

Dell PowerStore

Importing External Storage to PowerStore Guide

Version 4.1

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.

Additional Resources.....	6
Third-party content containing non-inclusive language.....	6
Chapter 1: Introduction.....	7
Importing block-based external storage to PowerStore overview.....	7
Non-disruptive import of external storage to PowerStore overview.....	7
Overview of the non-disruptive import process.....	8
Agentless import of external storage to PowerStore overview.....	9
Overview of the agentless import process.....	9
Importing file-based external storage to PowerStore overview.....	11
Overview of the file-based import process.....	12
PowerStore cluster fibre channel connectivity to source systems.....	14
Import security.....	15
Chapter 2: Import requirements and restrictions.....	17
General requirements for importing data.....	17
Dell EqualLogic PS Series specific requirements.....	18
Dell Compellent SC Series specific requirements.....	19
Dell Unity specific requirements.....	19
Dell VNX2 Series specific requirements.....	19
Dell XtremIO XI and X2 specific requirements.....	19
Dell PowerMax and VMAX3 specific requirements.....	19
NetApp AFF A-Series specific requirements.....	19
General block-based import restrictions.....	19
CHAP restrictions.....	21
Source system restrictions.....	22
General restrictions for hosts.....	22
Windows-based hosts.....	22
Linux-based hosts.....	23
VMware ESXi-based hosts.....	23
General file-based import restrictions.....	24
Restrictions and limitations for SMB-only VDM or NAS server file import.....	25
Restrictions and limitations for NFS-only VDM file import.....	26
Importing VNX2 or Unity file systems with File Level Retention (FLR) enabled.....	28
Dell VNX2 and Dell Unity port requirements for file-based data import.....	29
Chapter 3: Host plugin installation (block-based non-disruptive import only).....	30
Installing the host plugin for import on a Windows-based host	30
Install the host plugin for import on a Windows-based host.....	31
Upgrade the host plugin for import on a Windows-based host.....	31
Pre-requisites for an install using the .MSI file.....	32
Installing the host plugin for import on a Linux-based host.....	32
Install the host plugin for import on a Linux-based host.....	32
Upgrade the host plugin for import on a Linux-based host.....	34

Installing the Dell EqualLogic MEM kit on an ESXi-based host.....	35
Install the Dell EqualLogic MEM kit on an ESXi-based host using the vSphere CLI.....	35
Install the Dell EqualLogic MEM kit on an ESXi-based host using setup.pl script on VMA.....	36
Install the Dell EqualLogic MEM kit on an ESXi-based host using VUM.....	37
Install the Dell EqualLogic MEM kit during an ESXi-based host upgrade.....	38
Uninstalling the host plugin for import.....	38
Chapter 4: Import workflows.....	39
Non-disruptive import workflow.....	39
Cutover workflow for non-disruptive import.....	40
Cancel workflow for non-disruptive import	41
Agentless import workflow.....	41
Cutover workflow for agentless import.....	44
Cancel workflow for agentless import.....	44
File-based import workflow.....	45
Cutover workflow for file-based import.....	46
Cancel workflow for file-based import.....	46
Chapter 5: Configuring and managing import.....	48
Configure a non-disruptive import.....	48
Refresh hosts and volumes in a non-disruptive import.....	51
Manage non-disruptive import sessions.....	51
Configure an agentless import.....	53
Configure an agentless import for a Universal type remote system.....	57
Manage agentless import sessions.....	61
Configure a File Mobility Network for file-based import.....	63
Configure the connection to a remote system for file-based import.....	63
Configure file import interface.....	65
Configure a file-based import.....	65
Manage file-based import sessions.....	68
Appendix A: Import-CLI (Linux).....	70
Get help.....	70
Status.....	71
Host plugin version.....	71
List supported arrays.....	72
Server port.....	72
Log information.....	73
Microhttpd status.....	73
Restart the web server	73
Recover device.....	74
Appendix B: Additional tasks related to import for Linux-based hosts.....	75
Regenerate the host HTTPS certificate.....	75
Setting the Oracle ASM logical block size	75
Appendix C: ImportKit-CLI (Windows).....	77
How to run the ImportKit CLI commands.....	77
List supported arrays.....	78

Host plugin log information.....	78
Import kit version.....	78
Restart import kit host plugin service.....	79
Import volumes information.....	79
Get web server port information.....	80
Install import kit certificate.....	81
Regenerate the import kit certificate.....	81
Set web server port information.....	81
Set host plugin logging debug log level.....	82
Appendix D: Import-CLI (VMware).....	84
List log levels.....	84
List volumes.....	84
Revert SATP, VAAI, and PSP to default settings.....	85
equalRule options.....	85
Appendix E: CLI for EQL MPIO	87
Status.....	87
Host plugin version.....	88
Server port information.....	88
Log information.....	88
Microhttpd status.....	89
Restart the web server	89
Recover device.....	89
Appendix F: Fault handling by PowerStore import	91
Import processing and fault handling overview.....	91
Import network overview.....	92
Import alerts and error codes.....	92
Failures during non-disruptive import.....	92
Single fault.....	92
Source disaster recovery.....	93
Double fault.....	93
Exception case.....	94
Host reboot during a non-disruptive import.....	94
Failures during agentless import.....	94
Consistency group handling.....	95
Configuration changes during import.....	95
Application integration software.....	95

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 Info Hub](#).
- **Troubleshooting**—For information about products, software updates, licensing, and service go to [Dell Support](#) and locate the appropriate product support page.
- **Technical support**—For technical support and service requests, go to [Dell Support](#) and locate the **Service Requests** page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

Customer feedback

A feedback button is located at the right side of the PowerStore Manager. Selecting **Feedback** opens a browser window where you can fill and submit a feedback survey.

Third-party content containing non-inclusive language

This manual may contain language from third-party content that is not under Dell Technologies' control and is not consistent with current guidelines for Dell Technologies' own content. When such third-party content is updated by the relevant third parties, this manual will be revised accordingly.

Introduction

This document describes how to import data from external storage to PowerStore.

This chapter contains the following information:

Topics:

- [Importing block-based external storage to PowerStore overview](#)
- [Importing file-based external storage to PowerStore overview](#)
- [PowerStore cluster fibre channel connectivity to source systems](#)
- [Import security](#)

Importing block-based external storage to PowerStore overview

PowerStore provides the abilities of a traditional storage appliance to run embedded workloads. PowerStore enables users to respond quickly to changing business requirements and to scale quickly to meet changing needs without excessive business planning and complexity.

Importing block-based external storage to PowerStore is a migration solution that imports block data from any of the following Dell storage platforms to a PowerStore cluster:

- Dell Peer Storage (PS) Series
- Dell Storage Center (SC) Series
- Dell Unity Series
- Dell VNX2 Series
- Dell XtremIO X1 and XtremIO X2 (agentless import only)
- Dell PowerMax and VMAX3 (agentless import only)
- Universal system, either a legacy Dell EMC or third-party storage system (agentless import only)

This import solution can also be used to import block-based data from NetApp AFF A-Series platforms that use ONTAP. See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for more information.

Import of the following block storage resources is supported:

- LUNs and Volumes
- Consistency groups, Volume groups, and Storage groups
- Thick and thin clones

The following options are available to import block-based external storage to a PowerStore cluster:

- Non-disruptive import
- Agentless import

Non-disruptive import of external storage to PowerStore overview

The software that runs on the PowerStore cluster and manages the entire import process is known as the Orchestrator. In addition to the Orchestrator, host multipath I/O (MPIO) software and a host plug-in are required to support the import process. The host plug-in is installed on each host that accesses the storage to be imported. The host plug-in enables the Orchestrator to communicate with the host multipath software to perform import operations.

The Orchestrator supports Linux, Windows, and VMware host operating systems. The Orchestrator supports the following host MPIO configurations:

- Linux Native MPIO and Dell PowerStore Import Plugin for Linux
- Windows Native MPIO and Dell PowerStore Import Plugin for Windows

- Dell PS Series
 - Dell MPIO in Linux - Provided through Dell Host Integration Tools (HIT Kit) for Linux
 - Dell MPIO in Windows - Provided through Dell HIT Kit for Microsoft
 - Dell MPIO in VMware - Provided through Dell MEM Kit

NOTE: If you are using native MPIO and the Dell HIT Kit is not installed on the hosts, the PowerStore ImportKit must be installed on the hosts to support import to a PowerStore cluster. If the Dell HIT Kit is already installed on the hosts, ensure that the Dell HIT Kit version matches the version listed in the *PowerStore Simple Support Matrix*. If the HIT Kit version is earlier than the version that is listed in the *Simple Support Matrix*, it must be upgraded to the supported version.

For the most up-to-date supported versions of the supported combinations of host operating system, multipath software, host protocol to the source and to the PowerStore cluster, and the type of source system for non-disruptive (seamless) import, see the *PowerStore Simple Support Matrix* document at dell.com/powerstoredocs.

If the version of the operating environment running on your source system does not match what is listed for non-disruptive (seamless) import in the *PowerStore Simple Support Matrix* document, you may be able to use agentless import. The *Simple Support Matrix* also lists the most up-to-date information for supported versions of source systems and operating environment that are required for agentless import.

NOTE: For PowerStore with operating system versions 3.0 or later, the connection from some source systems to the PowerStore cluster for import can be over either iSCSI or FC. The *Simple Support Matrix* document for PowerStore lists what protocol is supported for the connection between the source system and PowerStore. When FC connections are used between the source system and PowerStore, only FC connections between the hosts and the source system and the hosts and PowerStore are supported. For PowerStore with operating system versions 2.1.x or earlier, the connection from the source system to the PowerStore cluster for import is only over iSCSI.

NOTE: For the most up-to-date supported versions of software, see the *Simple Support Matrix* document for PowerStore.

Overview of the non-disruptive import process

Before importing the external storage from a source system to a PowerStore cluster, the active path for the host I/O is to the source system. During the setup of import, the host or hosts build an inactive I/O path to the volumes that are created on the PowerStore cluster which match the specified volumes on the source system. When you start import, the active host I/O path to the source system becomes inactive and the inactive host I/O path to the PowerStore cluster becomes active. However, the source system is kept updated through the I/O forwarding from the PowerStore cluster. When the import reaches the Ready For Cutover state and you initiate cutover, the host I/O path to the source system is removed and the host I/O is directed only to the PowerStore cluster.

Review the following processes to gain an understanding of the import procedure:

1. Preconfigure – Set up the network connectivity.
 - The connection between an existing Dell PS Series or Dell SC Series source system and the PowerStore cluster must be over iSCSI.
 - For Dell PS Series or Dell SC Series source systems – All the connections between the hosts and the Dell PS Series or Dell SC Series source system and between the hosts and the PowerStore cluster must be over iSCSI.
 - The connection between an existing Dell Unity Series or Dell VNX2 Series source system and the PowerStore cluster can be over either iSCSI or Fibre Channel (FC). See the *PowerStore Simple Support Matrix* document at dell.com/powerstoredocs to determine which protocol to use.
 - For Dell Unity Series or Dell VNX2 Series source systems – The connections between the hosts and the Dell Unity Series or Dell VNX2 Series source system and between the hosts and the PowerStore cluster must be either all over iSCSI or all over Fibre Channel (FC) and match the connection between the source system and the PowerStore cluster. See the *PowerStore Simple Support Matrix* document at dell.com/powerstoredocs to determine which protocol can be used. Also, all host initiators that are connected to the source system should also be connected to the PowerStore cluster.

NOTE: When FC connectivity between the hosts and the source system, the hosts and the PowerStore cluster, and source system and the PowerStore cluster is used, the administrator must set up FC zoning between the hosts, the source system, and the PowerStore cluster.
2. Setup import – Install or upgrade the appropriate host plugin as needed on each host that accesses the storage to be imported. Add the source system to the PowerStore cluster, if it is not already listed. Select one or more volumes or consistency groups, or both to be imported. A volume group cannot be combined with any other volumes or volume group. Select to add the hosts that access the storage to be imported, the hosts build inactive I/O paths to the destination volumes. Set the import schedule and assign protection policies.

3. Start import – A destination volume is created for each selected source volume. A volume group is automatically created for each consistency group that is selected for import. The active I/O and inactive I/O paths from the host are switched to redirect the I/O to the PowerStore cluster. However, the source is kept updated through the I/O forwarding from the PowerStore cluster.
4. Cutover import – Cutover can be performed only when the import processing state is `Ready For Cutover`. In other words, cutover is a final confirmation. You can select to cut over automatically without user intervention. After the cutover step, I/O cannot go back to the source system volume.

In addition, the following processes are available during the import procedure:

- Pause import – Pause can be performed when the import processing state is `Copy In Progress`. When an import session is paused, only the background copy is stopped. The forwarding of host I/O to the source system continues to be active.

NOTE: The Pause import action on a CG only pauses the member volumes that are in the `Copy In Progress` state. The CG remains in the `In Progress` state. Other member volumes that are in other states, such as `Queued` or `In Progress`, are not paused and may proceed to the `Ready For Cutover` state. The other member volumes can be paused when they reach the `Copy In Progress` state by using the Pause import action again on the CG. If any of the member volumes are in the `Paused` state but the overall status of the CG is `In Progress`, both the Pause and Resume import action options are available for the CG.

- Resume import – Resume can be performed when the import processing state is `Paused`.
- Cancel import – Cancel can be performed only when the import processing state is `Copy In Progress` (for volume), `In Progress` (for consistency group), `Ready For Cutover`, `Queued`, `Paused` (for volume), or `Scheduled`, or `Cancel Failed` (for consistency group). Cancel allows you to cancel the import process with the click of a button and change the active path back to the source.

For Dell PS Series source systems only – The source volume is taken offline after a successful cutover operation.

For the Dell SC Series, Dell Unity Series, and Dell VNX2 Series source systems – Host access to the source volume is removed after a successful cutover operation.

Agentless import of external storage to PowerStore overview

Unlike nondisruptive import, agentless import of external storage to a PowerStore cluster is independent of the operating system and the multipathing solution on the host, and the front-end connectivity between the host and the source system. Agentless import does not require the installation of host plug-in software on the host. However, you must reconfigure the host application to work with the new PowerStore volumes. Only a one-time host application downtime is required before the migration. The downtime only includes renaming or reconfiguring the host application, file systems, and datastores to the new PowerStore volumes.

Use the agentless import option to migrate the external storage to a PowerStore cluster when the operating environment running on the source system does not match the respective non-disruptive supporting import operating environment. See the related list in the *Simple Support Matrix* for PowerStore. Also, use the agentless import option when the source system is one of the following:

- Dell PowerMax or VMAX3 system
- Dell XtremIO X1 or XtremIO X2 system
- NetApp AFF A-Series system
- Universal system (either a legacy Dell or third-party storage system)

NOTE: When the operating environment running on your source system matches the respective non-disruptive supporting import operating environment that is listed in the *Simple Support Matrix* for PowerStore, you can choose to use the agentless import option instead of the non-disruptive option. However, the host plug-in software must not be installed on the associated host or hosts.

See the PowerStore *Simple Support Matrix* [document for the supported types of source systems and the version of operating environment](#) that is required for the agentless import.

Overview of the agentless import process

Before importing the external storage from a source system to a PowerStore cluster, the active path for the host I/O is to the source system. The host or hosts are not automatically added to the PowerStore cluster and must be added manually before setting up the agentless import. During the setup of an agentless import, volumes are created on the PowerStore cluster that

match the specified volumes on the source system. However, unlike non-disruptive import, the host applications that access the source system volume or volumes must be shut down manually and the source volumes brought offline.

NOTE: For host clusters, the source LUNs could have SCSI reservations keys. The SCSI reservations must be removed for imports to be successful.

To start an agentless import, the destination volume must be manually enabled and the host application must be reconfigured to use the destination volume instead of the source volume. The destination volume is read-only until it is enabled. Once the destination volume has been enabled, the host application has to be reconfigured to access the destination volume. Start the import to copy the source volume data to the destination volume. The source system is kept updated through I/O forwarding from the PowerStore cluster. When the import reaches the `Ready For Cutover` state, you can initiate the cutover. The I/O forwarding from the PowerStore cluster to the source system ends when cutover is initiated.

Review the following processes to gain an understanding of the import procedure:

NOTE: You can also see the [Importing External Storage to PowerStore video to gain an understanding of the import procedure](#).

1. Preconfigure – Set up the network connectivity.

- The connection between an existing Dell PS Series source system and the PowerStore cluster must be over iSCSI.
- For Dell PS Series source systems – All the connections between the hosts and source system, and between the hosts and the PowerStore cluster must be over iSCSI.
- For Dell SC Series, Dell Unity Series, Dell VNX2 Series, Dell XtremIO X1 or XtremIO X2, and NetApp AFF A-Series or Universal (either legacy Dell or third-party) source systems – The connections between the hosts and the source system and between the hosts and the PowerStore cluster must be either all over iSCSI or all over Fibre Channel (FC). See the [PowerStore Simple Support Matrix document to determine which protocol to use](#)

NOTE: When FC connectivity is used between the hosts and the source system, the hosts and the PowerStore cluster, and the source system and the PowerStore cluster, the administrator must set up FC zoning between the hosts, the source system, and the PowerStore cluster. When the connections between the source system and the PowerStore cluster are all over iSCSI, the connections between the hosts and the source system and between the hosts and the PowerStore cluster can be either all over iSCSI or all over FC. However, when the connections between the source system and the PowerStore cluster are all over FC, the connections between the hosts and the source system and between the hosts and the PowerStore cluster must be all over FC.

- The connection between an existing Dell SC Series, Dell Unity Series, Dell VNX2 Series, or Dell XtremIO X1 or XtremIO X2 source system, or NetApp AFF A-Series or Universal source system and the PowerStore cluster can be over either iSCSI or FC. See the [PowerStore Simple Support Matrix document to determine which protocol to use](#).
- The connection between an existing Dell PowerMax or VMAX3 source system and the PowerStore cluster must be over FC.

NOTE: The administrator must set up FC zoning between the source system and the PowerStore cluster.

- For Dell PowerMax and VMAX3 source systems – All the connections between the hosts and the source system and between the hosts and the PowerStore cluster must be over FC.

NOTE: The administrator must set up FC zoning between the hosts, the source system, and the PowerStore cluster.

2. Setup import – If they are not already listed, add the source system and the hosts to the PowerStore cluster. Select one or more volumes or consistency groups (CGs), or both, or LUNs, or storage group to be imported. A volume group or storage group cannot be combined with any other volume or volume group. Select to map the hosts that access the storage to be imported. Set the import schedule and assign a protection policy.

NOTE: For a Universal remote source system, you must add PowerStore with either iSCSI initiators or FC as a host on the source system and map the applicable volumes to it.

3. Start import – A destination volume is created for each selected source volume. Except for the Universal type of remote source systems, a volume group is automatically created for each CG or storage group that is selected for import. When the destination volume is in the `Ready To Enable Destination Volume` state, shutdown or take off line the host application on the applicable host or hosts that use the source volume. Also, remove the host mapping to the applicable source system volume. Select and enable the destination volume which is in the `Ready To Enable Destination Volume` state. Reconfigure the host application to use the applicable destination volume. Ensure that the host application can work successfully using the destination volume. Select and Start Copy for the destination volume which is in the `Ready to Start Copy` state.

NOTE: It is recommended to remove the host mapping of the source volumes during the enable destination volume process. If the host mapping of the source volumes is not selected for removal by the orchestrator, the mapping should be removed manually. Also, only one agentless import can be processed from the PowerStore cluster at any point in time until the import process reaches the `Ready to Start Copy` state. A second agentless import will start execution only after the previous import reaches the `Copy In Progress` state.

NOTE: Only volumes are discovered for a Universal type remote system. Consistency groups are not discovered. If a consistency group exists on the source system and should also exist on the destination, PowerStore Manager provides options to create it and to add the applicable volumes to it. When a consistency group is created in this manner, a volume group is automatically created in place of the consistency group on PowerStore during import. If you would like to group discovered individual volumes as a volume group when they are imported, PowerStore Manager provides options to create the volume group and to add the applicable volumes to it.

4. Cutover import – Cutover can be performed only when the import processing state appears as `Ready For Cutover`. In other words, cutover is a final confirmation. You can select to cut over automatically without user intervention.

NOTE: After cutover of each volume or CG, it is recommended that the mapping of the volume or CG volumes to PowerStore in the source system be removed immediately before performing cutover of the next import session. If removal of the mapping of multiple volumes or CG is performed at once in the source system, it is recommended to leave a gap of at least 10 minutes before mapping the next set of volumes or CG to PowerStore for import. This delay is required for complete clean up of unmapped devices in PowerStore. Otherwise, new imports can fail because mirror service cannot be enabled on the destination volume of the import. In this case, retry the import and, if this error happens consistently, delete the remote system and re-add it to continue further imports.

In addition, the following actions are available during the import procedure:

- Pause import – Pause can be performed when the import processing state appears as `Copy In Progress`.

NOTE: The Pause import action on a CG only pauses the member volumes that are in the `Copy In Progress` state. The CG remains in the `In Progress` state. Other member volumes that are in other states, such as `Queued` or `In Progress`, are not paused and may go to the `Ready For Cutover` state. The other member volumes can be paused when they reach the `Copy In Progress` state by using the Pause import action again on the CG. If any of the member volumes are in the `Paused` state but the overall status of the CG is `In Progress`, both the Pause and Resume import action options are available for the CG.

- Resume import – Resume can be performed when the import processing state is `Paused`.
- Cancel import – For volumes, Cancel can be performed only when the import processing state is `Queued`, `Scheduled`, `Ready To Enable Destination Volume`, `Ready to Start Copy`, `Copy In Progress`, `Paused`, `Ready for Cutover`, or `Cancel Required` and the host application that is accessing the volume has been shut down. For volume groups, Cancel can be performed only when the import processing state is `Queued`, `Scheduled`, `In Progress`, `Paused`, `Ready for Cutover`, `Cancel Required`, `Cancel Failed`, and the host application that is accessing the volume has been shut down.
- Enable Destination Volume – Ensure the host application on the applicable host or hosts that use the source volume or volumes have been shut down or taken off line before enabling each destination volume in an import session.
- Start Copy – Start Copy can be performed for each of the destination volumes that are in the `Ready to Start Copy` state.

Importing file-based external storage to PowerStore overview

Importing file-based external storage to PowerStore is a migration solution that imports either of the following to a PowerStore cluster:

- A Virtual Data Mover (VDM) (file data) with its configuration and data from an existing source Dell VNX2 Series platform
- A NAS server (file data) with its configuration and data from an existing source Dell Unity Series platform

For either a VNX2 Series platform or Unity Series platform, this feature provides an integrated capability for NFS-only VDM or NAS server imports with minimal or no disruption to clients. It also provides an integrated capability for SMB (CIFS)-only VDM or NAS server imports. However, cutting over of an SMB-only VDM or NAS server import session can be a disruptive process. PowerStoreOS version 4.1 or later also supports the following types of import of NAS servers from Unity Series platforms:

- Dual protocol (NAS server with both NFS and SMB file systems)
- Multiprotocol (NFS and SMB on the same file system)

For a file-based VDM or NAS server import, after the cutover completes, the import process does an incremental copy automatically but you must complete the import manually.

An import is always conducted from the PowerStore appliance. The destination system makes a remote call to the source storage system and instigates a pull (for file-based import) of the source storage resources to the destination system.

VDM and NAS server import operations support:

- Import of VDM or NAS server with only NFSV3 protocol enabled (VDMs or NAS servers with NFSV4 protocol enabled are not supported)
- Import of VDM or NAS server with only SMB (CIFS) protocol enabled

i NOTE: Import of VDM with multiprotocol file systems or with both NFS and SMB (CIFS) file systems that are exported and shared is not supported. Import of NAS server with multiprotocol file systems or with both NFS and SMB (CIFS) file systems that are exported and shared is supported on PowerStore systems with operating system version 4.1 or later, but not earlier versions.

PowerStore systems with operating system version 4.1 or later support the following items that are associated with stub-aware import of NAS servers that contain Cloud Tiering Appliance (CTA) stubs from the Dell Unity platform:

- Recall the files from the backend cloud storage through the CTA once the clients access the stubs after cutover.
- CTA policy engine continues creating stubs on imported NAS servers according to CTA policy.
- Synchronous or Asynchronous replication works on imported NAS servers.
- CTA FQDN should be resolvable from the DR site and should have network connectivity for recalls working.
- Clone operations on imported NAS servers or file systems within.
- On the cloned NAS servers, only recalls would be supported and new stubs are not generated.
- Cloned file systems can support tiering as well, by adding required tasks on CTA.
- Snapshot operations like refresh and restore on imported NAS servers.
- Recall policies.
- Replication of NAS servers with stubs to compatible DR sites.

Overview of the file-based import process

Review the following processes to gain an understanding of the file import procedure:

1. Prepare the source VDM (on source VNX2 system) or NAS server (on source Unity system) for an import – Create a source import network interface.

i NOTE: Clients are connected to the source VDM or NAS server either through the NFSv3 or SMB1, SMB2, or SMB3 file sharing protocol. For VNX import, the interface must be named `nas_migration_<interface_name>`.

2. Add the remote system (to establish the import connection) – Establish a file import interface connection to the source VNX2 (Control Station management interface) or Unity (Storage Processor management interface) from PowerStore over SSH. The system is validated, source VDMs or NAS servers are discovered (the configuration of file systems, network interfaces, and such are retrieved), and pre-checks identify the import capability for each VDM or NAS server on the source system.

i NOTE: The procedure can be repeated on demand for an existing connection.

3. Create a file import session – Specify all the options for the import.

i NOTE: The user settings and the source VDM or NAS server are validated. If an import session is scheduled to start later, the **Import State** is shown as **Scheduled**. However, if two active import sessions (which is the maximum for active import sessions) are running, any new import sessions that are set to start are shown with an **Import State** of **Queued**. A maximum of ten import sessions can be scheduled or queued, however, only a maximum of eight import sessions can be scheduled or queued while two import sessions are active.

4. Start the file import session.

i NOTE: The basic configuration of the source VDM or NAS server must not change since an import session is created.

- a. The import session begins – Destination NAS server, destination file mobility network, and destination file systems are created. For an NFS import, unexported file systems are exported.
- b. Initial (baseline) data copy is initiated. Stable data and directory structure is pulled to the destination.
- c. Import of the configuration from the source VDM or NAS server to the destination NAS server occurs. The configuration includes:
 - Production network interfaces
 - Static routes
 - DNS
 - SMB server
 - SMB shares
 - NFS server
 - NFS exports
 - NIS
 - LDAP
 - Local files
 - Effective naming service
 - Quotas

i NOTE: The session state is shown as **Ready For Cutover** when the import of the configuration completes. If the file system on the destination system is low on space (reaches 95% of capacity) during import, import of the source file system will fail. In this case, you can either ensure that enough space is available and run **Resume** or **Cancel** the import session.

5. Cut over the import session – Production interfaces are disabled on the source side and enabled on the destination side.

i NOTE: For SMB imports, the Active Directory configuration is imported and the switch over is disruptive. For NFS imports, NLM locks are reclaimed for transparent switch over and clients may experience a 30-90 s downtime.

An incremental data copy begins – Live import and re-synchronization of data from the source to the destination occurs.

i NOTE: Clients are connected to the destination, and the source is updated with modifications from the destination. The source is authoritative. File Creation/Write is done first on the source. When re-synchronization occurs on a file, it is marked up to date, and further reads are done from the destination. For a file or directory that is not synchronized yet, all operations are forwarded to the source. During synchronization, file read can be done on the destination (partial read) for imported data that is already committed on this file. Some configuration changes on the destination during an import are pushed back to the source in a rollback. During an import, snapshots/backups can be created on the source VDM or NAS server. Replication from the source is still active, and user quota management is still active on the source VDM or NAS server. When all files are synchronized, the status of the import session is shown as **Ready For Commit**.

6. Commit the import session – Protocol data connections to the source terminate and synchronizing modifications stop. The destination import interface is deleted, and cleanup of the source system occurs. The final state is shown as **Completed**.

In addition, the following actions are available during the import procedure:

- Pause import – Pause can be performed when the import processing state is `Copy In Progress` during session create or cutover operations.

i NOTE: When a user tries to pause an import session when an incremental copy is about to complete, the session can be transitioned automatically from the `Paused` state to the `Ready For Commit` state without the user having to resume the import session. The `Ready For Commit` state is equivalent to the `Paused` state in terms of the load on the source system.

- Resume import – Resume can be performed when the import processing state is `Paused`.
- Cancel import – Cancel is allowed at any state of the file import session except `Completed`, `Failed`, `Cancelling`, and `Cancelled`. Production interfaces are disabled on the destination side and enabled on the source side. Cancel is disruptive for NFS and SMB clients. Some changes to the configuration will be synchronized from the destination to the source. The

source system is cleaned up, and the destination NAS server is deleted. **Cancelled** is a terminal state. Cancel can be forced if the source stops responding.

PowerStore cluster fibre channel connectivity to source systems

PowerStoreOS version 3.0 or later provides an option to import data from an external source system to a PowerStore cluster using Fibre Channel (FC) connectivity. Except for the Universal type of remote source systems, the World Wide Name (WWN) of the source system is automatically discovered for an FC data connection. The Connection is automatically established from PowerStore to the source system. Host groups are automatically created on the source system with FC initiators and mapped during import.

For the Universal type of remote destination system, the WWN of the destination system is not discovered automatically. In this case, PowerStore Manager lists discovered FC target WWNs during remote system addition. You must select WWNs from the list which belongs to the remote system that is being added and proceed with the remote system addition. PowerStore establishes an FC data connection with these selected FC WWNs. After remote system addition, you must create a host on the source system with the FC initiators of all the PowerStore appliances in the PowerStore cluster. The FC initiators of PowerStore are specified as the **Import Capable** FC ports in each appliance.

Intelligent volume placement occurs within the PowerStore cluster during Import. The host groups are created upon addition of the remote system in PowerStore.

Both agentless and nondisruptive import variants support FC connectivity. However, PowerStore with FC connectivity to a source system supports only FC connectivity with the hosts.

NOTE: The *Simple Support Matrix* document for PowerStore lists what protocol is supported for the connection between hosts, source system, and PowerStore.

Except for the Universal type of remote source systems, PowerStore creates connection to the remote destinations based on an internal high availability (HA) policy. The system determines the number of connections from an FC initiator to destinations. Each initiator port sequentially connects to a unique destination in each controller, SP, or Director of the respective remote system. Configuration on Node A is applied as is in Node B on a best-effort basis. PowerStore automatically determines the internal HA policy compliance during Create, or Verify, or Connection health change.

For the Universal type of remote source system, you must configure connectivity between the source system and PowerStore as shown in [FC connections between Controllers of remote system and PowerStore Nodes](#). You must select the target FC WWNs in accordance with [FC connections between Controllers of remote system and PowerStore Nodes](#) during remote system addition to ensure that the established connection is compliant with the internal HA policy of PowerStore.

Import capable I/O Module0 Ports

Importing data from an external source system into PowerStore with FC connectivity requires that ports 0 and 1 of PowerStore I/O Module0 are enabled as Dual (as both initiator and target). These ports are shown as P0 and P1, respectively, in the simplified connectivity example [FC connections between Controllers of remote system and PowerStore Nodes](#). A maximum of two destinations can be connected from each node. The destination ports in the remote system are shown as T0 and T2, respectively.

NOTE: The port labels in the figure are used for descriptive purposes only and do not represent the physical labels on the hardware platforms. Although two switches are shown in the figure, it is recommended to place the remote system and PowerStore ports on the same physical switch. Also, the use of ISL is optional. If ISL is used, ensure that there is sufficient ISL bandwidth and that the remote system and PowerStore system interfaces are separated by no more than two ISL hops. For implementation instructions, see the user manual of the Fibre Channel switch.

- For Dell Unity or Dell VNX2, make connections from each PowerStore node to two different Dell Unity or Dell VNX2 SPs or controllers. For example, connect port P0 of PowerStore Node A and Node B through a switch to the destination port T0 of SPA of the Dell Unity source system. Connect port P1 of PowerStore Node A and Node B through a switch to the destination port T2 of SPB of the Dell Unity source system.
- For Dell PowerMax or VMAX3, make connections from each PowerStore node to two different Dell PowerMax or VMAX3 directors. For example, connect port P0 of PowerStore Node A and Node B through a switch to the destination port T0 of PowerMax source system Director-X. Connect port P1 of PowerStore Node A and Node B through a switch to the destination port T2 of PowerMax source system Director-Y.

- For Dell Compellent SC, connection from each PowerStore node is made to two controllers through two fault domains. In case multiple fault domains are configured, make connection to a maximum of two fault domains. For legacy mode, make the connection to primary ports through two different fault domains. Make connections from each PowerStore node to two different Dell Compellent SC controllers. For example, connect port P0 of PowerStore Node A and Node B through Fault Domain 1 to the destination port T0 of Dell Compellent SC source system Controller A. Connect port P1 of PowerStore Node A and Node B through Fault Domain 2 to the destination port T2 of Dell Compellent SC source system Controller B. See [FC connections between Controllers of remote system and PowerStore Nodes](#) as an example.

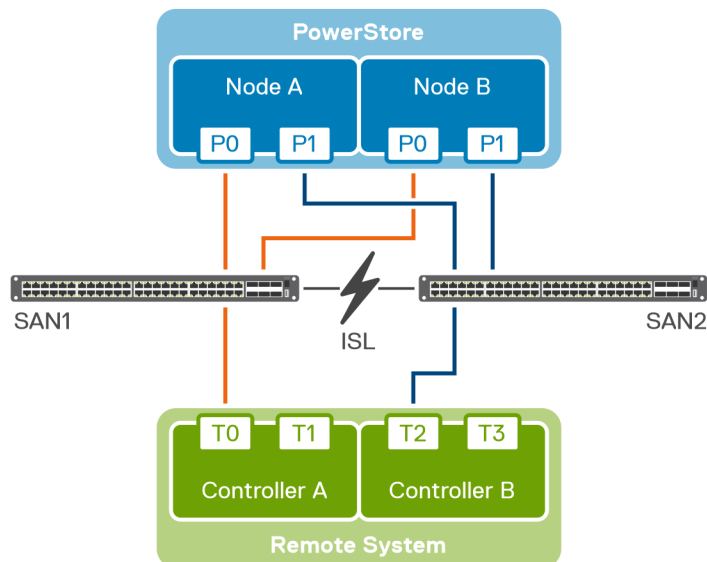


Figure 1. FC connections between Controllers of remote system and PowerStore Nodes

Table 1. PowerStore to remote system port configuration

PowerStore Node	PowerStore (P) to target remote system (T) port configuration
A	P0 to T0
	P1 to T2
B	P0 to T0
	P1 to T2

PowerStore ports P0 and P1 on Nodes A and B refer to Fibre Channel I/O Module0 FEPort0 and FEPort1, respectively. The **SCSI Mode** setting for these ports should be set to **Dual** (both initiator and target).

NOTE: To view the list of import capable ports on a PowerStore appliance in PowerStore Manager, select an appliance under **Hardware**, and then select **Fibre Channel** on the **Ports** card.

Login to the source system is initiated after the remote system is added. PowerStore connects only to the allowed list of destinations.

Import security

Communication between the source system, hosts, and the PowerStore cluster is provided by using HTTPS certificates. These certificates are used to establish secure communication between the following import components:

- PowerStore cluster and the source system
- PowerStore cluster and the host systems

PowerStore Manager provides a table that shows the configured remote system connections to the PowerStore cluster. You can select a remote system that is listed in the table and update and view the stored certificate of the remote system.

NOTE: Updating the certificate for PS EqualLogic and Universal type remote systems is not applicable.

PowerStore Manager provides an option to view and accept the remote certificates when adding a host to the PowerStore cluster.

 **NOTE:** PowerStore Manager is a web-based software application that enables you to monitor and manage storage resources, virtual machines, and appliances within a PowerStore cluster.

When the source storage volumes are configured with CHAP, data transfer is secured with CHAP support, Discovery CHAP, and Authentication CHAP. The PowerStore cluster supports both single and mutual CHAP. For more information about CHAP support, see [CHAP restrictions](#).

Import requirements and restrictions

This chapter contains the following information:

Topics:

- General requirements for importing data
- Dell EqualLogic PS Series specific requirements
- Dell Compellent SC Series specific requirements
- Dell Unity specific requirements
- Dell VNX2 Series specific requirements
- Dell XtremIO X1 and X2 specific requirements
- Dell PowerMax and VMAX3 specific requirements
- NetApp AFF A-Series specific requirements
- General block-based import restrictions
- General file-based import restrictions

General requirements for importing data

The following requirements apply to PowerStore before running import:

- The global storage IP address for PowerStore must be configured.
- Verify that PowerStore and its nodes are in a healthy state.

The following requirements apply to all source platforms:

- (For non-disruptive import) You must have the appropriate privileges on the source and its associated hosts to perform an import to a PowerStore cluster.
 - For Windows-based systems, Administrator privilege is required to perform an import to a PowerStore cluster.
 - For Linux-based and VMware-based systems, root privilege is required to perform an import to a PowerStore cluster.
- The size of any volume imported from a remote system to a PowerStore cluster must be a multiple of 8192 bytes.
- (For non-disruptive import) A Fibre Channel (FC) or iSCSI connection exists between the source system and each associated host system, and a matching FC or iSCSI connection exists between each associated host system and the PowerStore cluster. These connections to each host system should be of the same type, either all FC or all iSCSI.
- (For agentless import) For Dell PS source systems, all the connections between the hosts and the Dell PS source system and between the hosts and the PowerStore cluster must be over iSCSI. For Dell PowerMax or VMAX3, an FC connection exists between the source system and each associated host system, and a matching FC connection exists between each associated host system and the PowerStore cluster. For Dell SC or Unity, or Dell VNX2, XtremIO X1, XtremIO X2 source systems, or NetApp AFF A-Series, or Universal source systems, the connections between the hosts and the source system and between the hosts and the PowerStore cluster must be either all over iSCSI or all over Fibre Channel (FC).

NOTE: When FC connectivity between the host and source system and between the host and PowerStore cluster is used, the administrator must set up FC zoning between the host, the source system, and the PowerStore cluster.

- Only an iSCSI connection is supported between the following source systems and the PowerStore cluster.
 - Dell EqualLogic PS
 - Dell Compellent SC (non-disruptive import for Linux only)
- Only an FC connection is supported between a Dell PowerMax or VMAX3 source system (agentless import) and the PowerStore cluster.
- Either an iSCSI connection or an FC connection is supported between a Dell Compellent SC, or XtremIO X1, or X2 system, or a NetApp AFF A-series or Universal type system (agentless import), or a Dell Unity or VNX2 (either non-disruptive or agentless) source system and the PowerStore cluster.

NOTE: When the connection between the Dell Compellent SC, or XtremIO X1, or X2 system, or a NetApp AFF A-series or Universal type system (agentless import), or a Dell Unity or VNX2 (either non-disruptive or agentless) source system

and the PowerStore cluster are over iSCSI, the connections between the hosts and the source system and between the hosts and the PowerStore cluster can be either all over iSCSI or all over FC. However, when the connections between those source systems and the PowerStore cluster are all over FC, the connections between the hosts and the source system and between the hosts and the PowerStore cluster must be all over FC.

- (For non-disruptive import) Only one instance of MPIO should be running on the host in order to perform an import.
- The PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs lists the host operating system platforms that are supported for non-disruptive import.

NOTE: Use the agentless import option to migrate the external storage to the PowerStore cluster in either of the following cases:

- The operating environment running on the source system does not match what is listed in the PowerStore *Simple Support Matrix* for non-disruptive import.
- The source system is a Dell XtremIO X1 or XtremIO X2, or PowerMax or VMAX3, or a NetApp AFF-A Series.

The PowerStore *Simple Support Matrix* lists the supported types of source systems and operating environment that is required for agentless import. Agentless import can also be used to migrate the external storage from a source system running the operating environment listed in the PowerStore *Simple Support Matrix* for non-disruptive import. For the most up-to-date supported versions of the supported combinations of host operating system, multipath software, host protocol to the source and to the PowerStore cluster, and the type of source system for non-disruptive import, see the PowerStore *Simple Support Matrix* document.

- When Fibre Channel (FC) connectivity is used between the host and the PowerStore cluster, the administrator must set up FC zoning between the dual-mode FC ports to the destinations.

NOTE: For more information about FC zoning, see PowerStore Host Configuration Guide at dell.com/powerstoredocs.

- When Fibre Channel (FC) connectivity is used between the source system and the PowerStore cluster, the administrator must set up FC zoning between the source system and the PowerStore cluster.

NOTE: For FC connections, it is recommended to configure FC zoning in such a way that PowerStore can connect to at least two distinct targets on each remote system controller from a PowerStore node. See [PowerStore cluster fibre channel connectivity to source systems](#).

- (For non-disruptive import) Depending on the port number that is selected for the hosts that are added when creating an import session, that port must be open on the firewall. The predefined host ports for Windows and Linux are:
 - 8443 (default)
 - 50443
 - 55443
 - 60443The predefined host port for VMware is 5989.

Dell EqualLogic PS Series specific requirements

(For non-disruptive import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported combinations of host operating system, host multipath software, and host protocol that apply to Dell EqualLogic Peer Storage (PS) Series systems.

NOTE: (For non-disruptive import) If you are not running the Dell EqualLogic Host Integration Tools Kit, you can use the PowerStore cluster ImportKIT which uses native MPIO.

(For agentless import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported types of source systems and the version of operating environment that is required for the agentless import.

NOTE: All hosts taking part in an import process should have initiator names in the standard IQN format of `iqn.yyyy-mm.naming-authority:unique name`. Although PS source systems support friendly names, such as `*.*.*.*` or `172.92.*.*` for the standard IQN format, PowerStore only supports valid standard IQN format. Import fails when friendly IQN names are used. In this case, the initiator names must be changed to valid full IQN names on all the associated hosts before attempting an import of external storage to PowerStore.

Dell Compellent SC Series specific requirements

(For non-disruptive import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported combinations of host operating system, host multipath software, and host protocol that apply to Dell Compellent Storage Center (SC) Series systems.

 **NOTE:** While importing external storage from a Dell Compellent SC Series source system, do not delete or place the source resource in the Recycle Bin.

(For agentless import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported types of source systems and the version of operating environment that is required for the agentless import.

Dell Unity specific requirements

(For non-disruptive import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported combinations of host operating system, host multipath software, and host protocol that apply to Dell Unity systems.

(For agentless import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported types of source systems and the version of operating environment that is required for the agentless import.

Dell VNX2 Series specific requirements

(For non-disruptive import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported combinations of host operating system, host multipath software, and host protocol that apply to Dell VNX2 Series systems.

 **NOTE:** The supported OE on the Dell VNX2 has to be committed in order to perform an import of its storage resources.

(For agentless import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported types of source systems and the version of operating environment that is required for the agentless import.

Dell XtremIO XI and X2 specific requirements

(For agentless import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported types of source systems and version of operating environment that is required for agentless import.

When you select **iSCSI IP** for the **Data Connection Type** in the **Add Remote System** slide-out panel in PowerStore Manager, multiple iSCSI IP addresses separated by commas may be entered.

Dell PowerMax and VMAX3 specific requirements

(For agentless import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the following:

- The supported types of source systems and the version of operating environment that is required for the agentless import.
- The required version of Unisphere to use to configure and manage either a PowerMax system or a VMAX3 system.

NetApp AFF A-Series specific requirements

(For agentless import) See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported types of source systems and the version of operating environment that is required for the agentless import.

General block-based import restrictions

The following restrictions apply to importing block-based external storage to PowerStore:

- At any given time, a maximum of six source systems are supported.
- (For non-disruptive imports) A maximum of 64 hosts are supported. The applicable host plugin for import must be installed on the host.
- (For agentless imports) See the Dell *Simple Support Matrix* document at dell.com/powerstoredocs for the maximum number of hosts that are supported.
- A maximum of eight parallel import sessions can be in Copy-In-Progress at any instant of time. The remaining import sessions are queued up and automatically started when on going import sessions in Copy-In-Progress reach Ready-For-Cutover.
- (For non-disruptive imports) A maximum of 16 volumes in a consistency group (CG) is supported.

i NOTE: When a CG has 16 members, a maximum of eight members are imported in parallel, but they all start sequentially. That is, imports start one by one but, once they reach Copy-In-Progress, the next member is taken for processing. Once a member reaches Ready-For-Cutover, the next member is imported in parallel. Once all the members reach Ready-For-Cutover, the CG is Ready-For-Cutover.

- (For agentless import) A maximum of 128 volumes in a consistency group (CG) is supported.

i NOTE: When a CG has 128 members, a maximum of eight members are imported in parallel, but they all start sequentially. That is, imports start one by one but, once they reach Copy-In-Progress, the next member is taken for processing. Once a member reaches Ready-For-Cutover, the next member is imported in parallel. Once all the members reach Ready-For-Cutover, the CG is Ready-For-Cutover.

- (For non-disruptive imports) A CG that has volumes that are mapped to hosts running different types of operating systems cannot be imported. For example, a CG having volumes from a Linux host and Windows host cannot be imported.
- NVMe host mapping on PowerStore is not supported for importing a volume or CG.
- A maximum of 16 import sessions is supported in the Ready-For-Cutover state. Sometimes when several dozen import operations are run back-to-back, intermittent failures of alternate import sessions may occur. If these failures occur, do the following:
 1. Remove the remote (source) system and then add it again.
 2. Run fewer sets of imports (16 or less) at a time. It is recommended to start all these import sessions with automatic cutover turned off.
 3. Once all imports have reached the Ready-For-Cutover state, do a manual cutover.
 4. After one set of imports is completed, run the next set of imports after a delay of 10 minutes. This delay allows enough time for the system to cleanup any connections to the source system.
- You can import only an active volume or LUN. Snapshots are not imported.
- It is not recommended to change a host cluster configuration once the volume is selected for import.
- All the target port IP addresses returned by the iSCSI target portal of PowerStore should be reachable from the host where import is planned.
- Replication relationships are not imported.
- SAN boot disks are not supported.
- IPv6 is not supported.
- Veritas Volume Manager (VxVM) is not supported.
- (For non-disruptive imports) Only implicit ALUA mode is supported on source systems.
- The following configuration changes are not supported on the source system during import:
 - Firmware or Operating Environment upgrade
 - System re-configuration, including network configuration and restart of node or members
- When any configuration changes, such as moving a volume between hosts or resizing the source system volume capacity, are made to the source or a host system after they have been added to PowerStore, all the affected or involved systems must be refreshed from PowerStore Manager.
- Only an iSCSI connection is supported between the following source systems and the PowerStore cluster:
 - Dell EqualLogic PS
 - Dell Compellent SC (non-disruptive import for Linux only)
 (For agentless imports) Only an FC connection is supported between a Dell PowerMax or VMAX 3 source system and the PowerStore cluster. Either an iSCSI connection or a FC connection is supported between a Dell Compellent SC, or XtremIO X1 or X2 system, or Unity, or Dell VNX2, or Universal source system and the PowerStore cluster.

i NOTE: When the connection between the Dell Compellent SC, or XtremIO X1 or X2 system, or Unity, or Dell VNX2, or Universal source system, and the PowerStore cluster are over iSCSI, the connections between the hosts and the source system and between the hosts and the PowerStore cluster can be either all over iSCSI or all over FC. However, when

the connections between those source systems and the PowerStore cluster are all over FC, the connections between the hosts and the source system and between the hosts and the PowerStore cluster must be all over FC.

- (For non-disruptive imports) SCSI-2 clusters are not supported. Only SCSI-3 persistent reservation (PR) clusters are supported.
- PowerStore can only use one storage network for iSCSI data import.

NOTE: PowerStore automatically chooses the storage network for iSCSI data import when more than one storage network with replication and iSCSI purposes is found. If the remote system does have more than one of these networks, the Data Connection state is shown as Partially Connected, which is expected. If the storage network purposes are reconfigured, the system does not switch the data import connection of the remote system to another storage network. Once the remote system is added and the data connection is established using a storage network, it is recommended to retain the storage network purposes until import is complete. If a different storage network will be used for data import after the remote system is added, the remote system must be deleted and then re-added.

- Heterogeneous host cluster is not supported.
- Configuration changes must not be made during import, such as resizing a volume during import or adding or removing a host node in a cluster configuration, on either the source system or PowerStore. The following configuration changes are allowed but not supported on either the source system or PowerStore during import for consistency groups:
 - Removing members from consistency group
 - Restoring
 - Cloning
 - Snapshot
 - Consistency group migration
 - Creating replication
 - Refreshing volumeSuch operations should be done before starting import.
- Snapshot restore on a volume under import is not supported.
- Only 512b-sector sized devices are supported from the following systems, 4k-sector devices are not supported from these systems:
 - Dell EqualLogic PS
 - Dell Compellent SC
 - Dell Unity
 - Dell VNX2
- Both 512b-sector and 4k-sector resources are supported from XtremIO systems.
- iSCSI hardware initiators are not supported.
- Running in iSCSI Data Center Bridging (DCB) configurations is not supported for Dell EqualLogic PS series and Dell Compellent SC series.
- Do not delete then add the same VNX2 remote system again in a short interval (a few seconds). The Add operation may fail because the software cache on the VNX2 may not have completed being updated. Wait at least five minutes between these operations for the same VNX2 remote system.

CHAP restrictions

The following describes the CHAP support for importing external storage to a PowerStore cluster:

- For Dell Unity and VNX2 systems, source volumes with single CHAP can be imported, but source volumes with mutual CHAP cannot be imported.
- For Dell EqualLogic Peer Storage (PS) series, there are three cases:
 - When Discovery CHAP is disabled, source volumes with both single and mutual CHAP can be imported.
 - If Discovery CHAP is enabled, source volumes with single CHAP can be imported.
 - If Discovery CHAP is enabled, source volumes with mutual CHAP cannot be imported.

NOTE: If Dell Unity or VNX2 systems are added in CHAP enabled mode and if a Dell EqualLogic PS system is added, ensure that Discovery CHAP is enabled for the Dell EqualLogic PS system.

- For Dell Compellent Storage Center (SC) series, source volumes with both single and mutual CHAP can be imported.
- Each host must be added with unique CHAP credentials.

XtremIO XI and X2 support the iSCSI CHAP settings that are listed in [XtremIO XI and X2 supported iSCSI CHAP settings](#).

Table 2. XtremIO XI and X2 supported iSCSI CHAP settings

CHAP Discovery Mode	CHAP Authentication Mode
Disabled	Disabled
Disabled	Either Initiator or Initiator and Target
Initiator	Either Initiator or Initiator and Target

NOTE: The CHAP Discovery Mode **Initiator and Target** setting with either a CHAP Authentication Mode setting of **Initiator** or **Initiator and Target** is not supported.

The PowerStore iSCSI CHAP settings may differ from the XtremIO cluster. Configure the PowerStore iSCSI CHAP settings appropriately before setting up the import session. The supported iSCSI CHAP settings of XtremIO XI and X2 systems and the corresponding settings that should be selected in the **Add Remote System** slide-out panel from **Migration > Importing External Storage > Remote Systems > + Add Remote System** in PowerStore Manager are listed in [PowerStore Manager Add Remote System slide-out panel iSCSI CHAP settings for XtremIO](#).

Table 3. PowerStore Manager Add Remote System slide-out panel iSCSI CHAP settings for XtremIO

Configured XtremIO iSCSI CHAP setting	PowerStore Manager Add Remote System slide-out panel iSCSI CHAP setting
Disabled for CHAP Discovery Mode	Select Disabled for Discovery CHAP Mode.
Initiator for CHAP Discovery Mode	Select Enabled for Discovery CHAP Mode.
Disabled for CHAP Authentication Mode	Select Disabled for Session CHAP Mode.
Initiator for CHAP Authentication Mode	Select Single for Session CHAP Mode.
Initiator and Target for CHAP Authentication Mode	Select Mutual for Session CHAP Mode.

Source system restrictions

Each source system has its own restrictions, for example, the maximum number of volumes supported and the maximum number of iSCSI sessions allowed. Importing external storage to PowerStore must work within these limitations of the source systems and the limitations of the PowerStore cluster.

For restrictions specific to a source system, see the source-specific documentation. Go to Online Support (registration required) at: [Dell Support](#). After logging in, locate the appropriate **Product Support** page.

General restrictions for hosts

The following restrictions apply to hosts:

- (For non-disruptive import) Applications must be configured to use a given MPIO handle. In other words, the host applications must be actively using either EqualLogic MPIO, or Native MPIO. See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs. Use of dynamic multi-pathing (DMP), Secure-Path, and PowerPath MPIOs are not supported.
- (For non-disruptive import) Hosts should have only one MPIO installed that manages both the source and the PowerStore cluster.
- Heterogeneous host cluster is not supported.
- The maximum of a 16 node cluster import is supported.
- During import, the following configuration changes are not supported on the host:
 - (For non-disruptive import) Change of MPIO policy during import.
 - Changes to the paths (enable or disable) which can impact the import operation.
 - Host cluster configuration changes.
 - Operating system upgrades.

Windows-based hosts

The following restrictions apply during a non-disruptive import involving Windows-based hosts:

- Dell Compellent SC is not supported.
- The following Windows Dynamic Disk volume types are not supported:
 - Simple volume
 - Spanned volume
 - Mirrored volume
 - Striped volume
 - RAID 5 volume
- IDE device and SCSI device under Hyper-V configuration are not supported.
- Modifying the operating system disk state after initiating or canceling an import operation is not supported.
- A LUN having more than 32 paths (sum of source and destination paths) is not supported. This restriction is a Windows MPIO limitation.

NOTE: After a Windows host plugin install, certain `LogScsiPassThroughFailure` error messages may occur during import for Dell VNX2 systems. These messages can be ignored. Also, after the I/O path becomes active toward PowerStore during an import operation, all I/Os are bound to one port of the network interface controller.

Linux-based hosts

The following restrictions apply during a non-disruptive import involving Linux-based hosts:

- Change in user-friendly names of volumes being imported is not supported.

NOTE: Any device policy or user-friendly name on the source volume will not be applied to the destination volume after import.

- The `mpathpersist` command fails to get PR information for volumes mapped to clusters after the import. Use `sg_persist`.
- LUNs cannot be removed from the storage group.
- UUID-based mount points with EQL MPIO are not supported.
- Only Linear volume LVM is supported, other LVM types, like striped LVM, are not supported.
- For LVMs, ensure that the option `allow_changes_with_duplicate_pvs` is enabled in `/etc/lvm/lvm.conf`. If this option is set to 0 (disabled), change it to 1 (enabled). Otherwise, imported logical volumes will not become active again after a host reboot if duplicate Port VLAN identifiers (PVIDs) are discovered.
- The maximum length of the hostname must be within 56 characters.
- After or during the import of a volume and after reboot, the `mount` command displays the destination mapper name instead of the source mapper name. The same destination mapper name is listed in the `df -h` output.
- Before importing a volume, the mount point entry in `/etc/fstab` should have the `"nofail"` option to avoid boot failures on host reboots. For example: `/dev/mapper/364842a249255967294824591aa6e1dac /mnt/364842a249255967294824591aa6e1dac ext3 acl,user_xattr,nofail 0 0`
- Import to a PowerStore cluster from a Linux host running Oracle ASM on Dell Compellent SC storage is allowed only when the Oracle configuration uses logical sector size for ASM disk groups. See [Setting the Oracle ASM logical block size](#) for more details.
- The keyword `blacklist` and curly brace should appear in the same line for imports to be successful. For example, `"blacklist { "` in the `/etc/multipath.conf` file.
- If the keyword `blacklist` and curly brace are not in the same line, import will fail. If not present already, modify the `multipath.conf` file manually to the `"blacklist {"` form.
- If the `multipath.conf` file has `blacklist` keyword, such as `product_blacklist`, before the `blacklist` section, move that section after the `blacklist` section for imports to work successfully.

NOTE: Ensure that the disk space on the host is not filled to maximum capacity. Free disk space on the host is needed for import operations.

The following is a known behavior during import on Linux-based hosts:

- After host reboot, during import of the volume, the mount point in `/etc/fstab` points to the source device mapper. However, the output of the `mount` or `df -h` command displays the destination device mapper name.

VMware ESXi-based hosts

The following restrictions apply during a non-disruptive import involving VMware ESXi-based hosts:

- Import is supported only for those datastores that have a 1:1 mapping with a back-end volume.
- Linux Raw Device Mapping (RDM) configurations are not supported.
- If RDM LUNs which are exposed to the VM are imported, the inquiry command on those LUNs will report either the source UID or the destination UID depending on the ESXi cache enablement. If the ESXi cache is enabled and upon inquiry, the source UID would be reported, otherwise the destination UID would be reported.
- If xcopy is tried between imported and non-imported volumes, it will fail gracefully and user copy will be initiated instead.
- ESXi supports only dynamic discovery level CHAP.
- Non-disruptive import does not support vVols. If the host has vVols or a Protocol Endpoint that is mapped, it is recommended not to install the host plugin and to use agentless import instead.

The following restriction applies for an agentless import involving VMware ESXi-based hosts:

- The minimum host operating system version that is required is ESX 6.7 Update 1.

General file-based import restrictions

The following restrictions apply to importing file-based external storage to PowerStore:

- Only a Unified VNX2 or Unified Unity is supported as import source storage system.

NOTE: When you are adding either a Unified VNX2 or Unified Unity as the import source storage system and select **Unified** for its **Capability**, only **iSCSI** is available for the **Data Connection Type**. Fibre Channel cannot be selected. You must also enter an IP address. This configuration is applicable when only a file import is intended to be done, typically from a Unity system used for file only capability. Although the IP address must exist on the remote system, it is not required that it be accessible. Even if the ports or IP addresses are unreachable, the file import operations should succeed. An alert about datapath connectivity being faulty in the remote system details appears but can be disregarded.

- VDM or NAS server containing both NFS exports and SMB shares cannot be imported.

NOTE: PowerStore with operating system version 4.1 or later does support import of a NAS server that contains both NFS exports and SMB shares from a Unity Series platform.

- VDM or NAS server containing multiple SMB servers cannot be imported.
- VNX2 stub-aware import is not supported.
- An option to set readPolicy (full, passthrough, or partial) at a directory or file system level like Unity is not available.
- VDM or NAS server with the NFSv4 protocol enabled cannot be imported (no NFS ACL import).
- VDM or NAS server with Secure NFS or pNFS configured cannot be migrated.
- Do not import replication (although replication can be running during the import).
- Do not import checkpoint/snapshot or checkpoint/snapshot schedule.
- Compressed files are uncompressed during import.
- No transparency on cutover for SMB (even in SMB3 with Continuous Availability).
- NDMP restore is not supported during or after the cutover operation. Any direct data or configuration changes must not be made, otherwise the import is expected to fail.
- Changes to the file mobility network configuration or network issues that occur during an import session may cause an import operation to fail.
- Do not change network attributes (such as MTU size or IP address) and source VDM or NAS server attributes during an import session. These changes can cause an import operation to fail.
- Changes to the attributes of a Unity source NAS server, such as NAS server name, while an associated import session is in progress is not supported.
- File system limitations:
 - VDM or NAS server having a Nested Mount File System (NMFS) cannot be imported.
 - A file system that is mounted directly on DM cannot be imported.
 - A file system that is a replication destination cannot be imported.
 - A file system whose mount path contains more than two slashes cannot be imported.
 - The destination file system size may be larger than the source file system size.
 - The Copy Progress Percentage and Estimated Completion Timestamp that are shown for the Initial Copy and Incremental Copy operation may be imprecise in some instances.
- Rollback limitations:
 - Rollback may be disruptive (NFSv3 clients also have to remount).
 - Rollback of the configuration to the source is very limited.

- Do not import File Transfer Protocol (FTP) or Secure FTP, Hyper Text Transfer Protocol (HTTP), and Common Event Publishing Agent (CEPA) and Common Anti-Virus Agent (CAVA) settings.
- Do not import from unhealthy systems.

NOTE: For example, if a Data Mover (DM) is offline and does not respond during the remote system addition and object discovery for all importable objects, many commands that have to run may fail. Disable the problematic DM in the configuration. This action should allow the import to be created.

- Do not assign the session name of a deleted import session to an import session that is being created. The session name still exists in the file database and is deleted only when the remote system is deleted.
- When you configure an import and select a date and time for the import session to begin, do not schedule the import to begin within 15 minutes of the current time.
- When IP Multi-Tenancy is configured on a Unity system, those NAS servers cannot be imported. Only NAS servers that are configured as part of the default tenant can be imported.

NOTE: A user can change the source configuration, however, that action causes the import to fail.

Restrictions and limitations for SMB-only VDM or NAS server file import

The following restrictions and limitations relate to a SMB-only VDM or NAS server file migration from a respective VNX2 or Unity storage system to a PowerStore appliance:

- Only Unified VNX2 or Unified Unity storage systems are supported as the source storage system in a VDM or NAS server file-based import.
- Only VNX2 storage systems with operating environment (OE) version 8.1.x or later are supported.
- Only Unity storage systems with operating environment (OE) version 5.0.3 or later are supported.
- SMB1 must be enabled on the VNX2 source system. SMB2 and SMB3 are not supported in a VDM file-based import.
- SMB2 must be enabled on the Unity NAS server.

NOTE: SMB2 can be disabled on Unity NAS servers through a service parameter starting with Unity systems running operating environment (OE) version 5.4. If SMB2 is disabled, import of such NAS servers cannot occur in PowerStore systems running operating system version 4.1.x.

- Upgrading a PowerStore appliance when an import session is in progress is not supported.
- Creating an import session when an upgrade session is in progress is not supported.
- PowerStore supports a VDM import session with at most 500 file systems on the source VDM.
- The destination system must have enough available capacity to host the source resources to be imported.
 - PowerStore appliances use a different file system layout than Unified VNX2 storage systems. PowerStore appliances use UFS64 file systems while VNX2 storage systems use UFS32 file systems.
 - Import of deduplicate settings is not supported. During the import session, data is unduplicated and uncompressed.
 - A versioning file and fast clone are imported as a normal file. PowerStore appliances with operating system versions earlier than 3.0 do not support file-based import and File Level Retention (FLR). PowerStore appliances with operating system version 3.0 or later support file-based import and both FLR-E and FLR-C.
- Only udfs-type file systems are imported from the VNX2 source VDM. Import of non-udfs-type file systems or file systems that are mounted on a Nested Mount File System (NMFS) file system are not supported.
- A file system whose mount path contains more than two slashes is not supported. The destination system does not allow file systems with a name containing multiple slashes, for example, /root_vdm_1/a/c.
- Import of a file system that is a replication destination is not supported.
- Import of a checkpoint or checkpoint schedule is not supported.
- If the source replication file system is also the destination file system of a VDM or NAS server import session, failing over the replication session (synchronous or asynchronous) is not allowed until the import is complete.
- Restrictions that are related to Quota import:
 - Import of group quota or inode quota settings is not supported. (The destination system does not support either.)
 - Import of a tree quota whose path contains single quotation marks is not supported. (A VNX2 system can create it, but it cannot be queried or modified.)
- Limitations that are related to Host access:
 - After cutover, read access performance degrades until the related file is migrated.
 - After cutover, write access performance degrades until the VDM or NAS server file migration is completed.

- After cutover, a host cannot write data when the source file system is in the read-only mounted state.
- (Does not apply to PowerStore appliances running operating system 3.0 or later) PowerStore appliances running operating system version 2.1.x or earlier do not support file-based import and FLR.
- After cutover, a host cannot access data when the destination file mobility network cannot access the source file system, which includes the following cases:
 - The network between the source VDM or NAS server file migration interface and the destination file mobility network is disconnected.
 - The source VDM or NAS server is not in either the loaded or mounted state.
 - The user modifies the source export, which makes the file mobility network of the destination system unable to access the source file system.
- Protocol restrictions:
 - Import of NFS settings, multiprotocol settings, and related settings is not supported. For example, LDAP, NIS, local password, group and netgroup files, mount options other than synchronous write, op locks, notify on write, and notify on access.
 - Import of FTP or SFTP (File Transfer Protocol), HTTP (Hyper Text Transfer Protocol) or CEPP (Common Event Publishing Protocol) is not supported.
 - Before importing an SMB NAS server (CIFS server) from either a Unified Unity or VNX2 source system to a PowerStore appliance, you must update the parameter `acl.extacl` to **28** (default setting is 0) on the applicable source system.
- Cancel restrictions and limitations:
 - Only some configuration changes, such as the SMB shares of the destination VDM, or local users along with data changes to the source file systems are rolled back to the source VDM.
- Configuration restrictions and limitations:
 - Import of NTP configuration is not supported.
 - Only enabled network interfaces on the source VDM or NAS server are imported. Disabled network interfaces on the source VDM or NAS server are not imported. (The destination system does not allow you to enable or disable network interfaces.)
 - File Level Retention (FLR) file systems can be imported on PowerStore appliances running operating system version 3.0 or later. However, PowerStore appliances with operating system versions earlier than 3.0 do not support file-based import and FLR.
 - Distributed Hierarchical Storage Management (DHSM)/(Cloud Tiering Appliance (CTA) might be configured on the source VNX2 for archiving inactive files to secondary storage. If DHSM/CTA is configured on the source VNX2 system and a VDM import to a PowerStore cluster is run, all the files on the associated file system are recalled from the secondary storage to the source VNX2.
- Only limited configuration changes to the source VDM and the destination NAS server are supported during import:
 - Shares
 - Local groups
 - Local users
 - Privileges
 - Home directory
 - Distributed File System (DFS) (only pre-existing DFS shares are synchronized during a cancel operation)

Those are also the only configuration settings that are synchronized with the source if the migration is canceled.

Restrictions and limitations for NFS-only VDM file import

The following restrictions and limitations relate to an NFS-only VDM file migration from a VNX2 storage system to a PowerStore cluster:

- Only Unified VNX2 or Unified Unity storage systems are supported as the source storage system in a VDM or NAS server file import.
- Only VNX2 storage systems with operating environment (OE) version 8.1.x or later are supported.
- Only Unity storage systems with operating environment (OE) version 5.0.3 or later are supported.
- Upgrading a PowerStore appliance when an import session is in progress is not supported.
- Creating an import session when an upgrade session is in progress is not supported.
- PowerStore supports a VDM import session with at most 500 file systems on the source VDM.
- The destination system must have enough available capacity to host the source resources to be imported.
 - PowerStore appliances use a different file system layout than Unified VNX2 storage systems. PowerStore appliances use UFS64 file systems while VNX2 storage systems use UFS32 file systems.
 - Import of deduplication settings is not supported.

- A versioning file and fast clone are imported as a normal file. PowerStore appliances with operating system versions earlier than 3.0 do not support file-based import and File Level Retention (FLR) PowerStore appliances with operating system version 3.0 and later support file-based import and both FLR-E and FLR-C.
- Only udfs-type file systems are imported from the VNX2 source VDM. Import of non-udfs-type file systems or file systems that are mounted on a Nested Mount File System (NMFS) file system are not supported.
- A file system whose mount path contains more than two slashes is not supported. The destination system does not allow file systems with a name containing multiple slashes, for example, `/root_vdm_1/a/c`.
- Import of a file system that is a replication destination is not supported.
- Import of a checkpoint or checkpoint schedule is not supported.
- If the source replication file system is also the destination file system of a VDM or NAS server import session, failing over the replication session (synchronous or asynchronous) is not allowed until the import is complete.
- Restrictions that are related to Quota import:
 - Import of group quota or inode quota settings is not supported. (The destination system does not support either.)
 - Import of a tree quota whose path contains single quotation marks is not supported. (A VNX2 system can create it, but it cannot be queried or modified.)
- A VAAI operation is not allowed on either the source or destination systems during and after cutover.
 - A VAAI operation is not allowed on the destination system before cutover.
 - A VAAI operation on the source system must finish before cutover.
- Limitations that are related to Host access:
 - After cutover, read access performance degrades until the related file is imported.
 - After cutover, write access performance degrades until the VDM or NAS server file migration is completed.
 - After cutover, a host cannot write data when the source file system is in the read-only mounted state.
 - PowerStore appliances running operating system version 2.1.x or earlier do not support FLR, and the default import setting is to not import such file systems. However, you can override the default, and those file systems are imported as normal destination file systems (UFS64) without FLR protection. This means that after cutover, locked files can be modified, moved, or deleted on the destination PowerStore appliance, but not on the source VNX2 system. This discrepancy can cause the two file systems to be in an inconsistent state.
 - After cutover, a host cannot access data when the destination file mobility network cannot access the source file system, which includes the following cases:
 - The network between the source VDM file migration interface and the destination file mobility network is disconnected.
 - The source VDM or NAS server is not in either the loaded or mounted state.
 - The user modifies the source export, which makes the destination file mobility network unable to access the source file system.
- Protocol restrictions:
 - Import of SMB, multiprotocol settings, and related settings is not supported when performing an NFS-only import. These settings include settings for SMB server, SMB share path and options, Kerberos key, CAVA (Common AntiVirus Agent), usermapper, and ntmap.
 - Import of a VDM or NAS server using Secure NFS, NFSv4, or pNFS is not supported.
 - Import of FTP or SFTP (File Transfer Protocol), HTTP, or CEPP (Common Event Publishing Protocol) is not supported.
 - The NFS protocol is transparent, but sometimes client access behaviors can be impacted. Client access issues can arise from policy differences between the source VNX2 or Unity system and the destination PowerStore appliance.

i NOTE: NFSv3 I/O is transparent for SP failover and failback during the incremental copy stage. However, if a failover or failback begins as the node is imported, an error may occur, disrupting client access and resulting in an I/O error. This error is resolved when the node is re-synchronized.

i NOTE: NFSv3 operations such as CREATE, MKDIR, SYMLINK, MKNOD, REMOVE, RMDIR, RENAME, and LINK may fail with error during import cutover. For example, before cutover, an operation finishes successfully on the source VNX2 side. However, the client does not receive the response; after cutover, the client retries the same operation silently after cutover in an under layer. For example, if a file has already been removed on the source VNX2 side before cutover, the silent retry of the REMOVE operation fails with a `NFS3ERR_NOENT` message. You may see the remove failure even though the file has been removed on the file system. This failure notification occurs because after cutover, the XID cache that is used to detect duplicated requests does not exist on the destination PowerStore side. The duplicated request cannot be detected during cutover.

- Rollback restrictions and limitations:

- After rollback, a host may need to remount the NFS file system if the interface configurations are different between the source VDMs or NAS servers and the destination NAS Servers.
- Only rollback data changes to the source file systems are supported. Rollback of any configuration changes to the NAS server and file systems on the destination PowerStore appliance is not supported. For example, if you add an NFS export to a file system, a rollback does not add the new NFS export to the source VNX2 storage system.
- Configuration restrictions and limitations:
 - Import of NTP configuration is not supported.
 - Import of server parameter settings (VNX2 server_param settings except for the IP reflect parameter) is not supported.
 - Import of LDAP configuration with Kerberos authentication (SMB server is not imported) is not supported.
 - Import of client certificates, which the LDAP server requires (persona is not supported on the PowerStore appliance), is not supported.
 - Import of customized cipher list for LDAP connection (customized cipher list is not supported on the PowerStore appliance) is not supported.
 - If multiple LDAP servers are configured with different port numbers that are used by the source VDM or NAS server, only the server with the port number equal to the first server is imported.
 - If both NIS and LDAP are configured and taken into effect for the naming service on the source VDM or NAS server, you must select one of them to take effect on the destination NAS server.
 - If local files are configured and taken into effect for the naming service on the source VDM or NAS server, you can select whether the local files take effect on the destination NAS server. The search order of the local files is always higher than NIS or LDAP on the destination NAS server.
 - Only enabled network interfaces on the source VDM or NAS server are imported. Disabled network interfaces on the source VDM or NAS server are not imported. (The destination system does not allow you to enable or disable network interfaces.)
 - FLR file systems can be imported on PowerStore appliances running operating system version 3.0 or later. However, PowerStore appliances with operating system versions earlier than 3.0 do not support file-based import and FLR.
 - Distributed Hierarchical Storage Management (DHSM)/(Cloud Tiering Appliance (CTA) may be configured on the source VNX2 for archiving inactive files to secondary storage. If DHSM/CTA is configured on the source VNX2 system and a VDM import to PowerStore is run, all the files on the associated file system are recalled from the secondary storage to the source VNX2. Those files are then imported to the PowerStore cluster as normal files (that is, no stub files are imported).
 - DHSM/CTA may be configured on the source Unity for archiving inactive files to secondary storage. If DHSM/CTA is configured on the source Unity system and a NAS server import to PowerStore is run, PowerStore brings in CTA stub files (pointers to the cloud objects) as is.
- Restoring NDMP backups:
 - The NDMP backup path on VNX2 is `/root_vdm_xx/FSNAME` while the same path on PowerStore is `/FSNAME`. If any file system of the source VNX2 VDM is protected by NDMP and already backed up, then after VDM file import, those file systems cannot be restored to PowerStore using the original path option. A restore using the original path option fails due to an unavailable destination path. Instead, use the alternative path option.

Importing VNX2 or Unity file systems with File Level Retention (FLR) enabled

PowerStore appliances running operating system version 3.0 or later support both FLR-E and FLR-C. When importing an FLR-enabled file system from a VNX2 or Unity system to a PowerStore appliance, ensure the PowerStore appliance is running operating system version 3.0 or later.

 **NOTE:** PowerStore appliances running operating system version 2.1.x or earlier do not support file-based import and FLR.

Limitations related to host access and NFS datastores

When performing a VDM or NAS server import of FLR-enabled file systems to PowerStore, the source VNX2 Data Mover or NAS server must be running the DHSM service for the import to succeed. Also, if the source DHSM service authentication is set to **None**, you do not need to configure the DHSM credentials, username and password, on PowerStore for import. However, if the source DHSM service authentication is set to either **Basic** or **Digest**, you must configure those credentials at the PowerStore appliance as part of the import configuration. If DHSM is not already configured on the source file system, refer to the VNX2 or Unity system's Unisphere online help or the *VNX Command Line Interface Reference for File or Unity Command Line Interface Reference* for information about setting up the DHSM configuration on the respective source system.

PowerStore appliances do not support FLR on NFS datastores. Therefore, VNX2 or Unity FLR-enabled file systems cannot be imported to PowerStore as NFS datastores. They can only be imported as file system objects.

NOTE: If the source VNX2 or Unity file system is FLR-enabled, you cannot change the destination resource from a file system to an NFS datastore. This action is not allowed.

Port requirements for DHSM when FLR is enabled

The default DHSM service port is 5080 on VNX2, Unity, and PowerStore appliances. However, the VNX2 Data Mover (the physical Data Mover that hosts the VDM that is being imported) that is configured with the DHSM service can be set to a different port than the default. This port must match on both systems in order for the import of FLR-enabled file systems to succeed. To import FLR-enabled file systems when the source VNX2 Data Mover is using another port instead of the default, if possible, change the VNX2 Data Mover that is configured with the DHSM service to use the default port 5080.

Dell VNX2 and Dell Unity port requirements for file-based data import

To import file-based data from a Dell VNX2 system to a PowerStore cluster, PowerStore should be able to access the following ports on the Dell VNX2 system:

- To establish import connections: ports 22, 2022, 443 (for block import only), and 5989 (for block import only)
- For NFS VDM import: ports 111, 1234, and 2049
- For SMB (CIFS) VDM import: port 445
- For FLR-enabled file system import: port 5080

NOTE: On the Dell VNX2 source system, the physical Data Mover that is configured with the DHSM service can be set to a different port than the default port 5080. This port must match on both Dell VNX2 and PowerStore in order for the import of FLR-enabled file systems to succeed. To import FLR-enabled file systems, if the source Dell VNX2 Data Mover is not using the default port, If possible, change the Dell VNX2 Data Mover that is configured with the DHSM service to use the default port 5080 before creating the file import.

NOTE: ICMP or ICMPv6 pings must be allowed.

For more information related to ports on the Dell VNX2 system, refer to the *EMC VNX Series Security Configuration Guide for VNX*.

To import file-based data from a Dell Unity system to a PowerStore cluster, PowerStore should be able to access the following ports on the Dell Unity system:

- To establish import connections: ports 22, 443
- For NFS VDM import: ports 111, 1234, and 2049
- For SMB (CIFS) VDM import: port 445
- For FLR-enabled file system import: port 5080

NOTE: ICMP or ICMPv6 pings must be allowed.

For more information related to ports on the Dell Unity system, refer to the *Dell Unity Family Security Configuration Guide*.

Host plugin installation (block-based non-disruptive import only)

This chapter contains the following information:

Topics:

- [Installing the host plugin for import on a Windows-based host](#)
- [Installing the host plugin for import on a Linux-based host](#)
- [Installing the Dell EqualLogic MEM kit on an ESXi-based host](#)
- [Uninstalling the host plugin for import](#)

Installing the host plugin for import on a Windows-based host

See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for a list of the supported source systems and operating environments that are applicable to Windows-based hosts. In addition to single host, cluster configurations are supported. Also, two variants of the host plugin for import are available for Windows:

- Dell EqualLogic Host Integration Tools Kit
- Dell EMC Import Plugin for Windows (ImportKIT)

NOTE: The MSI installer, which is a Windows component and is spawned when `setup64.exe` runs, runs in the context of SYSTEM account (`msi server`). This process in turn spawns multiple sub-processes which are also named `msiexec.exe`. These sub-processes by default are provided a security right that is called `Log on as a service`. All installer-related services are provided this right by default by the operating system. However, there are specific cases where this right is not provided. In such systems you must use the group policy editor `gpedit.msc`, and assign this right. [Log-on-as-a-service](#) provides more information about this right.

Dell EqualLogic Host Integration Tools Kit

Both upgrade and fresh install are supported for the Dell EqualLogic Host Integration Tools Kit. For a fresh install, run the install file `Setup64.exe`, only once. For more information, see *Dell EqualLogic Host Integration Tools for Microsoft Installation and User's Guide* at [Dell Support](#).

Upgrade has two steps:

1. Run the install wizard, which upgrades existing components.
2. Run the install wizard a second time and select the **Modify** option on the **Program Maintenance** page that appears after you accept the Dell EULA.

Only a single reboot of the host is required for either an upgrade or fresh install.

ImportKIT

The ImportKIT supports native multipath I/O for Dell EqualLogic, Dell Unity, and Dell VNX2 systems and should be installed on all hosts that are part of the host cluster. Upgrade does not apply to this package since it is the first release of the package. Reboot of the host is required after installation.

NOTE: It is recommended to download the latest version of the ImportKIT and use the `.EXE` version of the installer. The `.MSI` version of the installer is provided to support administrative installations. To use the `.MSI` file, see [Pre-requisites for an install using the .MSI file](#).

Install the host plugin for import on a Windows-based host

Prerequisites

Verify the following:

- A supported operating system is running on the host. See the *PowerStore Simple Support Matrix* document at dell.com/powerstoredocs for a list of the supported source systems and operating environments that are applicable to Windows-based hosts.
- No other multipath driver is installed on the host.
- Ensure that MPIO is enabled on the host.

 **NOTE:** Configuring MPIO on the host during import is not supported.

Ensure that you know the management IP address and associated port number to use for import. This network configuration information must be provided so that the host gets added to the PowerStore cluster for import.

About this task

To install the host plugin, do the following:

 **NOTE:** By default, the installation runs interactively. To run the installation in the background, accept all defaults, and accept the Dell EULA, enter one of the following commands after downloading the applicable host plugin package to the host.

- For ImportKIT, enter:

```
Setup64.exe /quiet /v/qn
```

- For EQL HIT Kit with import capability, enter:

```
Setup64.exe /v"MIGSELECTION=1" /s /v/qn V"/q ADDLOCAL=ALL /L C:\setup.log
```

 **NOTE:** To avoid application disruption when running the installation on a Windows Cluster, Hyper-V clusters for example, move the host out of the cluster (maintenance mode) before installing the host plugin. After installing the host plugin and rebooting, rejoin the host to the cluster. The virtual machines running on the host should be moved out and moved back after the installation is complete. To avoid multiple reboots, the ImportKit or Dell EqualLogic HIT kit install can be planned and combined with any other operating system reboot task.

Steps

1. Download the applicable host plugin package to the host.

For Dell EqualLogic PS [download the Dell EqualLogic Host Integration Tools Kit from the Dell EqualLogic support site](#). For Dell EqualLogic, or Unity, or Dell VNX2 systems, download the ImportKIT from the Dell Technologies Support site at [Dell Support](#). See the *PowerStore Simple Support Matrix* document at dell.com/powerstoredocs for the applicable host multipath software versions.

2. As an administrator, run `Setup64.exe` for the host plugin.

 **NOTE:** For Dell EQL HIT Kit, ensure the **Host Integration Tools installation (with import capability)** option is selected on the **Installation Type Selection** page. Also, adding or removing additional components to an already installed Dell EQL HIT Kit version is not supported.

3. Reboot the host.

A reboot of the host is required to complete the installation.

Upgrade the host plugin for import on a Windows-based host

Prerequisites

Verify that the host is running an applicable version of the Windows operating system. See the *PowerStore Simple Support Matrix* document at dell.com/powerstoredocs for a list of the supported source systems and operating environments that are

applicable to Windows-based hosts. Also, ensure you know the management IP address and associated port number to use for import. This network configuration information must be provided so that the host is added to the PowerStore cluster for import.

About this task

To upgrade the EQL HIT Kit host plugin for Windows, do the following:

NOTE: By default, the upgrade runs interactively. To run the upgrade of the EQL HIT Kit in the background, enter the following command after downloading the host plugin update package to the host:

```
Setup64.exe /v"MIGSELECTION=1" /s /v/qn /V"/q ADDLOCAL=ALL /L C:\setup.log
```

NOTE: To avoid application disruption when running the installation on a Windows Cluster, Hyper-V clusters for example, move the host out of the cluster (maintenance mode) before installing the host plugin. After installing the host plugin and rebooting, rejoin the host to the cluster. The virtual machines running on the host should be moved out and moved back after the installation is complete. To avoid multiple reboots, the ImportKit or Dell EqualLogic HIT kit install can be planned and combined with any other operating system reboot task.

Steps

1. Download the [host plugin package update for the Dell EQL HIT Kit to the host](#).
2. As an administrator, run `Setup64.exe` for the host plugin.

NOTE: This install upgrades the existing HIT/ME components.

3. As an administrator, run the install wizard for the host plugin again.

Select the **Modify** option on the **Program Maintenance** page that appears after you accept the Dell EULA.

NOTE: Ensure the **Host Integration Tools installation (with import capability)** option is selected on the **Installation Type Selection** page. If the Dell EQL HIT Kit is installed with import capability, adding or removing additional components to an already installed Dell EQL HIT Kit version is not supported.

4. Reboot the host.
A reboot of the host is required to complete the installation.

Pre-requisites for an install using the .MSI file

The .MSI file must be run with an elevated command prompt, that is, run as Administrator. The following are the pre-requisites for .MSI installation for ImportKit and Equallogic HIT Kit:

- Microsoft Visual C++ runtime redistributable 2015 x64
- Microsoft Native MPIO is installed.
- Microsoft .Net 4.0 is installed.

Installing the host plugin for import on a Linux-based host

See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for a list of the supported source systems and operating environments that are applicable to a Linux-based host.

NOTE: Installing the DellEMC-PowerStore-Import-Plugin-for-Linux kit does not require a host reboot and it does not impact ongoing I/O operations.

Install the host plugin for import on a Linux-based host

Prerequisites

Verify the following on the host:

- Open-iscsi (iscsid) is installed and running.

NOTE: This process is optional in a fibre channel environment.

- sg_utils package is installed.
- For the DellEMC-PowerStore-Import-Plugin-for-Linux kit, multipathd is running.

NOTE: Ensure you know the host server port number, the host iSCSI IP address that will be used to reach the PowerStore cluster, and the host management IP address. This information must be provided during the host plugin installation.

NOTE: Import to PowerStore from a Linux host running Oracle ASM on Dell Compellent SC storage is allowed only when the Oracle configuration uses logical sector size for ASM disk groups. See [Setting the Oracle ASM logical block size](#) for more details.

About this task

To install the DellEMC-PowerStore-Import-Plugin-for-Linux kit, do the following:

NOTE: For information about installing the EQL HIT Kit host plugin, see the *Dell EqualLogic Host Integration Tools for Linux Installation and User's Guide*.

Steps

1. Download the host plugin package, DellEMC-PowerStore-Import-Plugin-for-Linux-*<latest version>*.iso, and the associated file for the GNU Privacy Guard (GPG) key to a temporary directory, such as /temp, from the Dell download site at [Dell Support](#).
2. Copy the downloaded GPG key file and install it.
For example,

```
#rpm --import <GPG key file name>
```

NOTE: The GPG key is required to install the host plugin and must be installed on the host before attempting to install the host plugin.

3. Run the mount command for the host plugin.
For example,

```
#mount DellEMC-PowerStore-Import-Plugin-for-Linux-<latest version>.iso /mnt
```

4. Change to the /mnt directory.
For example,

```
#cd /mnt
```

5. View the items in the /mnt directory for mininstall.
For example,

```
#ls
EULA LICENSES mininstall packages README support
```

6. Install the host plugin.
For example,

```
#./mininstall
```

NOTE: By default, the installation runs interactively. To run the installation in the background instead, accept all defaults, and accept the Dell EULA, then enter the following command after downloading the host plugin package to the host and installing the certificate key:

```
# ./mnt/minstall --noninteractive --accepted-EULA --fcprotocol (or --iscsiprotocol) --adapter=<ip_address>
```

Where ip_address = subnet IP address for MPIO. Failing to provide the --accepted-EULA option cancels a non-interactive installation. Also, the port for the host or hosts is set to 8443 by default.

NOTE: If a firewall exists, ensure it is enabled to allow the port for the host or hosts to be open. For example:

```
# sudo firewall-cmd --zone=public --add-port=8443/tcp
```

Upgrade the host plugin for import on a Linux-based host

Prerequisites

Verify the following on the host:

- Open-iscsi (iscsid) is installed and running.

NOTE: This process is optional in a fibre channel environment.

- GPG key has been installed.
- EqualLogic HIT Kit is running.

About this task

NOTE: The upgrade of the EQL HIT Kit host plugin for Linux is pertinent only for import of external storage from the Dell EqualLogic PS version that is listed in the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs which lists the supported source systems and operating environments that are applicable to a Linux-based host.

To upgrade the EQL HIT Kit host plugin, do the following:

Steps

1. Download the [host plugin package, equallogic-host-tools-<latest version>.iso](#), to a temporary directory, such as /temp, from the Dell EqualLogic support site.
2. Run the mount command for the host plugin.

For example,

```
#mount equallogic-host-tools-<latest version>.iso /mnt
```

3. Change to the /mnt directory.

For example,

```
#cd /mnt
```

4. View the items in the ./mnt directory for install.

For example,

```
#ls
EULA install LICENSES packages README support welcome-to-HIT.pdf
```

5. Install the host plugin.

```
#./install
```

NOTE: By default, the installation runs interactively. To run the installation in the background instead, see the latest version of the *Dell EqualLogic Host Integration Tools for Linux Installation and User's Guide*.

Installing the Dell EqualLogic MEM kit on an ESXi-based host

The following methods exist to install the Dell EqualLogic Multipathing Extension Module (MEM) kit on an ESXi host:

- Command line installation using esxcli commands
- Installation using install script on vSphere Management Assistant (VMA) or vSphere Command-Line Interface (VCLI)
- Installation using VMware Upgrade Manager (VUM)

Download the kit and the associated user guide from the Dell EqualLogic support site.

See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported versions of Dell EqualLogic Peer Storage (PS) source system and Dell EqualLogic MEM kit.

The following configurations are supported:

- Virtual machine file system (VMFS) datastores
- Raw device mapping (RDM) – Windows RDM
 - Clustering Microsoft Clustering Service (MSCS) virtual machines on a single host
 - Clustering virtual machines across physical hosts

NOTE: Linux RDM configurations are not supported.

Install the Dell EqualLogic MEM kit on an ESXi-based host using the vSphere CLI

Prerequisites

Verify that the supported VMware ESXi software is installed and running. See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported versions of Dell EqualLogic Peer Storage (PS) source system and Dell EqualLogic MEM kit.

About this task

NOTE: To avoid application disruption, move the ESXi host out of the cluster before installing the host plugin. After installing the host plugin and rebooting, rejoin the ESXi host with the cluster. Virtual machines should be moved out from the installing host and moved back after the install. Also, to avoid multiple reboots, the Dell EqualLogic MEM kit install can be planned and combined with any other operating system reboot task.

To install the supported Dell EqualLogic MEM kit (see the PowerStore *Simple Support Matrix* document), do the following:

NOTE: To enable only MEM functionality, perform only steps 1, 2 and 6.

Steps

1. Download the latest version of the [Dell EqualLogic MEM kit and associated installation guide from the Dell EqualLogic support site](#).

After login, the kit and its associated installation guide can be found under downloads for VMware Integration.

2. Run the install command.

For example,

```
#esxcli software vib install --depot /var/tmp/dell-eql-mem-esx6-<latest version>.zip
```

The following message appears:

```
Operation finished successfully. Reboot Required: true VIBs
Installed: DellEMC_bootbank_dell EMC-import-hostagent-provider_1.0-14112019.110359,
DellEMC_bootbank_dell EMC-import-satp_1.0-14112019.110359 VIBs Removed: VIBs Skipped:
```

3. Stop `hostd`.

For example,

```
#!/etc/init.d/hostd stop
Terminating watchdog process with PID 67143 hostd stopped.
```

4. Start `hostd`.

For example,

```
#!/etc/init.d/hostd start
```

`hostd` started.

5. Add import command rules.

For example,

```
#esxcli import equalRule add
```

After adding the SATP rules, they can be listed by running the `list` command. For example,

```
#esxcli import equalRule list
```

```
DellEMC_IMPORT_SATP EQLOGIC 100E-00 user VMW_PSP_RR All EQL Arrays DellEMC_IMPORT_SATP
DellEMC PowerStore user VMW_PSP_RR iops=1 All PowerStore Arrays
```

6. Reboot the system.

 **NOTE:** The system must be rebooted before the Dell EqualLogic Multipathing Extension Module with import becomes active.

Install the Dell EqualLogic MEM kit on an ESXi-based host using `setup.pl` script on VMA

Prerequisites

Verify that the supported VMware ESXi software is installed and running. See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported versions of Dell EqualLogic Peer Storage (PS) source system and Dell EqualLogic MEM kit.

About this task

 **NOTE:** To avoid application disruption, move the ESXi host out of the cluster before installing the host plugin. After installing the host plugin and rebooting, rejoin the ESXi host with the cluster. Virtual machines should be moved out from the installing host and moved back after the install. Also, to avoid multiple reboots, the Dell EqualLogic MEM kit install can be planned and combined with any other operating system reboot task.

To install the supported Dell EqualLogic MEM kit (see the PowerStore *Simple Support Matrix* document), do the following:

 **NOTE:** To enable only MEM functionality, in step 3 when prompted for import, respond with **no**.

Steps

1. Download the latest version of the [Dell EqualLogic MEM kit and associated installation guide from the Dell EqualLogic support site](#).

After login, the kit and its associated installation guide can be found under downloads for VMware Integration.

2. Run the `setup.pl` script command on VMA.

The script prompts to install the bundle, then it prompts to enable import. The command uses the following format:

```
./setup.pl -install --server <server name> --username <user name> --password <password> --bundle <bundle name>.
```

For example,

```
./setup.pl -install --server 10.118.186.64 --username root --password my$1234 --bundle /dell-eql-mem-esx6-<version>.zip
```

The following message appears:

```
Clean install of Dell EqualLogic Multipathing Extension Module.
Before install_package call Bundle being installed:
/home/vi-admin/myName/dell-eql-mem-esx6-<latest version>.zip Copying /home/dell-eql-mem-esx6-<latest version>.zip
Do you wish to install the bundle [yes]:
```

3. Type yes to continue.

The following message appears:

```
The install operation may take several minutes. Please do not interrupt it.
Do you wish to enable import? Enabling import would claim all PS and PowerStore volumes by IMPORT SATP and changes the PSP to VMW_PSP_RR [yes]:
```

4. Type yes to continue.

The following message appears:

```
Enabling import functionality. In add_claim_rules Clean install was successful.
```

5. Reboot the system.

 **NOTE:** The system must be rebooted before the Dell EqualLogic Multipathing Extension Module with import becomes active.

Install the Dell EqualLogic MEM kit on an ESXi-based host using VUM

Prerequisites

Verify that the VMware vSphere Upgrade Manager (VUM) is installed on the host. See the PowerStore *Simple Support Matrix* document at dell.com/powerstoredocs for the supported MEM kit to install.

About this task

To install the supported MEM kit, do the following:

Steps

1. Follow the instructions in the VMware documentation to install the supported MEM kit using the VUM method.
2. After the MEM kit is installed, but before rebooting, do the following on all the hosts where the MEM kit is installed:

- a. Stop `hostd`.

For example:

```
#/etc/init.d/hostd stop
Terminating watchdog process with PID 67143 hostd stopped.
```

- b. Start `hostd`.

For example:

```
#/etc/init.d/hostd start  
hostd started.
```

- c. Add import command rules.

For example:

```
#esxcli import equalRule add
```

3. Reboot the system.



NOTE: The system must be rebooted before the Dell EqualLogic Multipathing Extension Module with import becomes active.

Install the Dell EqualLogic MEM kit during an ESXi-based host upgrade

Prerequisites

Verify whether a version earlier than the supported VMware ESXi software is running on the host. See the *PowerStore Simple Support Matrix* document at dell.com/powerstoredocs.

About this task

To install the supported MEM kit (see the *PowerStore Simple Support Matrix* document at dell.com/powerstoredocs) during an upgrade of an earlier version of VMware ESXi software and to avoid multiple reboots, do the following:

Steps

1. Upgrade to the supported VMware ESXi software, but do not reboot the ESXi host.
2. Use one of the following methods to install the supported MEM kit on the prior version of the VMware ESXi software, apply SATP rules, and skip the reboot step in the following methods:
 - Install MEM Using the vSphere CLI [Install the Dell EqualLogic MEM kit on an ESXi-based host using the vSphere CLI](#)
 - Install the Dell EqualLogic MEM kit on an ESXi-based host using setup.pl script on VMA [Install the Dell EqualLogic MEM kit on an ESXi-based host using setup.pl script on VMA](#)
 - Install the Dell EqualLogic MEM kit on an ESXi-based host using VUM [Install the Dell EqualLogic MEM kit on an ESXi-based host using VUM](#)
3. Reboot the host.



NOTE: The system must be rebooted before the Dell EqualLogic Multipathing Extension Module with import becomes active.

Uninstalling the host plugin for import

Uninstalling any of the host plugin software for import is not recommended since it involves host or application down-time and VM/volume re-configuration sometimes. If a host plugin must be uninstalled, contact your service provider.

Import workflows

This chapter contains the following information:

Topics:

- [Non-disruptive import workflow](#)
- [Cutover workflow for non-disruptive import](#)
- [Cancel workflow for non-disruptive import](#)
- [Agentless import workflow](#)
- [Cutover workflow for agentless import](#)
- [Cancel workflow for agentless import](#)
- [File-based import workflow](#)
- [Cutover workflow for file-based import](#)
- [Cancel workflow for file-based import](#)

Non-disruptive import workflow

As part of the import process, the source volume or consistency group is pre-validated whether it is ready to be imported. An import session is not allowed when either a non-disruptive upgrade or a network reconfiguration is in progress.

NOTE: Only source volumes and consistency groups that have a status of **Ready for Import**, **System cannot determine cluster type**, or **All hosts have not been added** can be imported.

The following steps show the manual import workflow in PowerStore Manager:

1. If the source system does not appear in PowerStore Manager, add the information needed to discover and access the source system.

NOTE: (For importing storage from a Dell EqualLogic PS series system only) After you attempt to add a PS series system to PowerStore, the initial data connection state will appear as `No Targets Discovered`. However, you can proceed to create the import session and the state will be updated to `OK` after the import session moves to the `In Progress` state. This behavior is only specific to a PS series system and it is expected.

NOTE: If PowerStore discovery of PowerMax as a remote system fails with an internal error (0xE030100B000C), see the Knowledge Base Article 000200002, *PowerStore: Discovery of PowerMax as a remote system fails with an Internal Error (0xE030100B000C)*.
2. Select the volumes or consistency groups, or both to import.
3. (Optional) Assign selected volumes to a PowerStore Volume Group.
4. Select **Add hosts (Host Plugin) for non-disruptive import** and add the information needed to discover and access the host systems.
5. Set the schedule for the import.
6. (Optional) Assign a protection policy for the import sessions.
7. Review the summary of the import configuration information for accuracy and completeness.
8. Begin the import.

NOTE: The active I/O path between the host and the source system becomes passive and the passive I/O path between the host and the PowerStore cluster becomes active. Also, the background copy of the selected source volumes to the associated PowerStore volumes begins as well as the forwarding of host I/O from the PowerStore cluster to the source system.

You can cutover an import after the background copy operation is complete. After cutover, the source volume is no longer accessible to the associated hosts and the PowerStore cluster.

The states of a single volume import and the manual operations that are allowed for those states are as follows:

- Queued state – Cancel operation
- Scheduled state – Cancel operation
- Copy-In-Progress state – Cancel and Pause operations
- Paused state – Cancel and Resume operations
- Ready-For-Cutover state – Cancel and Cutover operations
- Cleanup-Required state – Cleanup operation
- Import-Completed state – No manual operations available

The states of a consistency group import and the manual operations that are allowed for those states are as follows:

- Queued state – Cancel operation
- Scheduled state – Cancel operation
- In-Progress state – Cancel operation

 **NOTE:** Once the first volume of a CG is picked up for import, the CG state changes to In-Progress. The CG remains in that state until it reaches Ready-For-Cutover.

- Ready-For-Cutover state – Cancel and Cutover operations
- Cleanup-Required state – Cleanup operation
- Cleanup-In-Progress state – No manual operations available
- Cancel-In-Progress state – No manual operations available
- Cancel-failed – Cancel operation
- Cutover-In-Progress state – No manual operations available
- Import-Cutover-Incomplete state – Cancel and Cutover operations
- Import-Completed-With-Errors – No manual operations available
- Import-Completed – No manual operations available
- Failed – Cancel operation

When an import session is paused, only the background copy is stopped. The forwarding of host I/O to the source system continues to be active on the PowerStore cluster.

 **NOTE:** Any I/O failures or network outages can cause import to fail during any of the states.

When a paused import session is resumed, the following occurs:

- For volumes, the import session state changes to Copy-In-Progress. For consistency groups, the state changes to In-Progress.
- The background copy restarts from the last copied range.
- The forwarding of host I/O to the source system continues to be active on the PowerStore cluster.

If an import session fails, the Orchestrator tries to automatically cancel the import operation to restore host I/O back to the source. If a cancel operation fails, the orchestrator will attempt to continue host I/O to the PowerStore cluster. If a catastrophic failure should occur and host I/O cannot continue, the import session state changes to Cleanup-Required. In this state you can run the Cleanup operation, which is specific to the source system. This action sets the source storage resource to Normal and deletes the associated destination storage resource.

Cutover workflow for non-disruptive import

You can cutover an import when the import session reaches the `Ready For Cutover` state. After cutover, the source volume, LUN, or consistency group is no longer accessible to the associated hosts and the PowerStore cluster.

The following steps show the manual import workflow in PowerStore Manager:

1. Select the import session to cutover.
2. Select the **Cutover** import action to cutover to the PowerStore cluster. The following cutover processing occurs:
 - a. Forwarding of host I/O from the PowerStore cluster to the source system stops.
 - b. The volume or volume group status updates to `Import Complete` upon successful cutover.

 **NOTE:** When all the volumes in a volume group are cutover successfully, the state of the import session is set to `Import Complete`. However, since the status of the volume group depends on the final status of the member volumes, if one or more of the member volumes are in a state other than `Import Complete`, the status of the

volume group is set to `Cutover_Failed`. Repeat the cutover operation again until it succeeds and the status for the volume group becomes `Import Complete`.

- c. Hosts and PowerStore cluster access to the source volume, LUN, or consistency group is removed.

NOTE: Import sessions are not deleted. If you want to delete the import session, use the delete operation that is available only through the REST API. For more information about the REST API, see the *PowerStore REST API Reference Guide*.

Cancel workflow for non-disruptive import

You can cancel an import session that is in any of the following states:

- Queued
- Scheduled
- For volume, Copy-in-Progress or, for CG, In-Progress
- Paused
- Ready-for-Cutover
- For CG, Import-Cutover-Incomplete
- For CG, Cancel-Required
- For CG, Cancel-Failed
- For CG, Failed

The cancel operation sets the state of the import session to `CANCELLED` and disables access to the destination volume or volume group. It also deletes the destination volume or volume group that is associated with the import session.

NOTE: After an import session is successfully cancelled, wait five minutes before retrying to import the same volume or consistency group. If you retry the import immediately after the successful cancel operation, the import may fail.

NOTE: A **Force Stop** option is provided in the confirmation popup for Cancel if either a source system or a host is down. Selecting this option terminates the import session without rolling back access to the volumes on the source system. Manual intervention may be required on the source system or host, or both.

The following steps show the manual cancel workflow in PowerStore Manager:

1. Select the import session to cancel.
2. Select the **Cancel** import action to cancel the import session.
3. Click **CANCEL THE IMPORT** in the pop up screen. The following cancel processing occurs:
 - a. The destination volume is disabled.
 - b. The source volume is enabled.
 - c. The state of the import session is set to `CANCELLED` on the successful completion of the operation.

NOTE: When all the volumes in a volume group are cancelled successfully, the state of the import session is set to `CANCELLED`. However, since the status of the volume group depends on the final status of the member volumes, if one or more of the member volumes are in a state other than `CANCELLED`, the status of the volume group is set to `Cancel_Failed`. You must repeat the cancel operation again until it succeeds and the status for the volume group becomes `CANCELLED`.

- d. The destination volume is deleted.

NOTE: Import sessions are not deleted but can be deleted through the REST API.

Agentless import workflow

As part of the import process, the source volume or LUN, or consistency group or storage group is pre-validated whether it is ready to be imported. An import session is not allowed when either a non-disruptive upgrade or a network reconfiguration is in progress.

NOTE: Source volumes and consistency groups can reflect a different status for import that depends on the method of import and the operating environment running on your source system. Storage group, which is a collection of volumes, is the basic unit of storage that is provisioned in a Dell PowerMax or VMAX3 system. Only storage groups can be imported

from Dell PowerMax or VMAX3 systems; individual volumes cannot be imported. Only LUNs can be imported from NetApp AFF A-Series systems, consistency group is not available in ONTAP.

- The **Ready for Agentless Import** status is applicable only when the version of the source system is earlier than the version that is supported for non-disruptive import.
- If the version of the source system supports non-disruptive import but the host plugin is not installed, volumes or consistency group member volumes have the status of **The host or host(s) have not been added..** In such cases, you can choose to do either a non-disruptive or an agentless import. Depending on the type of import you choose, you must do one of the following:
 - For a non-disruptive import, install the host plugin.
 - For an agentless import, under **Compute > Host Information > Host & Host Groups**, select **Add Host** as needed and specify the relevant information for the hosts.

The following steps show the manual import workflow in PowerStore Manager:

1. If the host or hosts do not appear in PowerStore Manager, add the necessary information to discover and access the hosts.
2. If the remote (source) system does not appear in PowerStore Manager, add the necessary information to discover and access the source system.

NOTE: Be aware of the following information related to the specific type of source system:

- For Dell EqualLogic PS series system – After you attempt to add a PS series system to PowerStore, the initial data connection state will appear as *No Targets Discovered*. However, you can create the import session and the state will be updated to *OK* after the import session moves to the *In Progress* state. This behavior is only specific to a PS series system, and it is expected.
- For NetApp AFF A-Series system – A data SVM can be added as a remote system in PowerStore. Also, multiple data SVMs from the same NetApp cluster can be added to PowerStore for import.
- For Dell PowerMax or VMAX3 system – Symmetrix is the legacy name of the Dell VMAX family and the Symmetrix ID is the unique identifier of the PowerMax or VMAX system. Multiple PowerMax or VMAX3 systems that the same Unisphere manages can be added to PowerStore for import.

NOTE: If PowerStore discovery of PowerMax as a remote system fails with an internal error (0xE030100B000C), see the Knowledge Base Article 000200002, *PowerStore: Discovery of PowerMax as a remote system fails with an Internal Error (0xE030100B000C)*.

- For Universal (either a legacy Dell EMC or third-party) storage system – To add the remote system as a Universal type with FC connections, select two FC targets (WWPNs) of the source system. It is advisable to select WWPNs from different nodes of the source system.

3. Select the volumes, or consistency groups, or both, or LUN, or storage group to import.

NOTE: An XtremIO source volume is assigned a World Wide Name (WWN) when it is mapped to a host. PowerStore discovers only such volumes with a WWN for import. For Universal source systems, you must also name the source volumes that are selected for import.

4. (Optional) Assign selected volumes to a PowerStore Volume Group.
5. Select **Map to hosts on PowerStore for agentless import** and map the applicable PowerStore Manager host or hosts to the source volumes or LUNs.

NOTE: (Optional) Volumes within a consistency group can be mapped individually to different hosts.

6. Set the schedule for the import.
7. (Optional) Assign a protection policy for the import sessions.
8. Review the summary of the import configuration information for accuracy and completeness.
9. Submit the import job.

NOTE: Volumes are created on PowerStore Manager. Access functions are set up for the source system so that data can be copied from the source volume or LUN to the destination volume.

10. After the destination volumes reach the Ready To Enable Destination Volume state, shut down the host application accessing the associated source volume, LUN, consistency group, or storage group.

11. Select and enable each destination volume that is in the Ready To Enable Destination Volume state. The destination volumes have to be enabled individually for each member volume of a volume group import session.

NOTE: (For a PowerMax to PowerStore import only) If multiple LUNs exist in the storage group being imported, all the LUNs in the storage group are unmapped immediately when you select **Enable Destination Volume** and select the option to unmap the volumes from the host for import. The source volumes are not visible to the host, and the host cannot access the source volumes. However, this action does not affect the relationship between the source volumes and their existing snapshots and clones.

NOTE: It is recommended to remove the host mapping of the source volume during the enable destination volume process. If the host mappings from the source volume in the source system are not selected to be removed by the orchestrator, remove them manually. If the host mappings of the source volume are not removed either by the orchestrator or manually, those mappings remain even after cutover of the import session. Also, if import fails or is cancelled, these host mappings must be restored to the source volume or volumes manually. They are not restored automatically.

NOTE: For a VMAX3 import, the recommended unmap volumes option deletes the LUN masking views of a volume, which is defined at the storage group level, so hosts cannot access data in the volume through the VMAX3 system. VMAX3 systems provide LUN masking views at the storage group level since the storage group is a container for all volumes that are used by a single application. When the recommended unmap volumes option is selected, the LUN masking view of the storage group is deleted. As all volumes from a single storage group are imported together and the application using these volumes is stopped until all the volumes are reconfigured, deleting the LUN masking view should not affect the migration process. However, if the import is cancelled and the storage group is rediscovered for a retry of the import, the storage group must be remapped to the hosts.

The import session changes to the Ready to start copy state when the enable destination volume action completes.

12. When the import session changes to the Ready to start copy state, rescan the volumes at the host. The destination volumes should be visible to the host after the rescan and destination volumes can be mounted immediately.
13. Ensure that the host application has been reconfigured to access the applicable destination (PowerStore) volumes, then bring up the host application.
14. Select **Start Copy** to start copying the source volume data to the destination volume. **Start copy** must be selected individually for each member volume of a volume group in an import session.

You can cut over an import after the copy operation is complete.

The states of a single volume import and the manual operations that are allowed for those states are as follows:

- Queued state – Cancel operation
- Scheduled state – Cancel operation
- Ready To Enable Destination Volume – Enable destination volume and Cancel operations
- Ready-to-Start-Copy – Start copy and Cancel operations
- Copy-In-Progress state – Cancel and Pause operations
- Paused state – Cancel and Resume operations
- Ready-For-Cutover state – Cancel and Cutover operations
- Cancel-Required – Cancel operation (the agentless import has failed during the copy operation)
- Cleanup-Required state – Clean up operation
- Import-Completed state – No manual operations available

NOTE: Before starting a Cancel operation after the host application has been shut down and reconfigured to use the destination volume in PowerStore, shut down the host application and reconfigure the host application to use the source volume. Shutdown of and reconfiguring the host application to use the source volume are not required when the host application has not been shut down and reconfigured to use the destination volume in PowerStore.

The states of a consistency group import and the manual operations that are allowed for those states are as follows:

- Queued state – Cancel operation
- Scheduled state – Cancel operation
- In-Progress state – Cancel operation

NOTE: Once the first volume of a CG is picked up for import, the CG state changes to In-Progress. The CG remains in that state until it reaches Ready-For-Cutover.

- Ready-For-Cutover state – Cancel and Cutover operations
- Cleanup-Required state – Cleanup operation
- Cleanup-In-Progress state – No manual operations available
- Cancel-In-Progress state – No manual operations available
- Cancel-failed – Cancel operation
- Cancel-Required – Cancel operation (the agentless import has failed during the copy operation)
- Cutover-In-Progress state – No manual operations available
- Import-Cutover-Incomplete state – Cancel and Cutover operations
- Import-Completed-With-Errors – No manual operations available
- Import-Completed – No manual operations available
- Failed – Cancel operation

NOTE: Any I/O failures or network outages can cause import to fail during any of the states. Before starting a Cancel operation after the host application has been shut down and reconfigured to use the destination volume in PowerStore, shut down the host application and reconfigure the host application to use the source volume. If the host application has not been shutdown and reconfigured to use the destination volume in PowerStore, shutdown of and reconfiguring the host application to use the source volume are not required.

When a paused import session is resumed, the following occurs:

- For volumes, the import session state changes to Copy-In-Progress. For consistency groups, the state changes to In-Progress.
- The copy restarts from the last copied range.

NOTE: Any I/O failures or network outages can cause import to fail during any of the states. If agentless import fails due to I/O or network failures, the import session goes into Cancel-Required state. Before starting a Cancel operation after the host application has been shutdown and reconfigured to use the destination volume in PowerStore, shut down the host application and reconfigure the host application to use the source volume. If the host application has not been shut down and reconfigured to use the destination volume in PowerStore, shutdown of and reconfiguring the host application to use the source volume are not required.

Cutover workflow for agentless import

You can cutover an import when the import session reaches the `Ready For Cutover` state. The following steps show the manual import workflow in PowerStore Manager:

1. Select the import session to cutover.
2. Select the **Cutover** import action to cutover to the PowerStore cluster. The volume or volume group status updates to `Import Complete` upon successful cutover.

NOTE: When all the volumes in a volume group are cutover successfully, the state of the import session is set to `Import Complete`. However, since the status of the volume group depends on the final status of the member volumes, if one or more of the member volumes are in a state other than `Import Complete`, the status of the volume group is set to `Cutover_Failed`. Repeat the cutover operation again until it succeeds and the status for the volume group becomes `Import Complete`.

NOTE: Import sessions are not deleted. If you want to delete the import session, use the delete operation that is available only through the REST API. For more information about the REST API, see the *PowerStore REST API Reference Guide*.

Cancel workflow for agentless import

For volume, Cancel can be performed only when the import processing state is `Queued`, `Scheduled`, `Ready To Enable Destination Volume`, `Ready to Start Copy`, `Copy-In-Progress`, `Paused`, `Ready for Cutover`, or `Cancel Required`. For volume group, Cancel can be performed only when the import processing state is `Queued`, `Scheduled`, `In-Progress`, `Paused`, `Ready for Cutover`, `Import-Cutover-Incomplete`, `Cancel Required`, `Cancel-Failed`, or `Failed`. Before cancelling an agentless import session, shut down the host application and reconfigure the host application that is accessing the destination volume or volumes of the import back

to the source volume or volumes. Shutdown of and reconfiguring the host application is applicable only when the import session is being cancelled after the host application has been reconfigured to use the destination volume in PowerStore.

The cancel operation sets the state of the import session to **CANCELLED** and disables access to the destination volume or volume group. It also deletes the destination volume or volume group that is associated with the import session.

NOTE: A **Force Stop** option is not available for Cancel during an agentless import.

The following steps show the manual cancel workflow in PowerStore Manager:

1. Select the import session to cancel.
2. Select the **Cancel** import action to cancel the import session.
3. Click **CANCEL THE IMPORT** in the dialog box.

NOTE: To enable **Cancel The Import**, check the checkbox to confirm that the host application has been shut down or taken offline.

The following cancel processing occurs:

- a. The destination volume is disabled.
- b. The state of the import session is set to **CANCELLED** on the successful completion of the operation.

NOTE: When all the volumes in a volume group are cancelled successfully, the state of the import session is set to **CANCELLED**. However, since the status of the volume group depends on the final status of the member volumes, if one or more of the member volumes are in a state other than **CANCELLED**, the status of the volume group is set to **CANCEL_Failed**. You must repeat the cancel operation again until it succeeds and the status for the volume group becomes **CANCELLED**.

- c. The destination volume is deleted.

NOTE: Import sessions are not deleted but can be deleted through the REST API. Manual intervention is required to reconfigure the host to access the source volumes again.

File-based import workflow

For a file-based import, a file mobility network and file import interface must be configured. Also, the source storage system must be added to the PowerStore cluster before creating a file import session. As part of the file import process, the source VDM or NAS server is pre-validated whether it is ready to be imported. The basic configuration (NAS server name, file systems, production interfaces) of the source file server must not change after the file import session is created. A file import session is not allowed when either a non-disruptive upgrade or a network reconfiguration is in progress.

NOTE: Only VDMs or NAS servers that have a status of **Ready** can be imported.

The following steps show the manual file-based import workflow in PowerStore Manager:

1. Configure the file mobility network.
2. If the remote (source) system does not appear in PowerStore Manager, add the information that is used to discover and access the source system (to establish the import connection).
3. Configure the file import interface.
4. Select the VDM or NAS server to import.
5. Set the schedule for the file import.
6. Assign a protection policy for the file import session.

NOTE: The protection policy is applied to the VDM or NAS server that contains the individual file systems.

7. Review the summary of the import configuration information for accuracy and completeness.
8. Submit the import job.

NOTE: A NAS server is created on PowerStore Manager, and access functions are set up for the source system so that data can be copied from the source VDM or NAS server to the destination NAS server. If an import session is scheduled to start later, the **Import State** is shown as **Scheduled**. However, if two active import sessions (which is the maximum for active import sessions) are running, any new import sessions that are set to start are shown with an **Import State**

of **Queued**. A maximum of ten import sessions can be scheduled or queued. However, only a maximum of eight import sessions can be scheduled or queued while two import sessions are active.

You can cut over a file import after the session state changes to `Ready For Cutover`.

The states of a VDM or NAS server import and the manual operations that are allowed for those states are as follows:

- Scheduled state – Cancel operation
- Queued state – Cancel operation
- In_Progress state – Cancel operation
- Completed – No manual operations available
- Pausing state – Cancel operation
- Paused state – Resume and Cancel operations
- Cancelling – Cancel operation
- Canceled – Cancel operation
- Failed – Cancel operation

When a paused file import session is resumed, the following occurs:

- The state changes to In-Progress.
- The copy restarts from the last copied range.

 **NOTE:** Any I/O failures or network outages can cause a file import to fail during any of the states.

Cutover workflow for file-based import

You can cut over a file-based import when the import session reaches the `Ready For Cutover` state. The following steps show the manual import workflow in PowerStore Manager:

 **NOTE:** If the source NAS server has Common Anti-Virus Agent (CAVA) enabled, disable CAVA before proceeding to cutover. This action helps to avoid potential data unavailability to NAS clients until the session is committed.

1. Select the file import session to cut over.
2. Select the **Cutover** import action to cut over to the PowerStore cluster. The following cutover processing occurs:

 **NOTE:** Cutover may cause a temporary data unavailability to the NAS clients.

- The production file interfaces are disabled on the source system and are enabled on the destination system.

 **NOTE:** For an SMB import, the switch-over is disruptive for the clients and the Active Directory configuration is imported if needed. For an NFS import, the switch-over is transparent as file handles are preserved, NLM locks are reclaimed on the destination.

- The incremental background data copy operation begins after the cutover completes. The file system data is moved to the destination in the background.
- The destination system serves the clients; client-requested data is synchronized immediately; write operations are synchronized back to the source system before acknowledging, so the source remains authoritative and a rollback is possible at any time. I/O throughput is degraded at this stage.

 **NOTE:** If the source data becomes unavailable, the service is interrupted.

When all files are synchronized, the file import session transitions to `Ready For Commit`.

Cancel workflow for file-based import

You can cancel a file import session that is in any one of the following states:

- Queued
- Scheduled
- In_Progress

- Pausing
- Paused

The cancel operation sets the state of the file import session to `CANCELLED` and disables access to the destination NAS server. It also deletes the destination NAS server that is associated with the file import session.

NOTE: A **Force Stop** option is provided in the confirmation dialog box for Cancel if a source system is down. Selecting this option terminates the file import session without rolling back access to the VDM on the source system. Manual intervention may be required on the source system. Also, if a cancel occurs during or after the cutover operation, clients are switched back to the source system. This action may be disruptive.

The following steps show the manual cancel workflow in PowerStore Manager:

1. Select the file import session to cancel.
2. Select the **Cancel** import action to cancel the file import session.
3. Click **Cancel The Import** in the confirmation dialog box for Cancel. The following cancel processing occurs:
 - a. For the selected file import session, data transfer between the source system and PowerStore is stopped, and all data that is imported to PowerStore is removed.
 - b. Production interfaces are disabled on the destination side and enabled on the source side. Cancel is disruptive for NFS and SMB clients.
 - c. The state of the import session is set to `CANCELLED` on the successful completion of the operation.

NOTE: When all the file systems in a NAS server are cancelled successfully, the state of the file import session is set to `CANCELLED`. However, since the status of the NAS server is dependent on the final status of the member file systems, if one or more of the member file systems are in a state other than `CANCELLED`, the status of the NAS server is set to `CANCEL_Failed`. You must repeat the cancel operation again until it succeeds and the status for the NAS server becomes `CANCELLED`.

- d. The destination NAS server is deleted.

NOTE: You can rerun the file import later, but it does not resume from where the previous import was cancelled.

Configuring and managing import

This chapter contains the following information:

Topics:

- [Configure a non-disruptive import](#)
- [Refresh hosts and volumes in a non-disruptive import](#)
- [Manage non-disruptive import sessions](#)
- [Configure an agentless import](#)
- [Configure an agentless import for a Universal type remote system](#)
- [Manage agentless import sessions](#)
- [Configure a File Mobility Network for file-based import](#)
- [Configure the connection to a remote system for file-based import](#)
- [Configure file import interface](#)
- [Configure a file-based import](#)
- [Manage file-based import sessions](#)

Configure a non-disruptive import

Prerequisites

Ensure the following conditions exist on the PowerStore cluster before running import:

- The global storage IP address for the PowerStore cluster is configured.
- The PowerStore cluster and its nodes are in a healthy state.

Ensure that the following connections exist:

- For a Dell Peer Storage (PS) Series or Dell Storage Center (SC) Series source system, an iSCSI connection between the source system and each associated host system, and a matching iSCSI connection between each associated host system and the PowerStore cluster.
- For a Dell PS Series or Dell SC Series source system, only an iSCSI connection is supported between the source system and the PowerStore cluster.
- For a Dell Unity Series or Dell VNX2 Series source system, a Fibre Channel (FC) or iSCSI connection between the source system and each associated host system, and a matching FC or iSCSI connection between each associated host system and the PowerStore cluster. Also, all host initiators that are connected to the source system should also be connected to the PowerStore cluster.

NOTE: These connections to each host system should be of the same type, either all FC or all iSCSI.

- For a Dell Unity Series or Dell VNX2 Series source system, a FC or iSCSI connection between the source system and the PowerStore cluster.

NOTE: Either an iSCSI connections or a FC connection is supported between a Dell Unity Series or Dell VNX2 Series source system and the PowerStore cluster. However, the connection between the Dell Unity Series or Dell VNX2 Series source system and the PowerStore cluster, and the connections between the hosts and the Dell Unity Series or Dell VNX2 Series source system and between the hosts and the PowerStore cluster must be either all over iSCSI or all over FC.

- Importing data from an external source system into PowerStore with FC connectivity requires that ports 0 and 1 of PowerStore I/O Module0 are enabled as Dual (as both initiator and target).

NOTE: To view the list of FC import capable ports on a PowerStore appliance in PowerStore Manager, under **Hardware** select **Ports**. Then, select **Fibre Channel** on the **Ports** card.

- For FC connections, it is recommended to configure FC zoning in such a way that PowerStore can connect to at least to 2 distinct targets on each remote system controller from a PowerStore node. .

Ensure the following conditions exist on the hosts before running import:

- The applicable host multipath input/output (MPIO) software and host plugin are installed on each host that accesses the storage to be imported. See [Non-disruptive import of external storage to PowerStore overview](#).
- For RHEL version 8.x, the current Security Enhanced Linux (SELinux) status for enforcing is set to disabled. To determine the SELinux status, do the following on the host:
 1. Run `getenforce`.

NOTE: If it is set to permissive or enforced, disable it in `/etc/selinux/config`. Change `SELINUX=enforcing` to `SELINUX=disabled`.

2. Reboot the host. SELinux will be disabled persistently.

NOTE: If you do not want to reboot the host, the configuration will clear after `reboot setenforce 0`.

It is recommended that the same NTP server is used on the source system, which hosts the source storage resource, and the destination PowerStore cluster. This configuration should provide the proper time synchronization between the source system and the destination PowerStore cluster.

Determine the following for the source system:

NOTE: The operation to add either a Dell Unity Series or a Dell VNX2 Series remote system may fail if the health of that source system is not OK. Ensure that the health of the remote system is OK before adding it.

- The type of source system for the import
- The management cluster IP address or FQDN, which is one of the following:
 - For the Dell PS Series, it is the group management IP address, if the management network is configured. Otherwise, it is the group IP address.
 - For the Dell SC Series and Dell Unity Series, it is the management IP address of the system.
 - For Dell VNX2 Series, it is the IP address of either SPA or SPB, however, the IP address of SPA is recommended.
- The data connection type, iSCSI or Fibre Channel.
- The iSCSI IP address of the source system, which is one of the following:
 - For Dell PS Series, it is the group IP address.
 - For Dell SC Series, it is the IP address of the fault domain.
 - For Dell Unity Series or Dell VNX2 Series, it is one of the IP addresses of the iSCSI front-end ports.
- The administrative username and password credentials to access the source system
- The session CHAP mode
- The names of the volumes or consistency groups, or both

NOTE: A volume group is automatically created for each consistency group that is selected for import. They cannot be combined with any other volumes or volume group.

- Which protection policy to use for the volume or volume group, or both.

NOTE: PowerStore automatically creates the host and its initiator records on the remote system as part of the import operation. However, PowerStore cannot differentiate whether the initiator records created on a Unity system are created by the user or the import operation. Addition of a Unity system always fails if the PowerStore initiators already exist in the Unity system. For example, during the delete operation of a Unity remote system, the connections from PowerStore to Unity are logged out and an attempt is made to remove the host/initiator that was automatically created. Since Unity is dual mode, the connection from PowerStore to Unity is logged out, but the connection from Unity to PowerStore is not logged out. Unity does not log out the connection to PowerStore. Only those PowerStore initiators used for import must be manually removed from the FC zone by doing the following:

1. Temporarily remove the PowerStore appliance from the FC zone.
2. Remove the initiator on the Unity side.
3. Add PowerStore back into the FC zone.
4. Add the Unity remote system to PowerStore.

Determine the following for the hosts connected to the PowerStore cluster:

- The management IP address of the hosts

- Host plugin port configured for import
- The operating system type of the hosts
- The administrative username and password credentials to access the VMware hosts.

NOTE: Username and password credentials are not required to access the Windows and Linux hosts.

Determine the schedule of the import:

- Immediately or set a time and date
- Whether to automatically cutover to the destination after import

Determine which protection policy to assign to the import session.

About this task

To configure an import, do the following:

Steps

1. Log in to PowerStore Manager.
2. Under **Migration**, select **Import External Storage**.
The **Import External Storage** page appears.
3. If the intended source system does not appear in the list of remote systems, select **Add Remote System** and specify the relevant information for the remote system. Otherwise, go to the next step.

NOTE: When an invalid, unreachable, or down group management IP address is added to a PowerStore cluster for any Dell PS Series remote system, the following error notification appears: Addition of PS remote system failed due to error in connecting PS Group as Unknown error 0 returned by the server.

Verify that the IP address is correct and reachable.

NOTE: Also, after you attempt to add a Dell PS Series remote system to the PowerStore cluster, the initial data connection state will appear as `No Targets Discovered`. However, you can proceed to create the import session and the state will be updated to `OK` after the import session moves to the `In Progress` state. This behavior is only specific to a Dell PS Series remote system and it is expected.

NOTE: While adding a remote system to PowerStore, you must provide the iSCSI IP address of the remote system along with other details. As part of the operation, PowerStore discovers the iSCSI portal of the remote system and tries to log in to all the targets listed in that portal. If anyone of those targets are unreachable, the associated **Data Connection** status appears as `Partial Data Connections Loss` in PowerStore Manager.

4. To configure an import session, select a source system from the list of remote systems on your network that you have previously entered manually in to PowerStore Manager.
 5. Select **Import Volume**.
The **Import Volumes from Source Array** wizard appears.
 6. Step through the wizard and specify the relevant information.
- NOTE:** Only volumes and consistency groups that have a status of `Ready for import`, `System cannot determine cluster type`, or `Host or Hosts have not been added` can be selected for import. However for a status of `Host or Hosts have not been added`, you must add all hosts in the `Add Hosts` step in the import wizard before beginning an import session. You cannot begin an import session when the volume or consistency group has a status of `Import is in progress` or `Import has completed`.

NOTE: Consistency Group is not supported in the Dell PS Series systems; therefore, consistency group import from these systems is not possible.

Once you have specified the necessary information, the system generates a summary of the import session information.

7. Verify that the import session information in the summary is accurate and complete.
8. Click **Begin Import** to create and start the import session.
The **Import External Storage** page appears and shows the **Imports** information once the operation is started.
9. To view the progress of ongoing import sessions, under **Migration**, select **Block Imports**.
10. To view the progress details of a specific ongoing import session, click the state of that import session.

The **Import Session Details** slide out for that import session appears.

Refresh hosts and volumes in a non-disruptive import

About this task

When any configuration changes, such as moving a volume between hosts or re-sizing the source system volume capacity, are made to the source or a host system after they have been added to PowerStore, all the affected or involved systems must be manually refreshed using PowerStore Manager. Otherwise, when you run import on that volume, the import will fail.

To refresh the source volumes or hosts, or both, do the following:

Steps

1. In PowerStore Manager, do the following to navigate to the **Import Volumes from Source Array** wizard:
 - a. Under **Migration**, select **Import External Storage**.
 - b. Select the source system from the list of **Remote Systems**.
 - c. Select **Import Volume**.
2. To refresh hosts, select **Refresh Hosts** under **Refresh Actions**; otherwise, go to Step 3.
 - a. Select **Refresh Hosts** for a host that must be refreshed.
 - b. When the **Host Refresh** dialog box appears confirming a successful operation, do one of the following as applicable:
 - Click **Close** to return to the **Import Volumes from Source Array** wizard.
 - Click **Refresh Other Hosts** to return to the **Refresh Hosts** slide out panel.
3. To refresh volumes, select **Refresh Volumes**.

Manage non-disruptive import sessions

About this task

An import session runs as a background job and establishes an end-to-end path for an import operation between a source and destination. The data follows the path as it moves from source to destination.

Steps

1. Under **Migration**, select **Import External Storage**.
The **Import External Storage** page appears and lists information about the existing remote systems.
2. Select **Block Imports**.
The **Import External Storage** page changes and lists information about the existing block import sessions.
3. Perform one of the following import actions:

 **NOTE:** The import actions that can be performed on an import session depend on the current state of the import session.

Action	Description
Cancel	Select an import session and under Import Actions, click Cancel. You can cancel an import session that is in one of the following states: • Queued • Scheduled • For volume, Copy In Progress, or, for consistency group, In Progress • Paused • Ready For Cutover • For consistency group, Import Cutover Incomplete • For consistency group, Cancel Failed • For consistency group, Failed The cancel operation sets the state of the import session to CANCELLED and disables access to the destination volume. It also deletes the destination volume or volume group that is associated with the import session.

Action	Description
	i NOTE: When all the volumes in a volume group are canceled successfully, the state of the import session is set to <code>CANCELLED</code>. However, if one or more of the member volumes are in a state other than <code>CANCELLED</code>, the status of the volume group is set to <code>Cancel Failed</code>. This action occurs because the status of the volume group depends on the final status of the member volumes. Repeat the cancel operation again until it succeeds and the status for the volume group becomes <code>CANCELLED</code>. i NOTE: Import sessions are not deleted. If you want to delete the import session, use the delete operation that is available only through the REST API. i NOTE: A Force Stop option is provided in the confirmation dialog box for Cancel if either a source system or a host is down. Selecting this option terminates the import session without rolling back access to the volumes on the source system. Manual intervention may be required on the source system or host, or both. i NOTE: After an import session is successfully cancelled, wait five minutes before retrying to import the same volume or consistency group. If you try the import again immediately after the successful cancel operation, the import may fail.
Cutover	i NOTE: Before performing the cutover, ensure that you can access your data as expected. You cannot revert after this step. Select an import session and under Import Actions, click Cutover to commit an import session. You can cut over an import session that is in the <code>Ready For Cutover</code> state. After cutover, the source volume or source consistency group is no longer accessible to the associated hosts and the PowerStore cluster. i NOTE: When all the volumes in a consistency group are cut over successfully, the state of the import session is set to <code>Import Complete</code>. However, if one or more of the member volumes are in a state other than <code>Import Complete</code>, the status of the consistency group is set to <code>Cutover Failed</code>. This action occurs because the status of the consistency group depends on the final status of the member volumes. Remove all the failed volumes from the consistency group and try the import again. i NOTE: After one set of imports is completed, run the next set of imports after a delay of 10 minutes. This delay allows enough time for the system to cleanup any connections to the source system.
Pause	Select an import session and under Import Actions, click Pause. Use Pause to pause an import session that is in the <code>Copy In Progress</code> state. i NOTE: The Pause import action on a CG only pauses the member volumes that are in the <code>Copy In Progress</code> state. The CG remains in the <code>In Progress</code> state. Other member volumes that are in other states, such as <code>Queued</code> or <code>In Progress</code>, are not paused and may proceed to the <code>Ready For Cutover</code> state. The other member volumes can be paused when they reach the <code>Copy In Progress</code> state by using the Pause import action again on the CG. If any of the member volumes are in the <code>Paused</code> state but the overall status of the CG is <code>In Progress</code>, both the Pause and Resume import action options are available for the CG.
Resume	Select an import session and under Import Actions, click Resume. Use Resume to start an import session that is in the <code>Paused</code> state.
Cleanup	Select an import session and under Import Actions, click Cleanup. Use Cleanup to cleanup an import session that is in the <code>Cleanup Required</code> state.

i NOTE: If import of a source volume is in progress and a disaster occurs making the source system unusable or unreachable, you may need to contact your service provider to recover the source system involved in the import.

i NOTE: During an import session with a Dell PS Series source system that has `not shared` volumes, those volumes are changed to `shared` volumes as part of the import processing. If that import session is canceled or fails, the Access Control List of the Group Manager shows that the Multiple access field remains as `shared`. Since the job has failed or has been canceled, it is assumed that the import on the same volume will be retried. The Multiple access field setting is not automatically reverted to `not shared`.

Configure an agentless import

Prerequisites

NOTE: The information that is presented here is applicable to importing external storage to PowerStore from the following remote system types:

- Dell Peer Storage (PS) Series
- Dell Storage Center (SC) Series
- Dell Unity Series
- Dell VNX2 Series
- Dell XtremIO X1 or Dell XtremIO X2
- Dell PowerMax and VMAX3
- NetApp AFF A-Series

For information about importing external storage to PowerStore from a Universal type of remote system, see [Configure an agentless import for a Universal type remote system](#).

Ensure that the following conditions exist on the PowerStore cluster before running import:

- The global storage IP address for the PowerStore cluster is configured.
- The PowerStore cluster and its nodes are in a healthy state.

Ensure that the following connections exist:

- For either a Dell SC Series, Dell Unity Series, Dell VNX2 Series, Dell XtremIO X1 or XtremIO X2, or a NetApp AFF A-Series source system, a Fibre Channel (FC) or iSCSI connection between the source system and each associated host system, and a matching FC or iSCSI connection between each associated host system and the PowerStore cluster.

NOTE: These connections to each host system should be of the same type, either all FC or all iSCSI.

- For a Dell PS Series source system, an iSCSI connection between the source system and each associated host system, and a matching iSCSI connection between each associated host system and the PowerStore cluster.
- For a Dell PowerMax or VMAX3 source system, an FC connection between the source system and each associated host system, and a matching FC connection between each associated host system and the PowerStore cluster.
- Only an iSCSI connection is supported between Dell PS Series source systems and the PowerStore cluster.

NOTE: For an iSCSI connection, the purpose of the storage network that will be used for import must be set for both **Storage (iSCSI)** and **Replication**. You can set the purpose on the **Network Details** step of the **Create Storage Network** wizard (**Settings > Network IPs > Storage > Create**). To view the mapped storage networks of a port and their purposes, under **Hardware** select **Ports**. Then, select **Ethernet** on the **Ports** card. See the PowerStore Manager online help and the PowerStore Protecting Your Data Guide for more information about creating a storage network and setting the purpose of a remote system.

- Only an FC connection is supported between a Dell PowerMax or VMAX3 source system and the PowerStore cluster.
- Either an iSCSI connection or an FC connection is supported between a Dell SC Series, Dell Unity Series, Dell VNX2 Series, Dell XtremIO X1 or XtremIO X2 source system, or a NetApp AFF A-Series source system and the PowerStore cluster.

NOTE: For an iSCSI connection, the purpose of the storage network that will be used for import must be set for both **Storage (iSCSI)** and **Replication**. You can set the purpose on the **Network Details** step of the **Create Storage Network** wizard (**Settings > Network IPs > Storage > Create**). To view the mapped storage networks of a port and their purposes, under **Hardware** select **Ports**. Then, select **Ethernet** on the **Ports** card. See the PowerStore Manager online help and the PowerStore Protecting Your Data Guide for more information about creating a storage network and setting the purpose of a remote system.

NOTE: When the connections between the source system and the PowerStore cluster are all over iSCSI, the connections between the hosts and a source system and between the hosts and the PowerStore cluster can be either all over iSCSI or all over FC. However, when the connections between the source system and the PowerStore cluster are all over FC, the connections between the hosts and a source system and between the hosts and the PowerStore cluster must also be all over FC.

- Importing data from an external source system into PowerStore with FC connectivity requires that ports 0 and 1 of PowerStore I/O Module0 are enabled as Dual (as both initiator and target).

NOTE: To view the list of FC import capable ports on a PowerStore appliance in PowerStore Manager, under **Hardware** select **Ports**. Then, select **Fibre Channel** on the **Ports** card.

- For FC connections, it is recommended to configure FC zoning in such a way that PowerStore can connect to at least two distinct targets on each remote system controller from a PowerStore node.

It is recommended that the same NTP server is used on the source system, which hosts the source storage resource, and the destination PowerStore cluster. This configuration should provide the proper time synchronization between the source system and the destination PowerStore cluster.

Determine the following for the source system:

NOTE: Ensure that the health of the remote system is OK before adding it. If the health of that source system is not OK, the operation to add any of the following remote systems may fail:

- Dell Peer Storage (PS) Series
- Dell Storage Center (SC) Series
- Dell Unity Series
- Dell VNX2 Series
- Dell XtremIO X1 or Dell XtremIO X2
- NetApp AFF A-Series
- The type of source system for the import
- The name of the source system (applicable only to Dell XtremIO X1 or XtremIO X2, PowerMax, VMAX3 systems, and NetApp AFF A-Series systems)

NOTE: For Dell PowerMax and VMAX3 systems, the name is the Symmetrix ID. For NetApp AFF A-Series systems, the name is the Storage Virtual Machine (SVM) name.

- The management cluster IP address or FQDN. The IP address is one of the following:
 - For the Dell PS Series, the group management IP address, if the management network is configured. Otherwise, it is the group IP address.
 - For the Dell SC Series and Dell Unity Series systems, the management IP address of the system.
 - For Dell VNX2 Series, the IP address of either SPA or SPB; however, the IP address of SPA is recommended.
 - For Dell XtremIO X1 and XtremIO X2 systems, the IP address of the XMS.
 - For Dell PowerMax and VMAX3, the Unisphere IP address and associated port number.
- The iSCSI IP address of the source system, which is one of the following:
 - For Dell PS Series, the group IP address.
 - For Dell SC Series, the IP address of the fault domain.
 - For Dell Unity Series, Dell VNX2, Dell XtremIO X1 and XtremIO X2 source systems, one of the IP addresses of the iSCSI front-end ports. For NetApp AFF A-Series systems, the iSCSI IP address (Logical Interface (LIF)) of the SVM.
- The administrative username and password credentials to access the source system.
- The session CHAP mode.
- The names of the volumes or consistency groups, or both, or LUNs, or storage group.

NOTE: A volume group is automatically created for each consistency group or storage group that is selected for import. They cannot be combined with any other volumes or volume group, or storage group.

- Which protection policy to use for the volume or volume group, or both, or LUN, or storage group.

NOTE: PowerStore automatically creates the host and its initiator records on the remote system as part of the import operation. However, PowerStore cannot differentiate whether the user or the import operation creates the initiator records on a Dell Unity Series system. If the PowerStore initiators exist in the Unity system, the addition of a Dell Unity Series system always fails. For example, during the delete operation of a Unity remote system, the connections from PowerStore to Unity are logged out and an attempt is made to remove the host/initiator that was automatically created. Since Unity is dual-mode, the connection from PowerStore to Unity is logged out, but the connection from Unity to PowerStore is not logged out. Unity does not log out the connection to PowerStore. Only those initiators that are used for import must be manually removed from the FC zone by doing the following:

1. Temporarily remove the PowerStore appliance from the FC zone.

2. Remove the initiator on the Unity side.
3. Add PowerStore back into the FC zone.
4. Add the Unity remote system to PowerStore.

Determine which hosts should be mapped to the PowerStore volumes.

Determine the schedule of the import:

- Immediately or set a time and date.

NOTE: When you configure an import and select a date and time for the import session to begin, do not schedule the import to begin within 15 minutes of the current time.

- Whether to automatically cut over to the destination after import.

Determine which protection policy to assign to the import volume.

About this task

To configure an import, do the following:

Steps

1. Log in to PowerStore Manager.
2. If the intended hosts that are associated with the import do not appear under **Compute > Host Information > Hosts & Host Groups**, select **Add Host** as needed and specify the relevant information for the hosts. Otherwise, go to the next step.
3. Under **Migration**, select **Import External Storage**.
The **Import External Storage** page appears.
4. If the intended source system does not appear in the list of Remote Systems, select **Add Remote System** and specify the relevant information for the remote system. Otherwise, go to the next step.

NOTE: When an invalid, unreachable, or down group management IP address is added to a PowerStore cluster for any Dell PS Series remote system, the following error notification appears: `Addition of PS remote system failed due to error in connecting PS Group as Unknown error 0 returned by the server.`

Verify that the IP address is correct and reachable.

NOTE: Also, after you attempt to add a Dell PS Series remote system to the PowerStore cluster, the initial data connection state will appear as `No Targets Discovered`. However, you can create the import session and the state will be updated to `OK` after the import session moves to the `In Progress` state. This behavior is only specific to a Dell PS Series remote system, and it is expected.

NOTE: While adding a remote system to PowerStore, you must provide the iSCSI IP address of the remote system along with other details. As part of the operation, PowerStore discovers the iSCSI portal of the remote system and tries to log in to all the targets listed in that portal. If anyone of those targets is unreachable, the associated **Data Connection** status appears as `Partial Data Connections Loss` in PowerStore Manager.
5. To configure an import session, select a source system from the list of remote systems on your network that you have previously entered manually in to PowerStore Manager.
6. Select **Import Volume**.
The **Import Volumes from Source Array** wizard appears.
7. Step through the wizard and specify the relevant information.

NOTE: Only source volumes and consistency groups that have a status of **Ready for Agentless Import** can be imported. **Ready for Agentless Import** is applicable only when the version of the source system is earlier than the version that is supported for non-disruptive import. However, if the version of the source system supports non-disruptive import and the host plugin is not installed, volumes or consistency group member volumes have the status **The host or host(s) have not been added..** In such cases, you can choose to do non-disruptive or agentless import. Depending on the type of import you choose, you must either install the host plugin or select the PowerStore host, respectively.

NOTE: An XtremIO source volume is assigned a World Wide Name (WWN) when it is mapped to a host. PowerStore discovers only such volumes with a WWN for import.

NOTE: Consistency Group is not supported in the Dell PS Series systems. Consistency group import from these systems is not possible.

Once you have specified the necessary information, the system generates a summary of the import session information.

8. Verify that the import session information in the summary is accurate and complete.

9. Click **Begin Import** to create and start the import session.

The **Import External Storage** page appears and shows the **Block Imports** information once the operation is started.

10. After the destination volume reaches the Ready To Enable Destination Volume state, shut down the host application accessing the source volume.

NOTE: When importing VMFS datastores, do the following from vCenter to unmount the datastore before proceeding to enable the destination:

- a. Power off the Virtual Machines (VMs).
- b. Unregister the VMs by right clicking and selecting **Remove from inventory** on each VM in the datastore.
- c. Right-click the datastore and select **Unmount datastore**.

11. When the volume in the import session is in the Ready To Enable Destination Volume state, select the volume and then select **Import Actions > Enable Destination Volume**.

The **Enable Destination Volume** dialog box appears.

12. Select the checkbox to confirm that you have shut down or taken offline the host application that is using the source volume.

13. Select whether to have the orchestrator automatically remove the host mappings during the enable destination volume process.

NOTE: It is recommended to remove the host mapping of the source volume during the enable destination volume process to prevent the host from accidentally accessing the source volume. If the orchestrator does not select the host mappings to be removed from the source volume in the source system, remove them manually. If the host mappings of the source volume are not removed either by the orchestrator or manually, those mappings remain even after cutover of the import session. Also, if import fails or is cancelled, these host mappings must be restored to the source volume manually. They are not restored automatically.

NOTE: (For a PowerMax to PowerStore import only) If multiple LUNs exist in the storage group being imported, all the LUNs in the storage group are unmapped immediately when you select **Enable Destination Volume** and select the option to unmap the volumes from the host for import. The source volumes are not visible to the host, and the host cannot access the source volumes. However, this action does not affect the relationship between the source volumes and their existing snapshots and clones.

NOTE: For a VMAX3 import, the recommended unmap volumes option deletes the LUN masking views of a volume, which is defined at the storage group level, so hosts cannot access data in the volume through the VMAX3 system. VMAX3 systems provide LUN masking views at the storage group level since the storage group is a container for all volumes that are used by a single application. When the recommended unmap volumes option is selected, the LUN masking view of the storage group is deleted. As all volumes from a single storage group are imported together and the application using these volumes is stopped until all the volumes are reconfigured, deleting the LUN masking view should not affect the migration process. However, if the import is cancelled and the storage group is rediscovered for a retry of the import, the storage group must be remapped to the hosts.

NOTE: For Dell PS Series systems, if the source volume is setup using access control lists (ACLs) that are based on Basic Access Point or Access Policy Group, the automated removal of host to source volume mapping does not work. You must manually remove the host mapping and log out. Also, when the Dell PS Series source volume is setup using ACLs based on Access Policy, the automated removal of host to source volume mapping removes the host mapping from the source volume. However, the iSCSI connections between the host and the source volume must be manually disconnected by logging out.

14. Select **Enable Destination Volume**.

The volume should progress to the Ready to start copy state.

15. When the import session changes to the Ready to start copy state, rescan the volumes at the host.

NOTE: The rescan at the host may take up to approximately 3 minutes to complete depending on the size of the volumes.

The destination volumes should be visible to the host after the rescan and those volumes can be mounted immediately.

16. Ensure that the host application has been reconfigured to access the applicable destination PowerStore volumes, then bring up the host application.
 - NOTE:** When importing VMFS datastores, do the following from vCenter:
 - a. Rescan the ESX storage adapter on which LUNs are visible.
 - b. Add the datastore back and select the **Assign a new signature** option.
 - c. Register the VMs by right-clicking the datastore and selecting **Register VM....** Do this operation for each VM that is in the datastore.
 - d. Power on the VMs.
17. When the volume in the import session is in the `Ready to start copy` state, select the volume and then select **Import Actions > Start Copy**.

The volume should progress to the `Copy in progress` state.
18. To view the progress of ongoing import sessions, under **Migration**, select **Import External Storage > Block Imports**.
19. To view the progress details of a specific ongoing import session, click the state of that import session. The **Import Session Progress Details** slide out for that import session appears.
20. Do one of the following to continue to manage the agentless import session:
 - Select an import session and under **Import Actions**, click **Cutover** to commit the import session.
 - NOTE:** You can cut over an import session that is in the `Ready For Cutover` state.
 - Cancel the import operation.
 - NOTE:** See [Manage agentless import sessions](#) for more information.

Configure an agentless import for a Universal type remote system

Prerequisites

- NOTE:** The information that is presented here is only applicable to importing external storage to PowerStore from a Universal type of remote system. For information about importing external storage to the following remote system types, see [Configure an agentless import](#).
 - Dell Peer Storage (PS) Series
 - Dell Storage Center (SC) Series
 - Dell Unity Series
 - Dell VNX2 Series
 - Dell XtremIO X1 or Dell XtremIO X2
 - Dell PowerMax and VMAX3
 - NetApp AFF A-Series

Ensure that the following conditions exist on the PowerStore cluster before running import:

- The global storage IP address for the PowerStore cluster is configured.
- The PowerStore cluster and its nodes are in a healthy state.

Ensure that the following connections exist:

- For a Universal (either a legacy Dell EMC or third-party) source system, a Fibre Channel (FC) or iSCSI connection between the source system and each associated host system, and a matching FC or iSCSI connection between each associated host system and the PowerStore cluster.

- NOTE:** These connections to each host system should be of the same type, either all FC or all iSCSI.
- Either an iSCSI connection or an FC connection is supported between a Universal source system and the PowerStore cluster.

NOTE: For an iSCSI connection, the purpose of the storage network that will be used for import must be set for both **Storage (iSCSI)** and **Replication**. You can set the purpose on the **Network Details** step of the **Create Storage Network** wizard (**Settings > Network IPs > Storage > Create**). To view the mapped storage networks of a port and their purposes, under **Hardware** select **Ports**. Then, select **Ethernet** on the **Ports** card. See the PowerStore Manager online help and the PowerStore Protecting Your Data Guide for more information about creating a storage network and setting the purpose of a remote system.

NOTE: When the connections between the Universal source system and the PowerStore cluster are all over iSCSI, the connections between the hosts and the Universal source system and between the hosts and the PowerStore cluster can be either all over iSCSI or all over FC. However, when the connections between the Universal source system and the PowerStore cluster are all over FC, the connections between the hosts and the Universal source system and between the hosts and the PowerStore cluster must also be all over FC.

- Importing data from an external source system into PowerStore with FC connectivity requires that ports 0 and 1 of PowerStore I/O Module0 are enabled as Dual (as both initiator and target).
- For FC connections, it is recommended to configure FC zoning in such a way that PowerStore can connect to at least two distinct targets on each remote system controller from a PowerStore node.

It is recommended that the same NTP server is used on the source system, which hosts the source storage resource, and the destination PowerStore cluster. This configuration should provide the proper time synchronization between the source system and the destination PowerStore cluster.

Determine the following for the source system:

- The type of source system that is selected for the import is **Universal**.
- The name of the source system
- The management cluster IP address or FQDN. For type **Universal**, see the documentation for the applicable remote system.

NOTE: PowerStore opens a new tab in the browser and uses this address to connect with the Universal remote system.

- The data connection type, either iSCSI IP or fibre channel.

NOTE: For the IP address of the source system, see the documentation for the applicable remote system. Multiple IP addresses can be entered separated with a comma.

- (For iSCSI IP only) The Discovery CHAP mode.
- (For iSCSI IP only) The Session CHAP mode.
- (For fibre channel only) The FC targets must be selected from those that are discovered.
- The names of the volumes.
- Which protection policy to use for the volume or volume group.

Determine which hosts should be mapped to the PowerStore volumes.

Determine the schedule of the import:

- Immediately or set a time and date.

NOTE: When you configure an import and select a date and time for the import session to begin, do not schedule the import to begin within 15 minutes of the current time.

- Whether to automatically cut over to the destination after import.

Determine which protection policy to assign to the import volume.

NOTE: The protection policy must exist.

About this task

To configure an import, do the following:

Steps

1. Log in to PowerStore Manager.

2. If the intended hosts that are associated with the import do not appear under **Compute > Host Information > Hosts & Host Groups**, select **Add Host** as needed and specify the relevant information for the hosts. Otherwise, go to the next step.
3. Under **Migration**, select **Import External Storage**.
The **Import External Storage** page appears.
4. If the intended source system does not appear in the list of Remote Systems, select **Add Remote System** and specify the relevant information for the remote system. Otherwise, go to the next step.

Verify that the IP address is correct and reachable.

NOTE: While adding a remote system to PowerStore, you must provide the iSCSI IP address of the remote system along with other details. As part of the operation, PowerStore discovers the iSCSI portal of the remote system and tries to log in to all the targets listed in that portal. If anyone of those targets is unreachable, the associated **Data Connection** status appears as `Partial Data Connections Loss` in PowerStore Manager.

5. Create PowerStore as a host on the remote system and do one of the following:

NOTE: When adding PowerStore as a host on the remote system, specify the PowerStore cluster name.

- For iSCSI, specify the HBAs that PowerStore will use to send I/O requests to the remote system.

NOTE: To view a list of the IQNs on the PowerStore appliance in PowerStore Manager, under **Hardware** select **Ports**. Then, select **Ethernet** on the **Ports** card. If the column IQN is not visible, select the IQN column to be visible. Also only the IQNs that are related to the storage network (with **Replication** purpose) that is used for import traffic must be added to the created host in the source system.

- For FC, specify the WWNs that PowerStore will use to send I/O requests to the remote system.

NOTE: Only the WWNs of FC ports that have **Import Capable** as **Yes** must be added to the created host in the source system. To view the list of the FC import capable ports on a PowerStore appliance in PowerStore Manager, under **Hardware** select **Ports**. Then, select **Fibre Channel** on the **Ports** card.

NOTE: IQNs or WWNs from all the appliances of the PowerStore cluster must be added to the created host in the source system. Ensure that all the PowerStore initiators have an active connection or initiator path to the source system. The host setting in the source system must ensure that the volume or CG that is mapped to it is visible to all the initiators in the host.

6. Select the newly created PowerStore host on the remote system and ensure that it is configured correctly.

NOTE: The host setting in the source system must ensure that the volume or CG that is mapped to it is visible to all the initiators in the host.

7. On the Universal remote system, map the volume or volumes to be imported to the PowerStore appliance.

NOTE: Up to 128 volumes can be mapped to import to a PowerStore cluster at one time. More or remaining volumes can be mapped and imported to PowerStore after the current set of volumes are imported.

8. To configure an import session, select a source system from the list of remote systems on your network that you have previously entered manually in to PowerStore Manager.

9. Select **Import Volume**.
The **Import Volumes from Source Array** wizard appears.

10. Select **Refresh Volumes** to discover the volumes that have been mapped on the Universal remote system to the PowerStore appliance.

11. Step through the wizard and specify the relevant information.

NOTE: Only source volumes that have a status of **Ready for Agentless Import** can be imported.

NOTE: For a Universal source system, the name of the volumes appears as a dash (–) the first time after discovery. You must provide a name for the volumes before they can be selected for import. Select the applicable volumes, then select **Name Volume** to update the name of the volumes. Up to 10 volumes at a time can be selected for naming. Click **Apply** to update the list of volumes. The name should appear in place of the dash (–). After all the applicable volumes have been named, select those volumes again and click **Next** to continue.

NOTE: Only volumes are discovered for a Universal type remote system. Consistency groups are not discovered. If a consistency group exists on the source system and should also exist on the destination, PowerStore Manager provides options to create it and to add the applicable volumes to it. When a consistency group is created in this manner, a volume group is automatically created in place of the consistency group on PowerStore during import. If you would like to group discovered individual volumes as a volume group when they are imported, PowerStore Manager provides options to create the volume group and to add the applicable volumes to it.

Once you have specified the necessary information, the system generates a summary of the import session information.

12. Verify that the import session information in the summary is accurate and complete.

13. Click **Begin Import** to create and start the import session.

The **Import External Storage** page appears and shows the **Block Imports** information once the operation is started.

14. After the destination volume reaches the Ready To Enable Destination Volume state, shut down the host application accessing the source volume.

15. When the volume in the import session is in the Ready To Enable Destination Volume state, select the volume and then select **Import Actions > Enable Destination Volume**.

The **Enable Destination Volume** dialog box appears.

16. Select the checkbox to confirm that you have shut down or taken offline the host application that is using the source volume.

NOTE: It is recommended to manually remove the host mapping of the source volume during the enable destination volume process to prevent the host from accidentally accessing the source volume. If the host mappings of the source volume are not removed manually, those mappings remain even after cutover of the import session. Also, if import fails or is cancelled, those host mappings must be restored to the source volume manually. They are not restored automatically.

17. Select **Enable Destination Volume**.

The volume should progress to the Ready to start copy state.

18. When the import session changes to the Ready to start copy state, rescan the volumes at the host.

NOTE: The rescan at the host may take up to approximately 3 minutes to complete depending on the size of the volumes.

The destination volumes should be visible to the host after the rescan and those volumes can be mounted immediately.

19. Ensure that the host application has been reconfigured to access the applicable destination PowerStore volumes, then bring up the host application.

NOTE: When importing VMFS datastores, do the following from vCenter:

- a. Rescan the ESX storage adapter on which LUNs are visible.
- b. Add the datastore back and select the **Assign a new signature** option.
- c. Register the VMs by right-clicking the datastore and selecting **Register VM....** Do this operation for each VM that is in the datastore.
- d. Power on the VMs.

20. When the volume in the import session is in the Ready to start copy state, select the volume and then select **Import Actions > Start Copy**.

The volume should progress to the Copy in progress state.

21. To view the progress of ongoing import sessions, under **Migration**, select **Imports**.

22. To view the progress details of a specific ongoing import session, click the state of that import session.

The **Import Session Progress Details** slide out for that import session appears.

23. Do one of the following to continue to manage the agentless import session:

- Select an import session and under **Import Actions**, click **Cutover** to commit the import session.

NOTE: You can cut over an import session that is in the Ready For Cutover state.

- Cancel the import operation.

NOTE: See [Manage agentless import sessions](#) for more information.

Manage agentless import sessions

About this task

An import session runs as a background job and establishes an end-to-end path for an import operation between a source and destination. The data follows the path as it moves from source to destination.

Steps

1. Under **Migration**, select **Import External Storage**.
The **Import External Storage** page appears and lists information about the existing remote systems.
2. Select **Block Imports**.
The **Import External Storage** page changes and lists information about the existing block import sessions.
3. Perform one of the following import actions:

 **NOTE:** The import actions that can be performed on an import session depend on the current state of the import session.

Action	Description
Cancel	 NOTE: For volume, Cancel can be performed only when the import processing state is <code>Queued</code>, <code>Scheduled</code>, <code>Ready To Enable Destination Volume</code>, <code>Ready to Start Copy</code>, <code>Copy In Progress</code>, <code>Paused</code>, <code>Ready For Cutover</code>, or <code>Cancel Required</code>, and the host application that is accessing the volume has been shut down and reconfigured to access the source volume. For volume group, Cancel can be performed only when the import processing state is <code>Queued</code>, <code>Scheduled</code>, <code>In Progress</code>, <code>Paused</code>, <code>Ready For Cutover</code>, <code>Import Cutover Incomplete</code>, <code>Cancel Required</code>, <code>Cancel Failed</code>, <code>Failed</code>, and the host application that is accessing the volume has been shut down. Before canceling an agentless import session, reconfigure the host application that is accessing the destination volume of the import back to the source volume. This action is applicable when the import session is being cancelled after the host application has been reconfigured to use the destination volume in PowerStore.  NOTE: For VMFS datastores, canceling an import when the import processing state is <code>Ready To Start Copy</code>, <code>Copy In Progress</code>, or <code>Ready For Cutover</code> requires additional steps: a. Power off the Virtual Machines (VMs). b. Unregister the VMs by right clicking and selecting Remove from inventory on each VM in the datastore. c. Right-click the datastore and select Unmount datastore. These additional steps for VMFS datastores are not needed when canceling an import and the import processing state is <code>Queued</code> or <code>Ready To Enable Destination Volume</code>. Select an import session and under Import Actions, click Cancel. The cancel operation sets the state of the import session to <code>CANCELLED</code> and disables access to the destination volume. It also deletes the destination volume or volume group that is associated with the import session.  NOTE: For VMFS datastores, canceling an import when the import processing state is <code>Ready To Start Copy</code>, <code>Copy In Progress</code>, or <code>Ready For Cutover</code> requires additional steps after the import session is cancelled: a. You must map the LUN from the source system now since the map was removed from the source system in the <code>Enable Destination Volume</code> step. b. After the LUN is mapped, rescan the ESX storage adapter on which the LUNs are visible. c. Add the datastore back to the ESX host and select Assign a new signature for the datastore mount. d. Register the VMs by right-clicking the datastore and selecting Register VM.... Do this operation for each VM that is in the datastore. e. Power on the VMs.

Action	Description
	These additional steps for VMFS datastores are not needed when canceling an import and the import processing state is <code>Queued</code> or <code>Ready To Enable Destination Volume</code>. NOTE: When all the volumes in a volume group are cancelled successfully, the state of the import session is set to <code>CANCELLED</code>. However, since the status of the volume group depends on the final status of the member volumes, if one or more of the member volumes are in a state other than <code>CANCELLED</code>, the status of the volume group is set to <code>Cancel Failed</code>. Repeat the cancel operation again until it succeeds and the status for the volume group becomes <code>CANCELLED</code>. NOTE: Import sessions are not deleted. If you want to delete the import session, use the delete operation that is available only through the REST API. Manual intervention is required to reconfigure the host to access the source volumes again. NOTE: A Force Stop option is not available for Cancel during an agentless import.
Cutover	NOTE: Before performing the cutover, ensure that you can access your data as expected. You cannot revert after this step. Select an import session and under Import Actions, click Cutover to commit an import session. You can cut over an import session that is in the <code>Ready For Cutover</code> state. NOTE: When all the volumes in a consistency group are cut over successfully, the state of the import session is set to <code>Import Complete</code>. However, since the status of the consistency group depends on the final status of the member volumes, if one or more of the member volumes are in a state other than <code>Import Complete</code>, the status of the consistency group is set to <code>Cutover_Failed</code>. You must remove all the failed volumes from the consistency group and try the import again. NOTE: After performing the cutover, ensure to remove the host mappings of the source volume in the source array. Also, after one set of imports is completed, run the next set of imports after a delay of 10 minutes. This delay allows enough time for the system to cleanup any connections to the source system.
Pause	Select an import session and under Import Actions, click Pause. Use Pause to pause an import session that is in the <code>Copy In Progress</code> state. NOTE: The Pause import action on a CG only pauses the member volumes that are in the <code>Copy In Progress</code> state. The CG remains in the <code>In Progress</code> state. Other member volumes that are in other states, such as <code>Queued</code> or <code>In Progress</code>, are not paused and may go to the <code>Ready For Cutover</code> state. The other member volumes can be paused when they reach the <code>Copy In Progress</code> state by using the Pause import action again on the CG. If any of the member volumes are in the <code>Paused</code> state but the overall status of the CG is <code>In Progress</code>, both the Pause and Resume import action options are available for the CG.
Resume	Select an import session and under Import Actions, click Resume. Use Resume to start an import session that is in the <code>Paused</code> state.
Cleanup	Select an import session and under Import Actions, click Cleanup. Use Cleanup to cleanup an import session that is in the <code>Cleanup Required</code> state.
Enable Destination Volume	Select each destination volume in the import session that is in the <code>Ready To Enable Destination Volume</code> state and under Import Actions, click Enable Destination Volume. NOTE: The import session changes to the <code>Ready to Start Copy</code> state when the enable destination volume action completes for all the volumes in the import session.
Start Copy	When the import session has reached the <code>Ready to Start Copy</code> state, select each destination volume in the import session that is in the <code>Ready to Start Copy</code> state and under Import Actions, click Start Copy.

- NOTE:** If import of a source volume is in progress and a disaster occurs making the source system unusable or unreachable, you may need to contact your service provider to recover the source system involved in the import.
- NOTE:** During an import session with a Dell PS Series source system that has `not shared` volumes, those volumes are changed to `shared` volumes as part of the import processing. If that import session is cancelled or fails, the Access Control List of the EqualLogic Group Manager shows that the Multiple access field remains as `shared`. Since the job has failed or has been cancelled, it is assumed that the import on the same volume will be retried. The Multiple access field setting is not automatically reverted to `not shared`.

Configure a File Mobility Network for file-based import

About this task

A file mobility network is a prerequisite infrastructure that is needed for the exchange of control traffic between NAS clusters in a file import environment. The configuration consists of the following IP addresses:

- A file mobility cluster IP address for the PowerStore appliance
- A file mobility IP address for Node A of the PowerStore appliance
- A file mobility IP address for Node B of the PowerStore appliance

Once the file mobility network is created, its IP addresses must be mapped to the PowerStore management interface. To configure a file mobility network for file-based import, do the following:

- NOTE:** For general information about file mobility network, see the PowerStore Manager online help. For detailed information about configuring a file mobility network, see the *PowerStore T and Q Networking Guide for Storage Services*.

Steps

1. In PowerStore Manager, select **Settings** and under **Networking** select **Network IPs**.
The **Network IPs** page appears.
2. Select the **File Mobility** tab.
3. Select **Create**.
The **Create File Mobility Network** slide out panel appears.
4. Specify the relevant information to create the file mobility network and then click **Create**.
The File Mobility Cluster is created.
5. Select **Map Network** to map the file mobility network to the PowerStore management interface.

Configure the connection to a remote system for file-based import

Prerequisites

Once the file mobility interface has been configured, you can add the remote system to establish the import connection with which to connect to the PowerStore appliance. You must enter the IP address of the source SPA or SPB and the credentials of a user with administrator privileges on the source system when you add the remote system. After adding the remote system, you are ready to create your file import session.

Ensure the following:

- For a source VNX system with two control stations, the home directory of a user with the Administrator role, which is used in configuring the remote system connection, must exist on the primary control station of the VNX.
- The remote system does not exist in the list of remote systems.
- For a VDM or NAS server import, ensure that file import interfaces are configured on each node of the destination system.
- The relevant SP and node pairs (source SPA and destination Node A or source SPB and destination Node B) are up and running.

- If STIG is enabled for the PowerStore cluster, ensure the SSL certificate of the VNX2 system or Unity system is FIPS compliant with a SHA256 signature algorithm.

i NOTE: For example, if the VNX2 system SSL certificate uses a non-FIPS compliant signature algorithm, make the following changes for IP_ADDR, HOSTNAME_SHORT, HOSTNAME_LONG, x509_extensions, and default_md in the configuration file `/nas/http/conf/celeerrssl.cnf` on the VNX2 system:

- IP_ADDR = *<management IP address of VNX system>*
- HOSTNAME_SHORT = *<HOSTNAME_SHORT for VNX>*
- HOSTNAME_LONG = *<HOSTNAME_LONG for VNX>*
- x509_extensions = v3_ca
- default_md = sha256

After the changes have been made in the configuration file, run the following openssl command for signature algorithm conversion:

- `usr/bin/openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout ssl.key/ssl_key.<HOSTNAME for VNX>-CS0 -out ssl.crt/ssl.crt.<HOSTNAME for VNX>-CS0 -config /nas/http/conf/celeerrssl.cnf`

After completing the conversion, check the algorithm using the following command:

- `/usr/bin/openssl x509 -in ssl.crt/ssl.crt.<HOSTNAME for VNX>-CS0.crt -text`

i NOTE: When adding a Unified VNX2 or Unity remote system for importing external storage and the block import capability is added successfully but the file Import capability fails, the **Add Remote System** operation should still be successful. However, a **File Not Ready** alert should appear in Unisphere which means the **Add Remote System** operation for file has failed. The failure can occur for several reasons, for example, an incorrect service password, the FQDN is passed instead of the management IP address, or SSH is disabled. Identify and fix the issue, and then do one of the following:

- Run the **Verify and Update** operation to retry adding the file replication capability.
- Run the **Modify** operation to retry adding the file import capability.

Obtain the SP IP management address and associated user credentials that are used to connect to the source system.

i NOTE: When you are adding either a Unified VNX2 or Unified Unity as the import source storage system and select **Unified** for its **Capability**, only **iSCSI** is available for the **Data Connection Type**, Fibre Channel cannot be selected. You must also enter an IP address. This configuration is applicable when only a file import is intended to be done, typically from a Unity system used for file only capability. Although the IP address must exist on the remote system, it is not required that it be accessible. Even if the ports or IP addresses are unreachable, the file import operations should succeed. An alert about datapath connectivity being faulty in the remote system details appears but can be disregarded.

Steps

1. In PowerStore Manager, under **Migration** select **Import External Storage**.
2. Perform one of the following actions:
 - To add a remote system for file import to PowerStore, select **+Add**. On the **Add Remote System** slide-out panel, specify the relevant information.
 - To modify an import connection, click the name of the remote system. On the **Properties** window, specify the relevant SP (SPA or SPB) IP address, username, and password to authenticate to the SP of the source storage system.
 - If new file import interfaces were added, or existing file import interfaces were deleted, the source system information may become outdated. Select the relevant remote system, and then select **Verify and Update** to update the source system information to pick up the latest file import interface changes on the destination and source systems.
 - If new source storage resources were added, or existing source storage resources were deleted or modified after you add a remote system and before you create an import session to the source system, you must rediscover the source storage system resources. Select the relevant remote system and then select **Discover** to rediscover the source system resources.
 - To manage a remote system, select the remote system, and then under **More Actions** select **Manage**. This action launches the native UI manager of the source system in a new tab in the browser.
 - If the certificate of the remote system has been renewed, select the remote system, and then under **More Actions** select **Update certificate**.
 - To delete a remote system, select the remote system, and then under **More Actions** select **Delete**.

NOTE: Before you delete a remote system, ensure that all ongoing or scheduled block imports are allowed to complete or be cancelled and all file import sessions are deleted before deleting the remote system. Deleting a remote system is idempotent. The remote system is updated to `Partial_delete` on failures. In these cases, the delete remote system operation can be retried to complete the delete.

Configure file import interface

Prerequisites

File import interface is configured to support VDM or NAS server imports and must be created after adding a remote system and discovering its importable objects.

NOTE: This procedure describes adding a file import interface by using the **File Import Interface** tab on the **Import External Storage** page in PowerStore Manager. The file import interface can be added later as part of the configuration of a NAS server import.

Ensure the following:

- The interface port is cabled and connected to a network switch.
- Both Node A and Node B are in a healthy state.

NOTE: For Unity, ensure that I/O clients are not connected to the production interface that is used as the File-Import-Interface connection of the destination system.

Obtain the following information for each Node:

- IP address associated with the file import interface. You can specify an IPv4 or IPv6-based address, but ensure that you specify the same type of address for both nodes.
- IP address mask or prefix length that identifies the associated subnet.
- Gateway IP address associated with the interface.
- If applicable, the VLAN ID (between 1 and 4095) you want to associate the interface with.

NOTE: For the network to continue functioning properly, only set the VLAN ID after configuring the network switch port to support VLAN tagging of multiple VLAN IDs. Ensure that the VLAN ID of the interface is different than the VLAN ID of the management, storage, and NAS servers.

Steps

1. In PowerStore Manager, under **Migration** select **Import External Storage**.
2. Perform one of the following actions:
 - To create an interface, select **+Add**. On the **Add File Import Interface** slide out panel, specify the relevant information.
 - To modify an interface, select the interface and then select **Modify**. On the **Modify File Import Interface** slide out panel, specify the relevant information.
 - To delete an interface, select the interface and then select **Delete**.

NOTE: Before you delete a file import interface, ensure that an import session is not using the interface. If an import session is not using the interface, select **Delete** in the **Delete File Import Interface** dialog box.

Configure a file-based import

Prerequisites

Ensure that the following conditions exist on the PowerStore cluster before running a file import:

- The global storage IP address for the PowerStore cluster is configured.
- The PowerStore cluster and its nodes are in a healthy state.

Ensure the following on the source system:

- The source storage system has been added to the PowerStore configuration before creating a file import session.

NOTE: The basic configuration (NAS server name, file systems, production interfaces) of the source file server must not change after the file import session is created.

- The source VNX VDM or Unity NAS server has at least one client network interface, and exactly one attached network interface that is named `nas_migration_<name>`, where `<name>` is a unique name that is provided to the interface, such as `nas_migration_vdm2`.

NOTE: The PowerStore import application uses this interface throughout the migration. This interface must be added to the CIFS Server in a separate subdomain. This action ensures that any hosts querying the DNS do not get directed to the migration interface. The VDM or NAS server must contain only a single CIFS Server and no NFS exports. Also, there can be no host access on the NAS migration interface.

- There can be no host access on the NAS migration interface. Either disable the SMB2 Multi-channel feature, or add the NAS migration interface into a separate subnet.

NOTE: After adding the production interface to a NAS server on a Unity system, clients may immediately connect to it. In this case, the Unity NAS server is dynamically updating DNS with the new IP address. However, file-based import to PowerStore does not support this NAS server setup in a Unity system. You must update the parameter `updateMode` to **0** (default setting is 2) on the Unity system before importing an SMB NAS server (CIFS server) to a PowerStore appliance. Use the `svc_nas` service command:

```
svc_nas <NASservername> -param -facility dns -modify updateMode -value 0
```

Before restarting the NAS server, remove the migration IP address from DNS so that clients do not use it. Then, restart the NAS server:

```
svc_nas <NASservername> -restart
```

If the `updateMode` value in the Unity environment must be changed back, it can be verified and reset to the default **2** as needed once the migration is committed. Also, once the migration is complete, re-enable dynamic DNS updates by setting the parameter to **2** on the new PowerStore NAS server as it will have migrated over the disabled setting. For more information about using Unity service commands, see the *Dell Unity Family Service Commands Technical Notes*. For information about using PowerStore service commands, see the *PowerStore Service Scripts Guide*.

- For import from a VNX2 system, verify that the physical Data Mover on which the source VDM is located has at least one IP Interface configured that is not attached to the VDM being migrated. This verification ensures that the source Data Mover can provide uninterrupted Name Services for the remaining file servers. If this additional interface is not present, the file import session fails.
- For import from either a Unified Unity or VNX2 source system, you must update the parameter `acl.extacl` to **28** (default setting is 0) on the applicable source system before importing an SMB NAS server (CIFS server) to a PowerStore appliance.

NOTE: Do one of the following on the source system:

- For Unity, use the `svc_nas` service command:

```
svc_nas <NASservername> -param -facility cifs -modify acl.extacl -value 28
```

For more information about using Unity service commands, see the *Dell Unity Family Service Commands Technical Notes*.

- For VNX2, modify the `acl.extacl` adjustable VNX server parameter of the cifs facility:

```
server_param <servername> -f cifs -modify acl.extacl -value 28
```

For more information about modifying an adjustable VNX server parameter, see the *VNX Series Parameters Guide for VNX for File*.

- If the remote system must be added during the configuration, determine whether an iSCSI connection or an FC connection will exist between the Dell VNX2 or Unity source system and the PowerStore cluster.

It is recommended that the same NTP server is used on the source system, which hosts the source storage resource, and the destination PowerStore cluster. This configuration should provide the proper time synchronization between the source system and the destination PowerStore cluster.

Determine the schedule of the import:

- Immediately or set a time and date

NOTE: When you configure an import and select a date and time for the import session to begin, do not schedule the import to begin within 15 minutes of the current time.

- Whether to automatically cutover to the destination after import

For importing FLR enabled file systems, determine the administrative username and password credentials to access the source DHSM.

Determine which file import interface to use for the import.

NOTE: If the file import interface does not exist, you can create it while creating the import session.

Determine which protection policy to assign to the VDM or NAS server to be imported.

If Distributed Hierarchical Storage Management (DHSM)/(Cloud Tiering Appliance (CTA) is configured on the source Unity system, the CTA which is configured with Unity should be accessible from PowerStore where the NAS server is being imported. In this case, the username and password of the CTA administrator must be entered when configuring a file-based import.

NOTE: For DHMS stub-aware imports from Unity to PowerStore, the default behavior of stub-aware imports should be used. The DHSM stub files are copied as is to PowerStore and are not imported as full files. Ensure that the value of `stubMigrationOrchestrationMode` is set to **0** using the `svc_nas_global_tools` serviceability script:

```
svc_nas_global_tools --args= "-param -facility import -modify  
stubMigrationOrchestrationMode -value 0
```

If the DHSM stub files must be imported as full files, which is not recommended, the value of `stubMigrationOrchestrationMode` should be set to **3**. For more information about the `svc_nas_global_tools` serviceability script, see the PowerStore Service Scripts Guide.

About this task

To configure a file-based import, do the following:

Steps

1. Log in to PowerStore Manager.
2. Under **Migration**, select **Import External Storage**.
The **Import External Storage** page appears.
3. If the intended source system does not appear in the list of remote systems, select **Add Remote System** and specify the relevant information for the remote system (also known as the import connection). Otherwise, go to the next step.
4. To configure a file-based import session, select a source system from the list of remote systems on your network that you have previously entered manually in to PowerStore Manager.
5. Select **Import NAS Server**.
The **Import NAS Servers from Source Array** wizard appears.
6. Step through the wizard and specify the relevant information.

NOTE: Only source VDMs or NAS servers that have a status of **Ready** can be imported.

Once you have specified the necessary information, the system generates a summary of the import session information.

7. Verify that the import session information in the summary is accurate and complete.
8. Click **Ok**.

NOTE: If an import session is scheduled to start later, the **Import State** is shown as **Scheduled**. However, if two active import sessions (which is the maximum for active import sessions) are running, any new import sessions that are set to start are shown with an **Import State** of **Queued**. A maximum of ten import sessions can be scheduled or queued. However, only a maximum of eight import sessions can be scheduled or queued while two import sessions are active. Sometimes ongoing operations on the source system can cause some queued import sessions that become active to fail. In these cases, wait a few minutes and try the import again.

NOTE: When importing several VDMs or NAS servers simultaneously, if anyone of those VDMs or NAS servers is not configured correctly and causes an IP address conflict, the import session for that VDM or NAS server will fail and may cause another of those VDM or NAS server import sessions to fail. You must resolve the VDM or NAS server IP address conflict to complete the import.

The VDM or NAS server should progress to the `Ready For Cutover` state.

- To view the progress of ongoing file import sessions, under **Migration** select **Import External Storage** and then select **File Imports**.

NOTE: If the file system on the destination system is low on space (reaches 95% of capacity) during import, import of the source file system will fail. In this case, you can either ensure that enough space is available and run **Resume** or **Cancel** the import session.

Manage file-based import sessions

About this task

A file-based import session runs as a background job and establishes an end-to-end path for an import operation between a source and destination. The data follows the path as it moves from source to destination.

Steps

- Under **Migration**, select **Import External Storage**.

The **Import External Storage** page appears and lists information about the existing remote systems and their import capability.

- Select the **File Imports** tab.

Information about the existing file import sessions is listed.

- Perform one of the following file import actions:

NOTE: The import actions that can be performed on a file import session depend on the current state of the import session.

Action	Description
Cancel	Select a file import session and under Import Actions, select Cancel. Cancel is allowed at any state of the file import session except <code>Completed</code>, <code>Failed</code>, <code>Cancelling</code> and <code>Cancelled</code>. NOTE: The source system is cleaned up, the destination NAS server and all imported objects including file systems are deleted. When cancel is complete, the state of the file import session is changed to <code>Cancelled</code>, which is a terminal state. Cancel can be forced if the source system is unresponsive.
Cutover	NOTE: If the source NAS server has Common Anti-Virus Agent (CAVA) enabled, disable CAVA before proceeding to cutover. This action helps to avoid potential data unavailability to NAS clients until the session is committed. Select a file import session and under Import Actions, select Cutover to cut over a file import session. You can cut over an import session that is in the <code>Ready For Cutover</code> state. NOTE: When the NAS server is cut over successfully, the state of the file import session is set to <code>Ready To Commit</code>. Cutover may cause a temporary data unavailability to the NAS clients. During cutover, the production file interfaces are disabled on the source system and are enabled on the destination system. For an SMB import, the switch-over is disruptive for the clients and the Active Directory configuration is imported if needed. For an NFS import, the switch over is transparent as file handles are preserved, NLM locks are reclaimed on the destination.
Commit	Select a file import session and under Import Actions, select Commit to commit the file import session. You can commit a file import session that is in the <code>Ready For Commit</code> state.
Pause	Select a file import session and under Import Actions, select Pause. Use Pause to pause an import session that is in the <code>Copy In Progress</code> state during Initial Copy or Incremental Copy operations.

Action	Description
	i NOTE: Background data transfer stops, but I/O to the source continues in the file import session during Incremental_Copy. A paused import session can be resumed or cancelled. When a user tries to pause an import session that has an incremental copy which is about to complete, the session can be automatically transitioned from the Paused state to the Ready For Commit state without the user having to resume the import session. The Ready For Commit state is equivalent to the Paused state in terms of the load on the source system.
Resume	Select a file import session and under Import Actions, select Resume. Use Resume to start an import session that is in the Paused state. i NOTE: The log message text stating that It is also possible to use Resume action requesting to repeat the configuration import. can be ignored. PowerStore does not support this action.
Delete	Select a file import session and under Import Actions, select Delete. Use Delete to delete a file import session that is in the Completed or Cancelled state. i NOTE: Delete removes the historical record of the import. To stop active file import sessions, use Cancel before deleting.

i **NOTE:** If import of a source VDM or NAS server is in progress and a disaster occurs making the source system unusable or unreachable, contact your service provider to recover the source system involved in the import.

Import-CLI (Linux)

IMPORT-CLI is a utility that is provided for the Linux host administrator to check import-specific details such as volume information, logging information, the installed version of the host plugin, systems supported in the current host plugin version, and such.

This appendix contains the following information:

Topics:

- [Get help](#)
- [Status](#)
- [Host plugin version](#)
- [List supported arrays](#)
- [Server port](#)
- [Log information](#)
- [Microhttpd status](#)
- [Restart the web server](#)
- [Recover device](#)

Get help

Get command-specific help.

Format

```
importcli help
```

Example

```
# importcli help
Usage: importcli <command> [options]

Available commands:
help Get command-specific help with '<command> help'

status Dump current multipathing status, if selected --importable, it displays info for
only importable volumes

ha_version Displays the current version of Host plugin installed

list_supported_arrays Displays a list of supported arrays in the current Host plugin
version

server_port Displays the server port that is used for communication and provides the
option to change it to a different port

log_show Displays Log level and location for logs

mhd_status Displays microhttpd status

restart_webServer Restarts webserver in case of microhttpd failure.
```

Status

Dumps the current multipathing status. If selected --importable, information for only importable volumes appears.

Format

```
importcli status <options>
```

Options

Table 4. Command options

Option	Description
-v --verbose	Show extra information.
--importable Display	Show information only for importable volumes.

Example

```
# importcli status
Generating diagnostic data, please wait...
=====
Volume list
=====

Target WWID: 6006016011404000a331505c1bd8223b
Array Type: UNITY
Dev mapper name: 36006016011404000a331505c1bd8223b
DM dev name: /dev/dm-12
SD devices list:
/dev/sdab
/dev/sdad
/dev/sdae
/dev/sdaf
Volume Size: 1.00 GB
Import Status: READY FOR IMPORT
```

Host plugin version

Shows the current version of the host plugin installed.

Format

```
importcli ha_version
```

Example

```
# importcli ha_version
Generating diagnostic data, please wait...

HA version: 1.0

Build version: 56e9023_558
```

List supported arrays

Shows a list of supported arrays in the current host plugin version.

Format

```
importcli list_supported_arrays
```

Example

```
# importcli list_supported_arrays
Generating diagnostic data, please wait...

=====
Array Name VID
=====
EQL EQLOGIC
Compellent COMPELNT
VNX2 DGC
UNITY DGC
PowerStore DellEMC
```

Server port

Shows the server port that is used for communication and provides the option to change it to a different port.

 **NOTE:** The server port should not be changed while import is in progress on the host. When the server port has been changed, delete the associated host on the **Hosts & Host Groups** page under **Compute** in PowerStore Manager, and then add the host again.

Format

```
importcli server_port {change [port_num]}
```

Options

Table 5. Command option

Option	Description
change <port_num>	Changes the server port to <port_num>. Valid values are: • 8443 • 50443 • 55443 • 60443

Examples

```
# importcli server_port
Generating diagnostic data, please wait...
Server port : 8443
```

```
# importcli server_port change 55443
Generating diagnostic data, please wait...
Changing Server port to : 55443
```

Log information

Shows log level and location for logs.

Format

```
importcli log_show
```

Example

```
# importcli log_show
Generating diagnostic data, please wait...

Log Level: 2
Log Location: /var/log/import
```

Microhttpd status

Shows microhttpd status.

Format

```
importcli mhd_status
```

Example

```
# importcli mhd_status
Generating diagnostic data, please wait...

Microhttpd Status: ACTIVE
```

Restart the web server

Restarts the web server if there is a microhttpd failure.

i NOTE: Use this command only if the Micro-http daemon (MHD) is inactive. The status of the MHD can be verified using the `importcli mhd_status` command. When the `restart_webServer` command runs successfully, MHD becomes active. Also, the web server should not be restarted while import is in progress on the host. Contact your service provider before using this CLI command.

Format

```
importcli restart_webServer
```

Example

```
# importcli restart_webServer
Generating diagnostic data, please wait...
Server port : 8443
```

Recover device

Recovers the specified device which is stuck in a bad state due to an internal error during the import process.

 **NOTE:** Contact your service provider before using this CLI command.

Format

```
importcli recover_device <device_WWID>
```

Example

```
# importcli recover_device 6006016011404000a331505c1bd8223b
Generating diagnostic data, please wait...

Recovered device successfully!
```

Additional tasks related to import for Linux-based hosts

This appendix contains the following information:

Topics:

- [Regenerate the host HTTPS certificate](#)
- [Setting the Oracle ASM logical block size](#)

Regenerate the host HTTPS certificate

About this task

During installation, the host plug-in generates a self-signed HTTPS certificate and uses it for secure communication. In the following instances this certificate must be regenerated:

- Host IP address has been changed.
- Host name has been changed, or it has been added to a new domain.
- Host HTTPS certificate has expired.

To regenerate a host HTTPS certificate for a Linux-based host, do the following:

Steps

After regenerating the certificate, delete the associated host on the **Hosts & Host Groups** page under **Compute** in PowerStore Manager, and then add the host again.

Setting the Oracle ASM logical block size

Prerequisites

 **CAUTION:** Avoid running anything below when Oracle is already installed. This procedure only applies when the Oracle database has not been created.

Determine whether you need to set the Oracle ASM logical block size before starting import. Check the logical and physical sector size on the Compellent SC LUN by running `fdisk -l`. The following is an example of the command output:

```
Disk /dev/mapper/36000d3100116f20000000000000001484: 53.7 GB, 53687091200 bytes,
104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 2097152 bytes / 2097152 bytes
```

The `Sector size` shown in the command output represents the logical and physical values. You do not need to run the following procedure when the physical sector size is 512 bytes. The physical sector size shown in the example is not supported by PowerStore and would need to be changed. Also note that the logical sector size needs to be 512 bytes.

About this task

Import to PowerStore from a Linux host running Oracle on a Compellent SC appliance is allowed only when the Oracle configuration, ASM or AFD, uses the logical sector size for ASM disk groups. Import of external storage to PowerStore does not support 4096 bytes sector size devices. It supports only 512 bytes sector size devices.

If you are planning to Import external storage to PowerStore from a Linux host running Oracle with ASM on Compellent SC storage and you need to set the Oracle ASM logical block size at the time of creating the database, use the following procedure before getting started with import.

Steps

1. Depending on the Oracle configuration, do one of the following when you create the Oracle database:

- NOTE:** PowerStore does not support import an existing database on Compellent SC storage that is created with **ORACLEASM_USE_LOGICAL_BLOCK_SIZE="false"** or **oracleafd_use_logical_block_size** defined with a value of 0.
 - For an ASMLib configuration, set **ORACLEASM_USE_LOGICAL_BLOCK_SIZE="true"**. Use the following standard **oracleasm configure** command to set the parameter to true: **oracleasm configure -b**. This setting allows Oracle ASM to use the logical sector size.
 - For an AFD configuration, create a file in the folder **/sys/module/oracleafd/parameters** by setting **echo 1 > oracleafd_use_logical_block_size** when you create the database. Make the setting permanent by creating a file in the folder **/etc/modprobe.d**, **echo "options oracleafd oracleafd_use_logical_block_size=1" > oracleafd.conf**

2. Before starting import, ensure that the logical sector size is 512 bytes by verifying that the SQL output shows 512 bytes for all the disks in the database.

```
SQL> select disk_number, mount_status, header_status, state, sector_size, path from  
v$asm_disk;
```

ImportKit-CLI (Windows)

The ImportKit-CLI is a utility that is provided for the Windows host administrator. The ImportKit-CLI commands list information about devices under import or devices ready for import. The commands also provide the following functionality:

- Get a list of supported arrays.
- Get a list of volumes or single volume.
- Get the version of different components.
- Enable logging level (No Log - 0, Error - 1, Informational - 2, Verbose - 3).
- Change port or IP address.
- Regeneration of certificate.
- Install the certificate.
- Restart service

 **NOTE:** The `Install-ImportKit-Certificate` command must be run first to install the host plugin certificate to be able to use all the ImportKit CLI commands.

This appendix contains the following information:

Topics:

- [How to run the ImportKit CLI commands](#)
- [List supported arrays](#)
- [Host plugin log information](#)
- [Import kit version](#)
- [Restart import kit host plugin service](#)
- [Import volumes information](#)
- [Get web server port information](#)
- [Install import kit certificate](#)
- [Regenerate the import kit certificate](#)
- [Set web server port information](#)
- [Set host plugin logging debug log level](#)

How to run the ImportKit CLI commands

To run the ImportKit CLI commands, do the following:

1. Open PowerShell.
2. Run the following command: `Import-Module <path where the ImportKIT-CLI.dll is present>`

Examples

For ImportKit:

```
> Import-Module "C:\Program Files\DELLEMC\ImportKIT\ImportKIT-CLI.dll"
```

For EQL HIT Kit with import capability:

```
Import-Module "C:\Program Files\EqualLogic\ImportKIT-CLI.dll"
```

List supported arrays

Shows all the arrays that are supported for import.

Format

Get-ImportKit-ImDsmSupportedArrays

Example

```
> Get-ImportKit-ImDsmSupportedArrays

VendorID      ProductID      ProductName
-----
EQLOGIC       100E-00        EqualLogic
DellEMC       PowerStore     PowerStore
DGC           VRAID          VNX2
DGC           RAID 5         VNX2
```

Host plugin log information

Shows the location and log-level of the host plugin log. Valid log-levels are:

- 0 – No log
- 1 – Error
- 2 – Error and Info
- 3 – Error, Info, and Verbose

Format

Get-ImportKit-LoggingInfo

Example

```
> Get-ImportKit-LoggingInfo

LofileLocation      Loglevel
-----
C:\ProgramData\DELL EMC\log\ClusterNode-2_DC_ha.log 2 , Error & Informational
```

Import kit version

Shows the version of the different components of the Import Kit.

 **NOTE:** The ImportKit certificate must be installed before running this command.

Format

Get-ImportKit-Version

Example

```
> Get-ImportKit-Version
HostAgentService HostAgentLibrary HostAgentCLI DSM_MPIODriver
-----
1.0              1.0              1.0              4.5.0.9859
```

Restart import kit host plugin service

Restarts the Windows host plugin service.

 **NOTE:** Do not run this command when an import session is in progress.

Format

Restart-ImportKit-HAService

Example

```
> Restart-ImportKit-HAService
ResultingString
-----
ImportKITHAService restarted successfully.
```

Import volumes information

Shows details of a list of volumes or the details of a specific volume that is associated with the import kit. Valid values are:

- NOT IN IMPORT
- IN IMPORT
- IMPORT DONE

Format

Get-ImportKit-Volumes <options>

Options

Table 6. Command options

Option	Description
Format-Table	Shows information in table form.
-VolumeName	Shows information for a specific volume.

Examples

```
> Get-ImportKit-Volumes
```

```
VolumeID      : 64ed2a75990a0d1738cd15b3ff0480eb
VolumeName    : ps-volumes-20
Size          : 1085276160 Bytes
SourceArray   : PS
ImportStatus  : NOT IN IMPORT
```

```
VolumeID      : 64ed2a75a96a0d016bc3f52d3ee8491a
VolumeName    : ps-volumes-21
Size          : 1085276160 Bytes
SourceArray   : PS
ImportStatus  : NOT IN IMPORT
```

```
> Get-ImportKit-Volumes -VolumeName ps-volumes-21
```

```
VolumeID      : 64ed2a75990a1d1738cd35b3ff04f07b
VolumeName    : ps-volumes-21
Size          : 1085276160 Bytes
SourceArray   : PS
ImportStatus  : NOT IN IMPORT
```

```
Get-ImportKit-Volumes | Format-Table
```

VolumeID	VolumeName	Size	SourceArray	ImportStatus
64ed2a75990a0d1738cd15b3ff0480eb	ps-volumes-20	15728640 Bytes	PS	NOT IN IMPORT
64ed2a75990a1d1738cd35b3ff04f07b	ps-volumes-20	15728640 Bytes	PS	NOT IN IMPORT
64ed2a75a96a0d036bc3252e3ee8f99a	debperf57	15728640 Bytes	PS	NOT IN IMPORT

Get web server port information

Shows the web server port that is used, network adapter in use, and a list of the available network adapters.

NOTE: The list of available network adapters can be large, Powershell automatically truncates the list in the output. To see the complete list, run the following command in Powershell:

```
$FormatEnumerationList = -1
```

Format

```
Get-ImportKit-WebServerPort <options>
```

Options

Table 7. Command option

Option	Description
Format-List	Shows information in list form.

Examples

```
> Get-ImportKit-WebServerPort | Format-List
```

```
WebServerPortUsed      : 8443
NetworkAdapter         : *.*
Available_AdaptersORInterfaces : {[ETHERNET] 10.0.0.1 [Microsoft Hyper-V Network Adapter], [ETHERNET] 10.11.0.117 [Microsoft Hyper-V Network Adapter #2], [ETHERNET] 10.11.0.118 [Microsoft Hyper-V Network Adapter #3], 10.254.1.113}
```

Install import kit certificate

Installs certificate in the host. Certificate installation in the host is required for the import kit CLI to run.

Format

Install-ImportKit-Certificate

Example

```
> Install-ImportKit-Certificate

ResultString
-----
Certificate installation was done successfully.
```

Regenerate the import kit certificate

During installation, the host plugin generates a self-signed HTTPS certificate and uses it for secure communication. In specific instances, such as host IP address, name, or port changes, or when the certificate expires, the certificate must be regenerated using the `Invoke-ImportKit-CertificateRegeneration` command.

 **NOTE:** Do not run this command when an import session is in progress. This command restarts the ImportKit host plugin service. To do a subsequent import operation, you must delete the associated host on the **Hosts & Host Groups** page under **Compute** in PowerStore Manager, and then add the host again.

Format

Invoke-ImportKit-CertificateRegeneration

Example

```
> Invoke-ImportKit-CertificateRegeneration

ResultString
-----
Certificate Regeneration done successfully.
```

Set web server port information

Changes the IP address or port number, or both.

 **NOTE:** Do not run this command when an import session is in progress. This command restarts the ImportKit host plugin service.

Format

```
Set-ImportKit-WebServerPort <options>
```

Options

Table 8. Command options

Option	Description
-IP <IP address>	The specified IP address must be from the list of available adapters.
-Port <port number>	The specified port can be any permissible numeric number (0–65536).

Examples

```
> Set-ImportKit-WebServerPort -IP 10.0.0.1

Resultstring
-----
IP is changed successfully.
```

```
> Set-ImportKit-WebServerPort -Port 8443

Resultstring
-----
Port is changed successfully.
```

```
> Set-ImportKit-WebServerPort -IP 10.0.0.1 -Port 8443

Resultstring
-----
IP and Port are changed successfully.
```

Set host plugin logging debug log level

Sets the debug level for the host plugin logging.

Format

```
Set-ImportKit-LoggingInfo <options>
```

Options

Table 9. Command option

Option	Description
-debugLevel <log level>	Valid debug log levels are: • 0 - No log • 1 - Error • 2 - Error and Info • 3 - Error, Info, and Verbose

Example

```
> Set-ImportKit-LoggingInfo -debugLevel 1  
  
ResultString  
-----  
Registry Key is updated successfully to value = 1
```

Import-CLI (VMware)

The Import-CLI is a set of commands available to list information about devices being imported. It enables Info-level logging to host plugin and Storage Array Type Plugin (SATP) components.

This appendix contains the following information:

Topics:

- [List log levels](#)
- [List volumes](#)
- [Revert SATP, VAAI, and PSP to default settings](#)
- [equalRule options](#)

List log levels

Import-CLI command for EQL HIT Kit package. Shows the log level that is set for host plugin and SATP components.

Format

```
esxcli import loglevel list
```

Example

```
# esxcli import loglevel list
SATP Log Level: Error,Warning,Info
Info Log Level: 0
HA Log Level: Warning
```

List volumes

Import-CLI command for EQL HIT Kit package. Shows the volumes claimed by SATP for import.

Format

```
esxcli import {volume list [-d <NAAID_of_source>]}
```

Options

Table 10. Command option

Options	Descriptions
-d <NAAID_of_source>	Specifies the NAA ID of the source volume.

Example

```
# esxcli import volume list
```

The following information appears for each volume in the list:

- SourceVolumeNAAID – Unique identifier for the source volume considered for import. For example,

```
naa.68fc61066c31fd6e37c28532f36f1de8
```

- SourceVendor – Vendor identification (VID) of the source array. For example,

```
EQLOGIC
```

- Size – Appears in GB. For example,

```
11.00G
```

- ImportStatus – The state of the volume, which can be one of the following:

- Not Applicable (device has not been selected for import)
- Import In Progress
- Cancel Completed
- Import Completed

- InternalNAAID – The PowerStore volume NAA ID under import or for volumes whose import is complete.

Revert SATP, VAAI, and PSP to default settings

NOTE: Import-CLI command for EQL HIT Kit package. This command is applicable to the Dell EqualLogic Peer Storage (PS) series and should only be run before the volume is selected for Import.

Reverts the SATP, VAAI, and PSP of Dell EqualLogic PS volumes claimed by DellEMC SATP (DellEMC_IMPORT_SATP, T10 Identification VAAI, and VMW_PSP_RR) to VMW_SATP_EQL, VMW_VAAIP_EQL, and DELL_PSP_EQL_ROUTED, respectively.

Format

```
esxcli import {changeToDefault [-d <NAAID_of_source>]}
```

Options

Table 11. Command option

Options	Descriptions
-d <NAAID_of_source>	Specifies the NAA ID of the source volume.

Example

```
# esxcli import changeToDefault -d naa.64ed2a75493a4a1b5abb45508ae779c6
```

```
SATP,VAAI and PSP VAAI set to VMW_SATP_EQL,VMW_VAAIP_EQL,DELL_PSP_EQL_ROUTED respectively  
Reboot the host to apply the set claimrules
```

equalRule options

The Import-CLI command equalRule options for the EqualLogic SATP rules allow you to do the following:

- Add SATP rules to the host.

- List SATP rules.
- Remove SATP rules from the host.

Format

```
esxcli import equalRule add
esxcli import equalRule list
esxcli import equalRule remove
```

Example

```
# esxcli import equalRule list
DellEMC_IMPORT_SATP EQLOGIC 100E-00 user VMW_PSP_RR All EQL ArraysDellEMC_IMPORT_SATP
DellEMC PowerStore user VMW_PSP_RR iops=1 All PowerStore Arrays
```

CLI for EQL MPIO

Ehcmcli is an existing utility that is provided for the host administrator to check EQL MPIO-specific details. These CLI commands show import-specific details such as volume information, logging information, the installed version of the EQL MPIO, and such.

This appendix contains the following information:

Topics:

- [Status](#)
- [Host plugin version](#)
- [Server port information](#)
- [Log information](#)
- [Microhttpd status](#)
- [Restart the web server](#)
- [Recover device](#)

Status

Dumps the current multipathing status. If selected `--importable`, information for only importable volumes appears.

Format

```
ehcmcli status <options>
```

Options

Table 12. Command options

Option	Description
<code>-v --verbose</code>	Show extra information.
<code>--importable</code> Display	Show information only for importable volumes.

Example

```
# ehcmcli status
=====
Volume list
=====

Volume: test
Target name: iqn.2001-05.com.equallogic:4-52aed6-21665a597-cef220441085da70-test
Status: Normal: Logging out
Resolution: If this situation persists, attempt a logout of the target manually
as follows: iscsiadm -m target -u -T iqn.2001-05.com.equallogic:4-52aed6-21665a597-
cef220441085da70-test
Volume Size: 0.40 GB
Import Status: READY FOR IMPORT
Session: 44      /dev/sdr    10.11.179.40    ->    10.11.181.7    04:17:04
Session: 45      /dev/sds    10.11.179.39    ->    10.11.181.7    04:17:03
```

Host plugin version

Shows the current version of the host plugin that is installed.

Format

```
ehcmcli version
```

Example

```
ehcmcli version
Version 1.7.0 Build 469794
```

Server port information

Shows the server port that is used for communication, and provides the option to change it to a different port.

NOTE: The server port should not be changed while import is in progress on the host. When the server port has been changed, delete the associated host under hosts and host groups on the **Compute** page of the PowerStore Manager and then add the host again.

Format

```
ehcmcli server_port {change [port_num]}
```

Options

Table 13. Command option

Option	Description
change <port number>	Changes the server port to <port_num>. Valid values are: 8443 50443 55443 60443

Examples

```
Generating diagnostic data, please wait...
Server port : 8443

ehcmcli server_port change 55443
Generating diagnostic data, please wait...
Server port : 55443
```

Log information

Shows the location and log-level of the host plugin log.

Format

```
ehcmcli log_show
```

Example

```
ehcmcli log_show  
  
Generating diagnostic data, please wait...  
Log Level: 2  
Log Location: /var/log/equallogic
```

Microhttpd status

Shows microhttpd status.

Format

```
ehcmcli mhd_status
```

Example

```
ehcmcli mhd_status  
Generating diagnostic data, please wait...  
  
Microhttpd Status: ACTIVE
```

Restart the web server

If there was a microhttpd failure, this command restarts the web server.

i NOTE: Use this command only if the Micro-http daemon (MHD) is inactive. The status of the MHD can be verified using the `ehcmcli mhd_status` command. When the `restart_webServer` command runs successfully, MHD becomes active. Also, the web server should not be restarted while import is in progress on the host. Contact Dell support before using this CLI command.

Format

```
ehcmcli restart_webServer
```

Example

```
ehcmcli restart_webServer  
Generating diagnostic data, please wait...  
Server port : 8443
```

Recover device

Recovers the specified device which remains in a bad state due to an internal error during the import process.

 **NOTE:** Contact Dell support before using this CLI command.

Format

```
ehcmcli recover_device <device_WWID>
```

Example

```
ehcmcli recover_device 6006016011404000a331505c1bd8223b
Generating diagnostic data, please wait...

Recovered device successfully!
```

Fault handling by PowerStore import

This appendix contains the following information:

Topics:

- [Import processing and fault handling overview](#)
- [Import network overview](#)
- [Import alerts and error codes](#)
- [Failures during non-disruptive import](#)
- [Failures during agentless import](#)
- [Consistency group handling](#)
- [Configuration changes during import](#)
- [Application integration software](#)

Import processing and fault handling overview

Import copies the source volume content to PowerStore volumes in the back end while continuing with host I/Os. For non-disruptive import, it does this without any interruptions. For agentless import, a one-time host application downtime is required before the migration. Given the sensitive nature of this operation, a few run-time checks are made before starting the import process. These checks help avoid failures in the import process. If any of these prechecks fail, import fails to start without host I/O impact. You are advised to rectify the issues and retry the import. Sometimes a simple retry may also lead to a successful import but this depends on the nature of the failure encountered.

Non-disruptive import fault handling overview

It is still possible that the import runs into a failure during run-time, after the import process starts. If any such failure occurs during import processing, an internal cancel of import occurs and the I/Os are redirected back to the source. This action is taken to ensure that host I/Os go on uninterrupted. After resolving the failure reason or reasons, you can retry the import.

You are also given an option to cancel the import and go back to the source. This option is also designed to work without any impact to ongoing host I/O. However, here also, it is expected that all the network connections are live for cancel to succeed. For example, if a host loses the SAN path to source volumes midway during import, an ongoing import operation is not impacted. There is no impact because the I/Os are going to the destination (PowerStore) volume. The paths from the host to source volume are not used. However, if you attempt a cancel operation in this situation of the host not having live SAN paths to the source volumes, it fails.

Depending on the load, the timing of path failure, and configuration, cancel operations can take a long time before timing out. Cancel operations can also cause stop responding like situations that impact host I/O. You are expected to ensure that these connections are up before attempting the cancel. If the connections fail unexpectedly, manual intervention is required to ensure the paths from host to source volumes are working. Based on the duration and nature of these network failures, either retry canceling import or a cleanup operation may be required to fully recover.

Agentless import fault handling overview

If the import runs into a failure during run-time after the import process starts, the import state changes to Cancel Required. Shut down the host application and reconfigure it to access the source volume and cancel the import. After resolving the failure reason or reasons, you can retry the import.

Import network overview

Import from source volume to PowerStore depends on several components. One of the most important components is network connections. These connections are:

1. SAN path1: The front-end from the host to the PowerStore cluster. The PowerStore cluster is the destination and good and steady network connectivity from the host to the destination is mandatory. Both Fibre Channel (FC) and iSCSI are options for this segment and must be the same as what the host has towards the source system.
2. SAN path2: The back-end from the PowerStore cluster to the source system. This connection is used for data transfer between the source volume and the PowerStore cluster. Here again, good and steady network connectivity is mandatory. Both Fibre Channel (FC) and iSCSI are options for this segment and must be the same as what the host has towards the source system and PowerStore cluster.
3. SAN path3: The front-end connection from the host to the source system. For this segment, both FC and iSCSI are options and the protocol must be the same as what the host has towards the PowerStore cluster. This connection can be removed from the source system once all the volumes for this host have been imported.
4. Control path1 (IP): PowerStore must have a management path connection to the source system for the management commands.
5. (For non-disruptive import only) Control path2 (IP): The PowerStore cluster must have a management path connection to the host or hosts involved. The PowerStore cluster import orchestrator uses this connection to communicate with the host or hosts.

All these network connections must be established before starting the import and they must be working well for the import and cancel to be successful. Also, it is highly recommended that the connection from the PowerStore cluster to the source array be a high-speed network with redundant connections. Also, both systems should be within a short distance of each other to minimize network latency issues.

Import alerts and error codes

When an import operation fails, the error message indicates the nature of the problem to help you resolve the issue. If you attempt to recover from a failure and do not succeed, the error messages include a numeric code for reference. This code is provided to help your service provider quickly resolve the issue. In certain types of failures, along with error messages, the PowerStore cluster generates import alerts.

Two categories of alerts are generated: critical and minor. Critical alerts are generated for situations that require manual intervention and, for non-disruptive import, automatic recovery has failed some reason. For example, the source system went down while a background copy from the PowerStore cluster was occurring. The import fails because the PowerStore cluster is not able to reach the source volume in the SAN path. Also, the subsequent automatic cancel does not fully succeed because the host could not reach the source system and the source volume could not restore back to its normal state. To recover, bring the source system back up, do any required cleanup, and try the import again. Minor alerts are generated when user intervention is not required but some operation has failed. For example, the import failed because the host did not have the appropriate connections to the destination volume. However, automatic recovery occurred and I/Os were redirected back to the source volume without I/O impact. Resolve the error, and retry the operation.

Failures during non-disruptive import

Some failures might be intermittent in nature, for example, due to the load of the system or network. Usually, if the import attempt is not successful, the I/Os are not affected and they continue with the source volumes. A simple retry of import suffices for them. Sometimes, the resolution of network or load issues is required before retrying the import. When an import fails, the error message attempts to indicate in simple words to the end user what went wrong without getting too technical. If repeated attempts fail or, if the message is not helping, or both, contact your service provider.

Single fault

Any single fault in the middle of an import is handled without any impact to host I/Os as described in the following examples:

- If the destination loses the back-end connection with the source system in the SAN path during a non-disruptive import, the import is automatically canceled by the PowerStore import orchestrator. I/Os from the host are redirected back to the source. In most situations, this process occurs without any I/O disruption. However, the import fails and must be retried after you fix the SAN paths from the PowerStore cluster to the source system.

- If one of the source SPs reboots but the surviving SP can service the source volume, both import and I/Os continue without any impact.

Depending on the nature of the fault, the import orchestrator handles them so that there is minimum impact on the host I/Os. In all these cases, error messages, or alerts, or both describe the issue to the user.

Based on system load, it is possible that the errors between the PowerStore cluster and the source network result in I/O errors to a user application, even when an automatic cancel occurs. For such rare cases, user intervention may be required to restart the I/Os to the source volumes. If the problem persists, contact your service provider for resolution.

Source disaster recovery

If the source system has a disaster recovery (DR) incident in which it becomes entirely unreachable during import, the following applies:

- If a different host is used in the DR site for recovery, then the existing source system-specific DR procedure should work. The import-specific states are only for the primary site system volume. These states have no bearing on the system volume of the secondary or DR sites.
- If the same host is used to run the applications when the primary system is impacted in a disaster, then the following applies:
 - When the primary (source) system fails, the import process initiates an automatic cancel operation. Check whether the automatic cancel is successful. Once this operation successfully completes, continue with the source-specific DR recovery procedure.
 - If an automatic cancel was not successful, for example, it failed due to network connectivity issues, then additional steps might be required based on the failure. The recovery steps are specific to the error. Contact your service provider for more information about recovery.
 - EqualLogic PS system has some limitations which affect DR during import. Contact your service provider for resolution.

Double fault

Double faults are defined as two separate fault events happening around the same time, such as the ones in the following examples:

- Paths from the host to the source go down and, around the same time, the connection between the PowerStore and the source system also goes down.
- Both SPs of the source system go down during import.

For such rare case double faults, recovery is not fully automatic and manual intervention is needed. The recovery depends on the specific fault condition. Contact your service provider for resolution.

A single problem may manifest as a double fault where the recovery needs some manual intervention. For example, if the source system or volume goes out-of-service (for example, a source volume goes offline) during import, this problem manifests as a double fault. First, the import fails because PowerStore is not able to reach the source volume in the SAN path. The subsequent automatic cancel does not fully succeed since the host is not able to reach the source volume, it is offline. To recover, repair the source volume state, do any required cleanup, then try the import again.

 **NOTE:** This error, which is due to a source volume going offline, results in data being unavailable temporarily, even when import is not occurring.

PowerStore is a dual-node, multiappliance scale-out cluster. Typically, most failures in data unavailable are not fatal and handled by the inherent PowerStore cluster high availability design. The import orchestrator runs inside the PowerStore appliance, and so the orchestrator is as highly available as PowerStore itself.

However, should there be an extreme case where a PowerStore cluster goes down during import before cutover, an option exists to recover and go back to the source system. Until this recovery, data is temporarily unavailable. The general idea is that you must do some manual intervention at the source system to clear the migration-specific states and then run the host platform-specific steps. Contact your service provider for such a recovery.

If an entire appliance is down, both nodes of the appliance are down. However, in a multiappliance cluster, ongoing imports continue in other running appliances. The imports, for which the destination volume is on that specific appliance which is down, get stalled. It is recommended that the appliance be brought up first before trying to cancel this stalled session.

Exception case

Most times, in cases of a single failure, such as a PowerStore node failure during import with host I/O, both import and I/Os are not impacted. The other node takes over. In rare cases, if import is not able to continue due to such failures, an automatic cancel occurs and I/Os are redirected back to the source volume.

Sometimes, the node recovery time might be long and host I/Os might experience latency issues. In worst cases, the I/O timeout expires, leading to temporary data unavailability. Recovery for such cases occurs once the node that went down recovers fully.

If the node cannot reboot or the recovery of the node is taking too long, an option exists to go back to the source. Select **Force Stop** as part of an **Import Actions Cancel** action for the import. Some manual intervention may be required at the host side that is based on the I/O load and platform. After the host recovery step, I/Os can resume at the source again. Once the PowerStore node has recovered and PowerStore cluster is healthy, you can attempt imports again. If you run into a problem in this procedure, it is recommended that you contact your service provider.

Host reboot during a non-disruptive import

An unplanned host reboot during import is possible. For a non-disruptive import, the import process handles this case. If the import has progressed beyond the cutover step, the import continues. If it has not, the import rolls back, which means the import gets automatically canceled and I/Os continue go to the source. These actions apply to both stand alone and host clusters. I/O failures may occur due to the host reboot, which is more likely in the stand-alone host case since, in the host-cluster case, the surviving node takes over. However, I/O failures may occur even without any ongoing import sessions.

It is possible that in some configurations, for example, iSCSI, the automatic login is not enabled. Also, the host to source SAN paths, as described in [Import network overview](#), are not live after reboot. In such cases, this connection must be set up before cancel can be initiated. However, imports may continue because these SAN paths are not used during import. For example, in a Windows-based host with iSCSI connections, you must enable the **option to add the connection to favorite targets** to ensure that the iSCSI connections are reestablished after any reboot.

Failures during agentless import

Some failures might be intermittent in nature, for example, due to the load of the system or network. Usually, if the import attempt is not successful, the I/Os are not affected and they continue with the source volumes. A simple retry of the import should suffice. Sometimes, the resolution of network or load issues is required before retrying the import. When an import fails, the error message attempts to indicate what went wrong without getting too technical. If repeated attempts to resolve the issue fail, contact your service provider.

If the destination loses back end connection with the source system in the SAN path during an agentless import, the import changes to the `Cancel Required` state. It is possible that the errors between the PowerStore cluster and the source network result in I/O errors to a user application. When import changes to the `Cancel Required` state, an alert is raised to reconfigure the user application to use the source volume. After reconfiguring the user application to use the source volume, cancel the import session manually. Import can be retried after the SAN paths from the PowerStore cluster to the source system issues are resolved.

PowerStore is a dual-node, multi-appliance scale-out cluster. Typically, most failures are not fatal and are handled by the inherent PowerStore high availability design. The import orchestrator runs inside the PowerStore appliance and is as highly available as the PowerStore appliance. However, should there be an extreme case where a PowerStore cluster goes down during import before cutover, reconfigure the user application back to the source system. If the entire appliance is down, both nodes of the appliance are down. However, in a multi-appliance cluster, ongoing imports continue in other running appliances. The imports, for which the destination volume is on that specific appliance which is down, stall. In this case, it is recommended that the appliance be brought up first before trying to cancel the stalled session.

If a PowerStore node failure occurs during import, both import and I/Os are not impacted. The other node takes over. If import is not able to continue, it changes to the `Cancel Required` state. When import changes to this state, an alert is raised to reconfigure the user application to use the source volume. After reconfiguring the user application to use the source volume, cancel the import session manually.

Sometimes, the node recovery time might be long and host I/Os might experience latency issues. In worst cases, the I/O timeout expires, leading to temporary data unavailability. If the node cannot reboot or the recovery of the node is taking too long, reconfigure the user application back to the source array. Recovery for such cases occurs once the node that went down recovers fully. Once the PowerStore node has recovered and PowerStore is healthy, try importing again. If the issue persists, contact your service provider.

Consistency group handling

PowerStore import supports import of Consistency Groups (CGs) from the source systems. At a CG level, either the import succeeds for all the volumes in the CG or, if any volume fails, the import fails for all of them. However, in rare situations, it is possible that the rollback fails for one of the volumes. In those situations, CGs end up in a `clean-up required` state. This cleanup of the CG must be done after resolving any faults, such as network issues, and then import can be attempted again. Depending on the fault, a manual host-side recovery may be required.

In extreme cases, such as a source SP reboot or source shutdown around the commit window, it is possible that some volumes are committed and some are not. For such rare cases, the source CG must be split, and the individual volumes imported. After import, the volumes can be added to a PowerStore volume group.

Configuration changes during import

It is not advisable to make any configuration changes to source volumes and the hosts once PowerStore import is set up. For a simple change, such as a volume size change, refresh of the host from the orchestrator is preferred. However for other changes, such as CHAP settings, it is preferred that you make them before setting up the import. If such changes are inevitable, the following steps should be followed:

1. Remove the hosts from the PowerStore cluster. This removal is not the removal of the import host but the removal of the generic host from the PowerStore cluster. This removal ensures that the host entry is cleaned up in both the PowerStore cluster and in the import orchestrator.
2. Remove the source system from the import orchestrator.
3. Make the necessary configuration changes in the host, or source system, or both.
4. Based on the platform, a reboot of the host may be required.
5. Add the source system to the import orchestrator.
6. Add the host or hosts to the import orchestrator.

 **NOTE:** It may be necessary to clear some stale entries in the host.

After these steps, you can start to import volumes or CGs. It is preferred that no configuration changes are made once the import setup is done. Also, these changes should be avoided until after all imports are complete. It is also possible that, based on the type of change, not all the steps may be required. The above procedure is provided to cover all the cases.

If the PowerStore cluster SAN IPs are changed, removing and re-adding the hosts suffices. Removal and re-adding the source systems is not necessary. In this example, it may be essential to clean up some stale entries on the host so that the new IPs are effective without source system impact. If the changes involve some CHAP settings for the source volume, that would impact everything the host accesses and the PowerStore cluster accesses. In this case, you must remove and then re-add both the hosts and the source system. The procedure varies depending on what is changed. If you are unsure, it is recommended to do the entire procedure. As a best practice, any configuration change should be avoided once import has been set up.

Application integration software

It is possible that the source volumes are managed with application integration software, such as VSM for EqualLogic volumes, in VMware environments. It is recommended that once import is done, PowerStore specific plug-ins, for example, VSI plug-in for PowerStore, are used. Users stop managing the source volumes with source system-specific plug-ins.