote logging** page appears.
2. Under **Remote Syslog Servers**, select **Add**.
   The **Add Remote Syslog Servers** slide out appears.
3. If not enabled, select **Enable remote logging**.
4. Type in the host IP address of the syslog server.
5. Select the **Protocol Type** and **Port**.

   ⓘ **NOTE:** The corresponding default port for UDP is 514. The corresponding default port for TCP is 1468.

6. If TLS encryption will be used, select **Use certificates (TLS encryption)**.

   ⓘ **NOTE:** TLS encryption is only allowed with the TCP protocol and when a valid signed server certificate has already been imported.

7. Under Audit Event Types, select the events that should be sent to the syslog server.
8. Click **Add**.
   The syslog server is added to the list of servers under **Remote Sysyslog Servers**.
9. (Optional) Select **Send Test Message** to verify the connection between PowerStore and the remote syslog server.
   The **Send Test Message** slide out appears.
10. (Optional) Type your test message in the **Message** box.
11. (Optional) Click **Send**.
    The **Send Test Message** slide out closes.

Import a certificate for remote logging

Prerequisites

Before importing a certificate, ensure that you know the location of the certificate file or have the certificate text available to copy and paste for import.

About this task

To import a certificate using the PowerStore Manager, do the following:

Steps

1. Click **Settings** and under **Security** select **Remote Logging**.
   The **Remote logging** page appears.
2. Under **Certificates**, select **Import** and select the type of certificate to import.
   The slide out for the respective certificate appears.
3. Do one of the following:
   - Select **Select Certificate File**, then locate and select the file to import.
   - Select **Paste Certificate File**, then copy and paste the certificate text in the text box.
4. Select **Import**.
   The certificate should appear in the list under **Certificates**.

Generate a Certificate Signing Request

Prerequisites

Before you generate a Certificate Signing Request (CSR), ensure that you have obtained the following information for the request:

- Common Name
- IP address
- DNS Name
- Organization
- Organization Unit
- Locality
- State
- Country
- Key Length
- (Optional) Passphrase

About this task

Generating a CSR is applicable to a Mutual Authentication Certificate, which is used in two-way authentication between PowerStore and the remote syslog server. To generate a CSR using the PowerStore Manager, do the following:

Steps

1. Select **Settings** and under **Security** select **Remote Logging**.
   The **Remote logging** page appears.
2. Select **Generate CSR**.
   The **Generate CSR** slide out appears.
3. Type in the information that is used to generate the CSR.
4. Click **Generate**.
   The **Generate CSR** slide out changes to show the next steps that must be taken along with the certificate text.
5. Click **Copy to clipboard** to copy the certificate text to your clipboard.
6. Click **Close**.
7. Have the certificate signed by the certificate authority (CA) so that it can be imported as a Mutual Authentication Certificate.

Manage remote logging settings

About this task

You can change the configuration settings of the remote syslog servers, delete remote syslog servers, and send a test message to a remote syslog server. You can also import either a Server CA Certificate for one-way authentication or an optional Mutual Authentication Certificate for two-way authentication, delete a certificate, and generate a Certificate Signing Request (CSR).

Steps

1. In PowerStore Manager, select **Settings** and, under **Security**, select **Remote Logging**.
   The **Remote Logging** page appears and lists information about remote syslog servers and associated certificates for authentication.
2. To modify the configuration settings of a remote syslog server, select the checkbox next to the hostname or IP address of the remote syslog server and click:

Option	Description
Modify	The **Modify Remote Syslog Server** slide-out appears. Change the remote syslog server settings as needed and click **Apply**. ⓘ **NOTE:** Using TLS Encryption requires a Server CA Certificate to be imported.
Delete	To delete the remote syslog server. ⓘ **NOTE:** To delete multiple remote syslog servers at one time, click the checkbox next to the hostname or IP address of each remote syslog server to be deleted, then click **Delete**.
Send Test Message	To send a test message to verify the connection between the PowerStore cluster and the remote syslog server. Sending a test message can only be performed on a single remote syslog server.

3. For certificates, click:

Option	Description
Import	Select whether to import a Server CA Certificate for one-way authentication or an optional Mutual Authentication Certificate for two-way authentication. Depending on the type of certificate selected to import, either the **Import Server CA Certificate** or **Import Mutual Authentication Certificate** slide-out appears. ⓘ **NOTE:** For either type of certificate, you have the options either to select a certificate file to import or copy and paste the certificate text to import. A certificate that is imported applies to each remote syslog server that is configured to use TLS Encryption. ⚠ **CAUTION: Importing a new CA Certificate will replace the existing certificate that is used by the PowerStore cluster.**
Delete	To delete a selected certificate. ⓘ **NOTE:** Deleting the Server CA Certificate prevents enabling TLS Encryption between the PowerStore cluster and your remote syslog server.
Generate CSR	The **Generate CSR** slide-out appears. Provide the information that is needed for generating a CSR. Once the CSR is generated and appears in the slide-out, copy the certificate text to your clipboard, then have the certificate signed by the certificate authority (CA). Import the signed certificate to PowerStore. A CSR can be signed by your CA and imported into PowerStore as a Mutual Authentication Certificate.

4

Data security settings

This section contains the following topics:

Topics:

- Data at Rest Encryption
- Encryption activation
- Encryption status
- Key management
- Keystore backup file
- Repurpose a drive in an appliance with encryption enabled
- Replacing a base enclosure and nodes from a system with encryption enabled
- Resetting an appliance to factory settings

Data at Rest Encryption

Data at Rest Encryption (D@RE) in PowerStore utilizes FIPS 140-2 validated Self-Encrypting Drives (SEDs) by respective drive vendors for primary storage (NVMe SSD, NVMe SCM and SAS SSD). The NVRAM caching device is encrypted but not FIPS 140-2 validated at this time.

Encryption is performed within each drive before the data is written to the media. This protects the data on the drive against theft or loss and attempts to read the drive directly by physically de-constructing the drive. The encryption also provides a means to quickly and securely erase information on a drive to ensure that the information is not recoverable. In addition to protecting against threats related to physical removal of media, you can readily repurpose media by destroying the encryption key used for securing the data previously stored on that media.

Reading encrypted data requires the authentication key for the SED to unlock the drive. Only authenticated SEDs will be unlocked and accessible. Once the drive is unlocked, the SED decrypts the encrypted data back to its original form.

The PowerStore appliance must contain all SEDs. If you try to add a non-self-encrypting drive to an appliance, the appliance raises an error. Also, having un-encrypted appliances in an encrypted cluster is not supported.

Encryption activation

The Data at Rest Encryption feature on PowerStore appliances is set at the factory. In all countries that allow the import of an appliance that supports encryption, encryption is enabled by default. When enabled, encryption cannot be disabled. In all countries that do not allow the import of an appliance that supports encryption, the Data at Rest Encryption feature is disabled.

ⓘ **NOTE:** Appliances that do not support data at rest encryption are not allowed to cluster with encrypted appliances.

Encryption status

Encryption status for an appliance is reported at the following levels:

- Cluster level
- Appliance level
- Drive level

Cluster level encryption status simply reflects whether an appliance is encryption enabled. It is not related to drive status.

Encryption status of an appliance appears as one of the following:

- Encrypted – Encryption capability is enabled on the appliance.

- Unencrypted – Encryption capability is not supported on the appliance.

Drive level encryption status is provided for each drive in an appliance and appears as one of the following:

- Encrypted – The drive is encrypted. This is the typical state of a drive in an appliance that is encryption capable.
- Processing – The appliance is enabling encryption on the drive. This status can be seen during the initial activation of encryption on an appliance or during the addition of new drives to a configured appliance.
- Disabled – The drive cannot have encryption enabled due to country specific import restrictions. If any drives report this status, then all drives in the cluster will also report the same status.
- Not Supported – The drive does not support encryption.
- Foreign – The drive is supported, but has been locked by another appliance. It needs to be decommissioned before it can be used.

Key management

An embedded key manager service (KMS) runs on the active node of each PowerStore appliance. This service manages the local keystore file lockbox storage to support automatic encryption key backup to system and boot drives. It also controls the Self-Encrypting Drive (SED) lock and unlock process on the appliance and is responsible for managing the local keystore content for the appliance. The local keystore file is encrypted with a 256-bit AES key and the keystore file lockbox storage leverages RSA's BSAFE technology.

The KMS automatically generates a random authentication key for SEDs during the initialization of the appliance. Each drive has a unique authentication key, including those that are added to the appliance later on, that is used in the SED lock and unlock processes. A key encryption key encrypts authentication and encryption keys in the keystore file storage and in flight within the appliance. Media encryption keys are stored on the dedicated hardware of the SEDs and cannot be accessed. When encryption is enabled, all the authentication keys are stored within the appliance.

Keystore backup file

The KMS supports the creation and download of an off-appliance backup of the keystore archive file. The off-appliance backup reduces the chances of a catastrophic key loss, which would render an appliance or cluster unusable. If a particular appliance is unavailable when a cluster keystore backup is initiated, the overall operation will succeed, but a warning is issued that the backup does not contain keystore files for all appliances in the cluster and that the operation should be retried when the offline appliance is available.

ⓘ **NOTE:** The primary appliance in a cluster contains a cluster keystore archive file that contains a copy of keystore backups from each appliance that is discovered in the cluster, including the primary appliance.

When changes to the configuration of a system within the cluster occur that result in changes to the keystore, it is recommended that you generate a new keystore archive file for download. Only one backup download operation of the keystore archive file can be run at a time.

ⓘ **NOTE:** It is strongly recommended that you download the generated keystore archive file to an external, secure location. If the keystore files on a system become corrupted and inaccessible, that system will enter service mode. In this case, the keystore archive file and a service engagement are required for resolution.

A user role of Administrator or Storage Administrator is required to back up the keystore archive file. To back up the keystore archive file, click **Settings** and under **Security** select **Encryption**. On the **Encryption** page under **Lockbox backup**, click **Download Keystore Backup**.

ⓘ **NOTE:** To restore the keystore backup in case of a failure, contact your service provider.

Repurpose a drive in an appliance with encryption enabled

A self-encrypting drive (SED) is locked when an appliance is initialized or when it is inserted into an already initialized appliance.

About this task

The drive cannot be used in another system without first being unlocked. The locked drive becomes unusable when it is inserted into a different appliance and its encryption status appears as `Foreign` in the new appliance. The drive can be repurposed for the new appliance, however, all the existing data on the drive will be lost.

To repurpose a drive having an encryption status of `Foreign` on an appliance, do the following:

Steps

1. Record the Physical Security ID (PSID) that is on the label on the back of the drive. The PSID must be provided as part of the repurposing process.
2. In PowerStore Manager, select **Hardware**, and select the appliance with the drive to repurpose on the **Appliances** tab.
3. On the **Appliance Details** page, select the **Components** card.
4. On the **Drives** tab, expand the enclosure with the drive to repurpose and select the drive.

   The **Encryption Status** for the drive should appear as `Foreign`.
5. Click **Repurpose Drive**.
   The **Repurpose Drive** slide-out panel appears.
6. Type the PSID of the drive and click **Apply**.

Results

The drive is repurposed in the appliance as a new drive and its encryption status changes to `Encrypted` when the repurpose process completes.

Replacing a base enclosure and nodes from a system with encryption enabled

A service engagement is required to replace a base enclosure and nodes from an appliance with encryption enabled.

Resetting an appliance to factory settings

A service script, `svc_factory_reset`, returns a single appliance cluster back to its factory-delivered state, deleting all user data and persistent configurations.

For multi appliance clusters, `svc_factory_reset` cannot be run on the secondary appliances. The service script `svc_remove_appliance` must be run instead. This script returns a secondary appliance to its factory-delivered state, deleting all user data and persistent configurations. When only the primary appliance remains in the cluster, you can run `svc_factory_reset` to reset that appliance.

ⓘ **NOTE:** It is recommended that these scripts be run by only a qualified service provider.

For more information about these scripts, refer to the *PowerStore Service Scripts Guide*.

5

Secure serviceability settings

This chapter contains the following information:

Topics:

- Operational description of SupportAssist
- SupportAssist options
- SupportAssist Connect via Gateway option
- SupportAssist Connect Directly option
- Requirements for SupportAssist Connect via Gateway
- Requirements for SupportAssist Connect Directly
- Configuring SupportAssist
- Configure SupportAssist
- CloudIQ
- Cybersecurity

Operational description of SupportAssist

SupportAssist is a secure support technology that takes the guesswork out of issue prevention and resolution through remote monitoring and management to:

- Collect system state information and telemetry.
- Automate issue detection and support case creation.
- Resolve common issues remotely.
- Provide critical information to Dell EMC remote support to resolve complex issues.

> **NOTE:** It is strongly recommended that you enable the SupportAssist feature to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. If you do not enable the SupportAssist feature, you may need to collect appliance information manually to assist Dell EMC Support with troubleshooting and resolving problems with your appliance. Also, the SupportAssist feature must be enabled on the appliance for data to be sent to CloudIQ and to enable use of the Cybersecurity application. For information about CloudIQ and the Cybersecurity application, go to https://www.dell.com/support. After logging in, locate the CloudIQ **Product Support** page.

SupportAssist and security

SupportAssist employs multiple security layers throughout each step in the remote connectivity process to ensure that you and Dell EMC can use the solution with confidence:

- All notifications to Dell EMC originate from your site – never from an outside source – and are kept secure through the use of Advanced Encryption Standard (AES)-256 bit encryption.
- IP-based architecture integrates with your existing infrastructure and maintains the security of your environment.
- Communications between your site and Dell EMC are bilaterally authenticated using RSA® digital certificates.
- Supports TLS 1.2
- Only authorized Dell EMC Customer Service professionals verified through two-factor authentication can download the digital certificates needed to view a notification from your site.

SupportAssist management

You can manage SupportAssist using the PowerStore Manager or the REST API. You can enable or disable the service and provide the relevant information necessary for the SupportAssist options you select.

SupportAssist communication

SupportAssist cannot be enabled on PowerStore models configured with IPv6 for the management network. SupportAssist is not supported over IPv6. Also, management network reconfiguration from IPv4 to IPv6 is not allowed when SupportAssist is configured on a cluster.

ⓘ **NOTE:** Access to a DNS server is required for SupportAssist to work.

The **Connection Status** of SupportAssist indicates both the state of the connection between PowerStore and the Dell EMC backend Support services and the quality of service of the connection. The connection state is determined over five minute periods and the quality of service of the connection is determined over 24 hour periods. The **Connection Status** of the connection can appear as one of the following based on any of the appliances in the cluster:

- `Unavailable` – Connectivity data is unavailable. You may have lost contact with an appliance or SupportAssist has just been enabled and there is insufficient data to determine the state.
- `Disabled` – SupportAssist has not been enabled.
- `Not connected` – Connectivity has been lost. Five consecutive keepalive failures have been detected.
- `Reconnecting` – PowerStore is attempting to reconnect after loss of connectivity. Five consecutive successful keepalive requests are needed to transition back to a connected status.

The **Connection Status** of the connection can appear as one of the following based on the average of all the appliances in the cluster when PowerStore is connected to the Dell EMC backend Support services:

- `Evaluating` – The quality of service for the connection will be undetermined for the first 10 minutes after SupportAssist is first initialized.
- `Good` – 80% or more of the consecutive keepalive requests were successful.
- `Fair` – Between 50% and 80% of the consecutive keepalive requests were successful.
- `Poor` – Less than 50% of the consecutive keepalive requests were successful.

SupportAssist remote support

SupportAssist and its remote support features are disabled by default. As part of the enabling of SupportAssist and to use its remote support services, you must accept the Dell EMC End User License Agreement (EULA). Otherwise, SupportAssist cannot be enabled and its remote support features cannot be used. Once the SupportAssist EULA is accepted, SupportAssist and its remote support features can be configured.

Enabling the SupportAssist Remote Support feature allows support engineers who are authorized by Dell EMC to securely access and troubleshoot your system. When the Remote Support feature is enabled without enabling the associated Remote Secure Credentials feature, support personnel must engage with you to get access to your system after an event has occurred. Enabling the Remote Secure Credentials feature allows Dell EMC support personnel to remotely log in to the system to address issues that may occur. Support personnel can remotely log in to your system through SSH or PowerStore Manager. Your support contract determines what and when support personnel are allowed to do. By enabling this feature, you grant access to your system so that troubleshooting and fixing issues can happen as they occur. For example, if a call home, data unavailable or loss, or any otherwise abnormal event occurs, this feature allows Dell EMC service personnel to respond faster to correct issues.

Enabling or disabling the Remote Secure Credentials feature is a cluster-wide operation. An audit event is created anytime the Remote Secure Credentials feature is enabled or disabled. Disabling the Remote Secure Credentials feature does not downgrade your level of service or disable SupportAssist.

SupportAssist options

The SupportAssist connection options that are available by which to send appliance information to Dell EMC Support for remote troubleshooting are:

- **Connect via Gateway Server** – For centralized SupportAssist and runs on a customer-supplied gateway server with two-way file transfer, which includes:
  - Call-homes
  - CloudIQ and Cybersecurity support
  - Software notifications
  - Operating environment and firmware download from Dell EMC Support to the cluster

  It also includes remote access for Dell EMC Support personnel. The SupportAssist gateway server is the single point of entry and exit for all IP-based SupportAssist activities for the appliances associated with the gateway.

- **Connect Directly** — For distributed SupportAssist that runs on individual appliances with the same two-way file transfer as connecting through a SupportAssist gateway server.

Another option, Disabled, is available but not recommended. If you select this option, Dell EMC Support will not receive notifications about issues with the appliance. You may need to collect appliance information manually to assist support representatives with troubleshooting and resolving problems with the appliance.

SupportAssist Connect via Gateway option

When you select the **Connect via Gateway** option, your appliance is added to other appliances in a SupportAssist cluster. The cluster resides behind a single common (centralized) secure connection between Dell EMC Support servers and an off-array gateway server. The gateway server is the single point of entry and exit for all IP-based Dell EMC SupportAssist activities for the appliances associated with the gateway.

The gateway server is a remote support solution application that is installed on one or more customer-supplied dedicated servers. The **Connect via Gateway** option supports up to two gateway servers, one as primary and one as a backup. The gateway server functions as a communication broker between the associated appliances and the Dell EMC enterprise.

To configure your appliance to use the **Connect via Gateway** option for SupportAssist, you need to provide the IP address and port number (9443 is the default) for each gateway server. Also, ensure that the port is open between the gateway server and the appliance.

NOTE: The gateway server must be up and running before you configure your appliance to use it. Appliances can only be added to the gateway from the PowerStore Manager. If the appliance is added from the gateway server, it will appear to be connected, but will not successfully send system information.

For more information about the SupportAssist Gateway, access the SupportAssist product page on the Dell Support website (https://www.dell.com/support).

SupportAssist Connect Directly option

For the **Connect Directly** option, SupportAssist runs directly on the primary node of each appliance. In a cluster, each appliance establishes its own connection to Dell EMC Support. Traffic is not routed through the primary appliance in a cluster. However, SupportAssist can only be managed at the cluster level, that is, all changes are applied to every appliance in the cluster.

Enable and configure the **Connect Directly** option from the **Support Assist** page, which can be accessed through **Settings** and is listed under **Support** in the PowerStore Manager. These actions set up the appliance to use a secure connection between itself and Dell EMC Support.

When you select the **Connect Directly** option and accept the End User License Agreement (EULA), the appliance sets up a secure connection between itself and Dell EMC Support. This option enables remote access service connectivity capability with the appliance to and from Dell EMC Support along with two-way file transfer. If applicable, you can configure the connection from the appliance to an associated proxy server (optional).

When a new appliance is added to an existing cluster, the new appliance will detect the cluster SupportAssist settings and automatically configure the new appliance to match. If the Connect Directly option is currently enabled, it will be automatically enabled on the new appliance. Additional actions are not necessary. If Connect Directly option cannot be enabled, it will not prevent the add-appliance process from completing.

Requirements for SupportAssist Connect via Gateway

The following requirements are applicable to the **Connect via Gateway** SupportAssist implementation:

- Network traffic (HTTPS) must be permitted on port 9443 (or customer specified port, if different) between the appliance and the SupportAssist Gateway server. Also, allow access to ports 22, 443, and 8443 between PowerStore and the SupportAssist Gateway server for PowerStore Manager and SSH accessing.
- The SupportAssist Gateway server must be version 4.0.5.3 or version 3.38 and above.
- Ensure that the PowerStore cluster is running PowerStore OS version 1.0.1.0.5.002 or higher.

NOTE: Never manually add or remove an appliance from the gateway server. Only add or remove an appliance from the PowerStore Manager SupportAssist configuration wizard.

Requirements for SupportAssist Connect Directly

The following requirement is applicable to the **Connect Directly** SupportAssist implementation:

- Network traffic (HTTPS) must be permitted on ports 443 and 8443 (outbound) to Dell EMC Support. Failure to open port 8443 results in significant performance impact (30–45 percent). Failure to open both ports may result in a delay in resolving issues with the end device.

Configuring SupportAssist

Configure SupportAssist for an appliance by using any of the following means:

- Initial Configuration wizard – A user interface that walks you through the initial set up of PowerStore Manager and prepares the system for use.
- **SupportAssist** – A settings page that you can access from the PowerStore Manager (click **Settings** and under **Support** select **SupportAssist**).
- REST API server – Application interface that can receive REST API requests to configure SupportAssist settings. For more information about the REST API, see the PowerStore REST API Reference Guide.

To determine the status of the SupportAssist feature, click **Settings** and under **Support** select **SupportAssist** in the PowerStore Manager.

Configure SupportAssist

About this task

To configure SupportAssist using the PowerStore Manager, do the following:

Steps

1. Click **Settings** and under **Support** select **SupportAssist**.
2. If the status of SupportAssist is shown as `Disabled`, click the **SupportAssist** control icon to begin enabling SupportAssist. The Dell EMC End User License Agreement (EULA) appears.
3. Click **Accept** to accept the EULA and enable SupportAssist.

   Although SupportAssist can be disabled, it is not recommended. Also, if the EULA is not accepted, SupportAssist cannot be enabled.

   The **Enabled/Disabled** control should move to the right and change its indication to `Enabled`. However, the connection status will not change until after you enter the necessary configuration information and click **Apply**.
4. Select the **Type** of SupportAssist option you intend to use from the list.
5. Depending on which type of SupportAssist option you select, do one of the following:
   - For the **Connect via Gateway** option:
     - Specify the IP address of each gateway server, the primary server and, if available, the backup server.

       ⓘ **NOTE:** Each gateway server must be up and running before you configure your appliance to use it.
     - If the port that will be used to connect to the gateway server is different than the default (9443), use the controls to select the number of the port that will be used in your network.
   - For the **Connect Directly** option:
     - If your network connection uses a proxy server, specify the IP address of the proxy server.

       ⓘ **NOTE:** The proxy server must be up and running before you configure your appliance to use it.
     - Use the controls to select the number of the port that will be used to connect to the proxy server in your network.
6. Depending on which type of SupportAssist option you select, do one of the following:
   - For the **Connect Directly** option, go to the next step.
   - For the **Connect via Gateway** option, select **Test Connection** for each configured gateway server to check the status of the connection to the gateway server.

   ⓘ **NOTE:** If the Connectivity Status appears to remain as `Transitioning` and does not change after several minutes (the time it should take to test connectivity), contact Online Support.

7. Select **Send Test Alert** to send a test alert to Dell EMC Support to ensure end-to-end connectivity.
8. The **Connect to CloudIQ** checkbox is selected by default; if you do not want to send files to CloudIQ and be able to use the Cybersecurity application, clear the checkbox; otherwise, leave the checkbox selected.
9. The **Remote Support** checkbox is selected by default; if you do not want to allow support engineers authorized by Dell EMC to securely troubleshoot your system, clear the checkbox; otherwise, leave the checkbox selected.
10. The **Remote Secure Credentials** checkbox is not selected by default; if you want to allow authorized Dell EMC service personnel to authenticate to your system, select the checkbox; otherwise, leave the checkbox unselected.
11. Select **Apply** to retain the SupportAssist configuration information.
12. Select **Support Contacts** and ensure the contact information that is entered is accurate. Correct any information that appears incorrect or outdated.

    Your SupportAssist contact information is critical for quick response to support issues and must be accurate and current.
13. Select **Apply** to retain the SupportAssist configuration information.

CloudIQ

ⓘ **NOTE:** SupportAssist must be enabled on the storage system to connect and send data to CloudIQ.

CloudIQ is a Dell EMC-hosted service that uses data (logs, system configuration, alerts, performance metrics, and capacity metrics and capacity forecast data) that is collected by SupportAssist to allow users to monitor performance in near real-time and utilization and health time across multiple PowerStore clusters and perform basic service actions. The CloudIQ interface is accessible through a web browser at any time and from any location. CloudIQ provides dashboard views of all connected clusters, showing key information such as performance and capacity trending and predictions. CloudIQ also provides proactive serviceability that informs the user about issues before they occur and provides the user with simple, guided remediation.

Users can enable CloudIQ during the configuration process for SupportAssist implementation. CloudIQ support is enabled by default when any SupportAssist option is enabled. When SupportAssist and CloudIQ are both enabled, CloudIQ can be launched from any PowerStore Manager page and is constantly visible. On the CloudIQ.emc.com page, users can log in with their valid service credentials to view their PowerStore clusters in CloudIQ.

ⓘ **NOTE:** Once CloudIQ is enabled, it is possible to disable SupportAssist without changing the CloudIQ setting. Without SupportAssist, data is not collected and sent to CloudIQ, but if SupportAssist is re-enabled, the system remembers the CloudIQ setting and immediately resumes sending data to CloudIQ. Disabling CloudIQ support does not disable the transfer of service related telemetry, that is, call-homes and data proactive collections provided by SupportAssist.

Cybersecurity

ⓘ **NOTE:** SupportAssist and CloudIQ must be enabled on the storage system to enable use of the Cybersecurity application.

Cybersecurity is a software as a service cloud-based storage security analytics application that provides security assessment and measures the overall cyber security risk level of storage systems using intelligent, comprehensive and predictive analytics. Cybersecurity uses SupportAssist to collect system logs, system configurations, security configurations and settings, alerts, and performance metrics from your PowerStore system.

6

Security Alert Settings

This chapter describes the different methods available to notify administrators of alerts that occur on a PowerStore cluster.

Topics:

- Alert settings

Alert settings

PowerStore alerts inform administrators of actionable events that occur on the PowerStore cluster. These alerts can be reported as shown in the following table.

Table 8. Alert settings

Alert notification type	Description
Visual notification	PowerStore Manager displays informational messages when users log in to the interface and in real time to indicate when alert conditions occur. These messages provide basic information about the alert condition. ⓘ **NOTE:** PowerStore visual alert notifications are not configurable.
Email notification	Enables you to specify one or more email addresses to which to send alert messages. You can configure the following settings: ● Email addresses to which to send storage system alerts. ● Severity level (Critical, Major, Minor, and Info) required for email notification. ⓘ **NOTE:** For PowerStore alert email notification to work, you must configure a target SMTP server for the PowerStore cluster. PowerStore does not have an option of authentication to an SMTP mail server. If your mail server requires all clients to authenticate to relay an email, PowerStore cannot send email alerts through that mail server.
SNMP traps	Transfer alert information to designated SNMP Managers (trap destinations) that act as repositories for generated alert information by the PowerStore cluster. You can configure the following settings: ● Network Name or IP address of a network SNMP Manager ● Port number. ⓘ **NOTE:** The default port set for SNMP is 162. Valid port values are 162 or between 1024–49151. ● Minimal Severity Level of Alerts: Notifications are sent for the configured severity level or higher. ● Version: Version used for SNMP traps (v2c or v3) ● Trap Community String: SNMP community string (applicable only to v2c SNMP destination) ● Security Level: Authentication security level (applicable only to a v3 SNMP destination) ● Username: Security Name of the SNMPv3 user sending the message (applicable only to a v3 SNMP destination) ● Password: Generated (applicable only to a v3 SNMP destination) ● Authentication protocol: Hashing algorithm used for SNMP traps (SHA or MD5) (applicable only to a v3 SNMP destination) ● Privacy protocol: Encryption algorithm used for SNMP traps (TDES or AES) (applicable only to a v3 SNMP destination)
SupportAssist	SupportAssist provides an IP-based connection that enables Dell Support to receive error files and alert messages from the PowerStore cluster, and to perform remote troubleshooting resulting in a fast and efficient time to resolution. ⓘ **NOTE:** For SupportAssist to work, you must enable it on the PowerStore cluster.

Table 8. Alert settings (continued)

Alert notification type	Description
CloudIQ	CloudIQ is a Dell EMC-hosted service that uses data (logs, system configuration, alerts, performance metrics, and capacity metrics and capacity forecast data) collected by SupportAssist to allow users to monitor performance in near real-time and utilization and health time across multiple PowerStore clusters and perform basic service actions. The CloudIQ interface is accessible through a web browser at any time and from any location. **NOTE:** SupportAssist must be enabled on the storage system to connect and send data to CloudIQ.

Configure email notifications

About this task

You can configure your system to send alert notifications through email using an SMTP server.

NOTE: For the storage system alert email mechanism to work, a target SMTP server must be configured for the storage system.

Using PowerStore Manager, do the following:

Steps

1. Select **Settings**, and then select **SMTP Server** under **Networking**.
2. To access the SMTP server settings, change the status to **Enabled**.
3. Add the SMTP server address and the email address that notifications should be sent from and click **Apply**.
4. Select **Settings**, and then select **Email Notifications** under **Users**.
5. To add email recipients, click **Add** under **Email Subscribers**.
6. Type the email address that you want to send alert notifications to. When you add an address, you can select the severity level of the alert notifications that are sent to that address. (Optional) To verify whether email addresses are entered correctly, select the target email addresses, and then click **Sent Test Email**.

Configure SNMP

About this task

You can configure your system to send alert information to up to 10 designated SNMP Managers (trap destinations).

NOTE: Only notifications are supported.

The authoritative **Local Engine ID** used for SNMPv3 messages is given as a hexadecimal string. It is discovered and added automatically.

NOTE: To verify the **Local Engine ID** select **Settings**, and under **Networking**, select **SNMP**. The **Local Engine ID** appears under **Details**.

Using PowerStore Manager, do the following:

Steps

1. Select **Settings** and, under **Networking**, select **SNMP**.
   The **SNMP** card appears.
2. To add an SNMP Manager, click **Add** under **SNMP Managers**.
   The **Add SNMP Manager** slide out appears.
3. Depending on the version of SNMP, configure the following information for the SNMP Manager:
   - For SNMPv2c:
     - Network Name or IP address
     - Port
     - Minimal Severity Level of Alerts

    - Version
    - Trap Community String
- For SNMPv3
    - Network Name or IP address
    - Port
    - Minimal Severity Level of Alerts
    - Version
    - Security Level

        ⓘ **NOTE:** Depending on the security level selected, additional fields appear.

        - For the level None, only **Username** appears.
        - For the level **Authentication only**, **Password** and **Authentication Protocol** appear along with **Username**.
        - For the level **Authentication and privacy**, **Password**, **Authentication Protocol**, and **Privacy Protocol** appear along with **Username**.
    - Username

        ⓘ **NOTE:** When the Security Level of **None** is selected, the username must be NULL. When a Security Level of **Authentication only** or **Authentication and privacy** is selected, the username is the Security Name of the SNMPv3 user sending the message. The SNMP username can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
    - Password

        ⓘ **NOTE:** When a Security Level of either **Authentication only** or **Authentication and privacy** is selected, the system determines the password.
    - Authentication Protocol

        ⓘ **NOTE:** When a Security Level of either **Authentication only** or **Authentication and privacy** is selected, select either **MD5** or **SHA256**.
    - Privacy Protocol

        ⓘ **NOTE:** When a Security Level of **Authentication and privacy** is selected, select either **AES256** or **TDES**.

4. Click **Add**.
5. (Optional) To verify whether SNMP Manager destinations can be reached and the correct information is received, click **Sent Test SNMP Trap**.

A

TLS cipher suites

This appendix contains the following information:

Topics:

- Supported TLS cipher suites

Supported TLS cipher suites

A cipher suite defines a set of technologies to secure your TLS communications:

- Key exchange algorithm (how the secret key used to encrypt the data is communicated from the client to the server). Examples: RSA key or Diffie-Hellman (DH)
- Authentication method (how hosts can authenticate the identity of remote hosts). Examples: RSA certificate, DSS certificate, or no authentication
- Encryption cipher (how to encrypt data). Examples: AES (256 or 128 bits)
- Hash algorithm (ensuring data by providing a way to determine if data has been modified). Examples: SHA-2 or SHA-1

The supported cipher suites combine all these items.

ⓘ **NOTE:** Security is improved in PowerStore version 2.0.x with the removal of weak ciphers, such as those starting with TLS_RSA_. For example, TLS_RSA_WITH_AES_128_CBC_SHA is not supported.

The following list gives the OpenSSL names of the TLS cipher suites for the appliance and the associated ports.

Table 9. Default/Supported TLS cipher suites supported on the appliance

Cipher Suites	Protocols	Ports
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	443, 8443

The following list gives the OpenSSL names of the additional TLS cipher suites for the appliance and the associated ports when TLS 1.1 is enabled.

Table 10. Additional TLS cipher suites supported on the appliance when TLS 1.1 is enabled

Cipher Suites	Protocols	Ports
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.1	443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.1	443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.1	443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.1	443

B

Directory Services

This appendix describes how to configure PowerStore to connect to an LDAP server for authentication, and how to assign roles to LDAP users and groups.

Topics:

- Configuring Directory Services
- Configure LDAP server
- Configure LDAP account

Configuring Directory Services

The Lightweight Directory Access Protocol (LDAP), is an application protocol for querying and modifying directory services running on TCP/IP networks. LDAP helps centralize the management of network authentication and authorization operations. Integrating PowerStore Manager users into an existing LDAP environment provides a way to control management access based on established user and group accounts within the LDAP directory.

PowerStore supports the following LDAP server types:

- Active Directory—a Microsoft directory service. It runs on Windows Server and allows administrators to manage permissions and access to network resources.
- OpenLDAP—a free, open-source implementation of LDAP.

Networked entities that exchange data use certificates to authenticate each other. For secure communications to occur between two networked entities, one entity must trust (accept) the certificate from the other. PowerStore Manager uses the SSL/TLS and the X.509 certificate standard to secure client (storage system) and server (LDAP) communications. PowerStore requires the certificate chain file to be uploaded, to properly verify the server certificate received from the LDAP server when the TLS session is established.

After you configure the LDAP settings for PowerStore, you can perform user management functions. For example, you can assign access permissions to PowerStore Manager based on existing users and groups, within the context of an established LDAP directory structure.

Follow this sequence of steps to configure LDAP on PowerStore:

1. Configure the LDAP server.
2. Verify the LDAP server connection.
3. (Optional) Configure LDAPS for the LDAP server.
4. (Optional) Verify the LDAP server connection using the LDAPS protocol.
5. Configure LDAP Users and Groups.

NOTE: The PowerStore Manager Online Help provides more information about LDAP and the steps to configure PowerStore to connect to an LDAP server, and how to assign roles to manage LDAP users and groups.

Configure LDAP server

About this task

LDAP server configuration consists of specifying the configuration information needed to connect to the LDAP server.

To configure LDAP, do the following:

Steps

1. In PowerStore Manager, select **Settings** in the top menu bar to display the **Settings** page.
2. In the left panel under **Users**, click **Directory Services**.

The **Directory Services** page appears.

3. The options that appear depend on whether LDAP has been configured. Do one of the following:
   - To configure LDAP for the first time, click **Configure LDAP**. Go to the next step.
   - To edit an existing LDAP configuration, click **Edit LDAP Configuration**. Go to the next step.
   - To delete an LDAP configuration, click **Delete LDAP Configuration**.

   When either **Configure LDAP** or **Edit LDAP Configuration** are selected, the **Directory Services** slide out panel appears. When **Delete LDAP Configuration** is selected, a confirmation dialog box appears that describes the effect of the delete operation. All data, including certificates and LDAP user/role settings, will also be deleted.
4. Under **LDAP Settings Server Type**, select the type of the LDAP authentication server.
5. Under **Servers**, do one of the following:
   - To manually add a server address, click **Configure IPs Manually**, enter the IP address and click **Add**.

     ⓘ **NOTE:** Only IP addresses are accepted, FQDN is not supported.
   - To remove a server address, select the address in the list box and click **Delete**.
   - To move an IP address up or down in the list, select the address in the text box and click **Up** or **Down**, respectively, as needed.
6. For **Domain Name** under **Domain Settings**, type the domain name of the LDAP authentication server.

   The domain name must be filled in when the LDAP server configuration is created. After that, it is grayed out because it cannot be changed without deleting and re-creating the LDAP server configuration.
7. For **Bind DN** (Distinguished Name), type the distinguished name of the LDAP user with administrator privileges.

   The distinguished name should be specified in one of the following formats:
   - (For AD and OpenLDAP) LDAP notation format (for example, **`cn=ldapbinduser,cn=Users,dc=mycompany,dc=com`**)
   - (For AD only) *<user>*@*<domain>* format (for example, **`ldapbinduser@mycompany.com`**)
8. For **Bind DN Password**, type the password for the user specified in **Bind DN**.
9. For **Timeout (secs)**, type the amount of time in seconds that will be allowed for the LDAP connection and query to occur.
10. For enabling Global Catalog for Active Directory, select **Global Catalog**.
    The port automatically sets to 3268 and the default value for **User ID Attribute** under **Advanced Settings** changes from `sAMAccountName` to `UserPrincipalName`.
11. The port for LDAP cannot be customized. The LDAP server uses one of the following default ports:
    - 389 for LDAP
    - 3268 for LDAP (global catalog)

    For example, `nsroot.net` instead of `nam.nsroot.net` using LDAP allows customers to query the entire AD forest (port 3268) instead of just the AD domain (TCP port 389). Also, AD role association is based on group scopes for Domain Local Groups and Universal Groups. This allows end-users to search the AD using an appropriate scope as needed and to avoid unnecessary group searches.

    ⓘ **NOTE:** It is strongly recommended that LDAP be configured and verified before configuring Secure LDAP (LDAPS). These actions will minimize any troubleshooting that may be necessary when enabling LDAPS.
12. Click **Advanced Settings** to list all the fields under **User Search Settings** and **Group Search Settings**. Verify the default values and, if necessary, make changes if required.

    For example, if the LDAP server has a different **Search Path** than the default `cn=Users,dc=` for either **User Search Settings** or **Group Search Settings**, or both, click **Advanced Settings** and update the search paths or other fields as necessary, then click **Apply** to save the advanced configuration changes.

    ⓘ **NOTE:** The default values that appear under **Advanced Settings** are based on the type of server as shown in the following list:
    - Active Directory server
      - **User Search Settings**:
        - **ID Attribute**: `sAMAccountName`
        - **Object Class**: `user`
        - **Search Path**: `cn=Users,dc=<domain>`
      - **Group Search Settings**:
        - **Member Attribute**: `member`
        - **ID Attribute**: `cn`

        - **Object Class**: `group`
        - **Search Path**: `cn=Users,dc=<domain>`
        - **Search Level**:
- Active Directory - Global Catalog server
    - **User Search Settings**:
        - **ID Attribute**: `UserPrincipalName`
        - **Object Class**: `user`
        - **Search Path**: (greyed out)
    - **Group Search Settings**:
        - **Member Attribute**: `member`
        - **ID Attribute**: `cn`
        - **Object Class**: `group`
        - **Search Path**: (greyed out)
        - **Search Level**:
- OpenLDAP server
    - **User Search Settings**:
        - **ID Attribute**: `uid`
        - **Object Class**: `inetOrgPerson`
        - **Search Path**:
    - **Group Search Settings**:
        - **Member Attribute**: `member`
        - **ID Attribute**: `cn`
        - **Object Class**: `groupOfNames`
        - **Search Path**:
        - **Search Level**:

13. Update the search paths or other fields as necessary, then click **Apply** to save the advanced configuration changes.

    For example, if you are configuring forest-level authentication, specify **`userPrincipalName`** in the **ID Attribute** field. If the LDAP server has a different search path than the default (cn=Users,dc=) for either users, groups, or both, update the search paths or other properties as necessary.
14. After all the LDAP configuration information is specified, click **Apply** to save the configuration.

Next steps

After the LDAP server configuration is saved and to avoid the possibility of data being unavailable, you must verify the configuration to confirm that the connections to the LDAP server will be successful.

Verify LDAP configuration

About this task

NOTE: To avoid the possibility of data being unavailable, you must verify the LDAP connection after every LDAP configuration change.

To verify connection to the LDAP server will be successful, do the following:

Steps

1. Click **Verify Connection** on the **Directory Services** page.
   If the configuration is valid, a connection will be established with the LDAP server and a green check mark along with the text **Connection Verified** will appear.
2. If the verification fails, the following steps are recommended to troubleshoot the failure:

a. Verify the **Directory Services** configuration information, in particular the **Distinguished Name** (user name), **Password**, and the **Server Address** (IP address).
b. Verify the LDAP server is online.
c. Verify there are no network issues; for example, firewall rules that would block access to the LDAP port, network router configuration that prevents the connection, and such.

Configure Secure LDAP

About this task

Configuring Secure LDAP (LDAPS) requires the following:

- Configure LDAPS protocol and the port
- Configure the certificate chain

When LDAPS is configured, PowerStore connects to the LDAP server using TLS. PowerStore requires the certificate chain file to be uploaded, to properly verify the server certificate received from the LDAP server when the TLS session is established.

PowerStore does not support DNS for LDAP. The LDAP server certificate must have IP addresses, as specified in the LDAP configuration, in the Subject or Subject Alternative Name field in the certificate. This is required to verify that the certificate is from the desired LDAP server.

The format of the certificate file to be uploaded is as follows:

- The certificate file must end in one of the following file extensions:
  - `.pem`
  - `.crt`
  - `.cer`
  - `.ca-bundle`

  Example: `LdapServerChain.crt`
- All certificates in the certificate file to be uploaded must be in PEM format. PEM formatted certificates are ASCII text that begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.
- If the LDAP server certificate is self-signed, only the server certificate is required.
- If the LDAP server certificate is signed by a Certificate Authority, then the certificate chain, up to the root certificate Authority, must be in the certificate file to be uploaded in the following order:
  1. Intermediate Certificate Authority certificate (if any).
  2. ...
  3. Root Certificate Authority certificate.
  4. If there are multiple certificates in the file to be uploaded, there must be a new line between each certificate.

To configure LDAPS, do the following:

Steps

1. Click **Edit LDAP Configuration**.
   The **Directory Services** slide out panel appears.
2. Under **Domain Settings**, select the **LDAP Secure (Use SSL)** checkbox.

   The port for LDAPS cannot be customized. The LDAP server uses one of the following default ports:
   - 636 for LDAPS
   - 3269 for LDAPS (global catalog)

   For example, `nsroot.net` instead of `nam.nsroot.net` using LDAPS allows customers to query the entire AD forest (port 3269) instead of just the AD domain (TCP port 636). Also, AD role association is based on group scopes for Domain Local Groups and Universal Groups. This allows end-users to search the AD using an appropriate scope as needed and to avoid unnecessary group searches.) Also, **Upload** for **LDAP Certificate** appears when the **LDAP Secure (Use SSL)** checkbox is selected.
3. Click **Upload**.
   The **Upload File** dialog box appears.
4. Click **Choose File**.
5. Browse to the desired certificate file, then select the file and click **Open**.
6. After the file upload completes, click **Apply** to save the configuration changes.

Next steps

You must verify the configuration after configuring LDAPS and uploading the server certificate file.

Verify LDAPS configuration

About this task

ⓘ **NOTE:** To avoid the possibility of data being unavailable, you must verify the LDAPS connection after every LDAPS configuration change.

To verify the LDAPS configuration, do the following:

Steps

1. Click **Verify Connection** on the **Directory Services** page.
   If the configuration is valid, a connection will be established with the LDAP server and a green check mark along with the text **Connection Verified** will appear.
2. If the verification fails, the following steps are recommended to troubleshoot the failure:
   a. Verify the **Directory Services** configuration information, in particular the port number.
   b. Verify the LDAP server is online and configured for LDAPS.
   c. Verify the certificates in the uploaded certificate file are valid, for example, not expired and in the correct order.
   d. Verify the configured **IP address** is in the Subject or Subject Alternative Name field in the LDAP server certificate.
   e. Verify there are no network issues; for example, firewall rules that would block access to the LDAPS port, and such.

Next steps

After the LDAP server is configured, one or more LDAP users or groups must be added to PowerStore to map the users (or groups) to roles. Otherwise, LDAP authentication will succeed on login, but the login will fail because no role could be assigned to the user.

Configure LDAP account

About this task

The procedure for creating an LDAP user or group account on PowerStore is similar. However, the LDAP group must also be created on the LDAP server, and LDAP users added as members of that group. The advantage of creating an LDAP group account is that all the users which are members of the added group get access to PowerStore with the privileges and role mapped to that group.

To create an LDAP user or group account, do the following:

ⓘ **NOTE:** LDAP server must be configured before an LDAP user or group account can be created.

Steps

1. In PowerStore Manager, click **Settings** in the top menu bar to display the **Settings** page.
2. In the left panel under **Users**, click **Users**.
   The **Powerstore Users** page appears.
3. Click **LDAP**.
   The LDAP account information appears.
4. Click **Add**.
   The **Add Account** slide out panel appears.
5. For **Type**, select the type of LDAP account, either User or Group.
6. For **Account Name**, type the user name that is listed in the LDAP server.

   ⓘ **NOTE:** The account name must be the value of the **ID Attribute** defined in **Advanced Settings** under **Domain Settings** on the **Directory Services** slide out panel. For example:

> - When **Global Catalog** (forest-level authentication) is selected while configuring the PowerStore LDAP server, the default value for **User ID Attribute** under **Advanced Settings** is `UserPrincipalName`. So the **Account Name** must be a UserPrincipalName which is unique, and the format is `username@DomainName.com`
> - When **Global Catalog** is not selected, the default value for the **User ID Attribute** under **Advanced Settings** is `sAMAccountName`. The **Account Name** must be an sAMAccountName.
> - When adding a group, the **Account Name** must be the value of the **Group ID Attribute** (example: `cn`)
>
> Also, the account name cannot include colon (:), backslash (\), slash (/) or at (@) characters.

7. For **Account Role**, select the role to assign to the account from the drop down list.
8. After verifying that the LDAP user or group name and the role are correct, click **Apply** to complete the transaction.
   The added LDAP user or group account appears in the list of accounts on the **PowerStore Users** page.
9. If the adding LDAP account operation fails, do the following to troubleshoot the failure:
   a. Verify the fields in **User Search Settings** under **Advanced Setting** are correct.
   b. Verify the fields in **Group Search Settings** under **Advanced Setting** are correct.
   c. Verify that the group search level is set properly.