Dell PowerStore

Planning Guide

Version 4.x

February 2025
Rev. A12

DELL Technologies

Notes, cautions, and warnings

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

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

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

Contents

Preface

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

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

Where to get help

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

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

1

Introduction

Use this document to better understand the installation process and prepare your site and workstation for a successful PowerStore implementation. This chapter includes the following topics:

Topics:

Introduction to PowerStore

PowerStore achieves new levels of operational simplicity and agility. It uses a container-based microservices architecture, advanced storage technologies, and integrated machine learning to unlock the power of your data. A versatile platform with a performance-centric design, PowerStore delivers multidimensional scale, always on data reduction, and support for next-generation media.

PowerStore brings the simplicity of public cloud to on-premises infrastructure, streamlining operations with an integrated machine learning engine and seamless automation, while offering predictive analytics to monitor, analyze, and troubleshoot the environment. PowerStore is highly adaptable, providing the flexibility to host specialized workloads directly on the appliance and modernize infrastructure without disruption. It also offers investment protection through flexible payment solutions and data-in-place upgrades.

PowerStore T model appliances and PowerStore Q model appliances are storage-centric, and enable you to manage and provision block and file storage to external hosts. During initial configuration, you can choose to configure an appliance for unified (block and file) or block optimized (block-only) storage.

PowerStore Q model appliances are populated with large capacity quad-level cell (QLC) SSDs. The supported QLC SSDs have a lower cost per Gigabyte than the triple-level cell (TLC) SSDs used in PowerStore T model appliances.

Appliances

A PowerStore appliance is a preconfigured infrastructure component that has both storage and compute resources. An appliance consists of:

- Base enclosure – Holds up to 25 drives (minimum of six drives) and includes two nodes for high availability with data protection that is implemented across the nodes.
- Expansion enclosures – Enable you to add more drives and increase the storage capacity for the appliance. You can add up to three expansion enclosures.
  - The PowerStore 500T supports the NVMe expansion enclosure.
  - All other PowerStore models support the NVMe expansion enclosure or the SAS expansion enclosure.

NOTE: Mixing NVMe expansion enclosures and SAS expansion enclosures in the same appliance is not supported.

Go to **Hardware** > **Appliances** to review the overall health of the appliances in the cluster and collect support materials for the appliances for troubleshooting issues.

Click the appliance name to launch the **Appliance details** page where you can review the metrics, alerts, and health information of the appliance and its components. Use the **More Actions** options on the details page to collect support materials for the appliance for resolving minor issues.

PowerStore Clusters

A PowerStore cluster is a group of one to four appliances acting as a single component for resource management, efficiency, and availability purposes. A cluster can contain up to four appliances. In this release, you can only have appliances of the same configuration in one cluster.

The following diagram shows the components of a cluster:

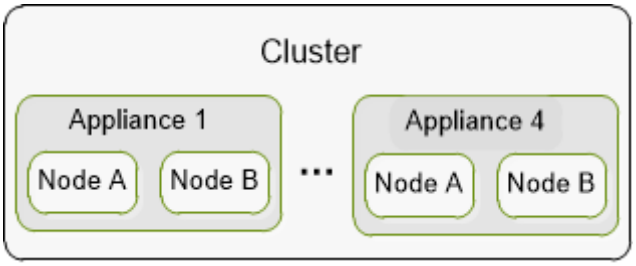

Figure 1. Cluster components

A cluster provides the following benefits:

- Reduced management complexity.
- Enhanced performance and resource efficiency—Compute and storage resources are pooled within a cluster and the resources usage is balanced across the appliances in the cluster. Resources are rebalanced to maintain and optimize the performance and resource usage on the cluster. Rebalancing is done based on the storage space usage trends and system performance evaluations occurring in the backend.
- Scalability—Start with a small configuration and add capacity or performance to the system by adding more appliances later to meet business demand.

To manage and configure a cluster, perform the following operations in PowerStore Manager:

- Monitor and review aggregated metrics for the cluster on the **Dashboard** page.
- Review and configure various settings for your cluster on the **Settings** page.
- Add appliances to or remove them from the cluster **Hardware** page.

Planning and installation overview

This section provides a high-level map of the steps that you should plan on taking from planning through installation, and finally logging on to the PowerStore Manager user interface.

Before the appliance arrives:

1. Work with your infrastructure administrators to:
   a. Configure your network and management switch based on the recommendations that are provided in the *PowerStore Networking Guide for Initial Deployment* .
   b. Obtain network-related information that you require for the initial configuration of your cluster. Use the *PowerStore Networking Guide for Initial Deployment* to plan and collect this information.
   c. Configure the network ports to allow the cluster to communicate with pertinent hosts and applications securely and efficiently. See Port usage for more information.
2. PowerStore requires a data center or server room that is equipped with controlled electrical, environmental, cabling, and safety systems. Plan the site where you will install the appliances and the location of the appliance components (base enclosures and expansion enclosures) in a rack. See Site Planning for more information.
3. Set up a workstation that you will use to discover the appliances and configure the cluster.
4. Determine the drive failure tolerance level that you want to set on each appliance. The drive failure tolerance level indicates the number of concurrent drive failures that the appliance can sustain without causing a data unavailable or data loss event. The single drive fault tolerance level meets availability requirements for all drive types and capacity points, but the double drive failure tolerance can provide higher resiliency and protection. You cannot change the drive fault tolerance level after you have set it. Ensure that the enclosure includes the following number of SSD drives:
   - At least six drives for single drive failure tolerance
   - Seven drives for double drive failure tolerance

Once the appliance arrives:

See the *PowerStore Quick Start Guide* to:

1. Unbox and install your appliance (base enclosure and expansion enclosures).
2. Connect the enclosures to the network, and power on.
3. Start the initial configuration process. For more information, see the *PowerStore Networking Guide for Initial Deployment* .

The *PowerStore Installation and Service Guide* also includes installation instructions for later reference.

NOTE: Either during the initial configuration process or once you log in to PowerStore Manager, it is recommended that you enable the Support Connectivity feature to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. For more information, see Support Connectivity.

Once you complete the initial configuration:

1. Log in to PowerStore Manager using the administrator credentials you set up during the initial configuration.
2. Configure settings for your cluster and start provisioning PowerStore Manager user accounts, storage resources, and policies. See the *PowerStore Setting Up PowerStore Manager Guide* for more information about the recommended steps when you log in to the PowerStore Manager for the first time.

2

Site Planning

This chapter contains the following topics:

Topics:

Rack space guidelines

Consider the following rack space guidelines when planning the location of the appliance components:

- Leave 2U at the bottom of the rack for serviceability and power cable management.
- Stack base enclosure with no expansion enclosures from the bottom, starting at the 3U mark.
- Stack base enclosure in order from least attached expansion enclosures to most, then from most drives to least drives.
- Stack the expansion enclosure attached to the first base enclosure directly above the base enclosure.
- Subsequent base enclosures are stacked in alternating, flipped order.

See Rack Space Planning Worksheets to view a sample rack space plan and then use the blank worksheet to plan for the appliances in your cluster.

Technical specifications

Review the technical specifications to plan and prepare the site where you are installing the PowerStore cluster.

Dimensions and weight for the base enclosure

Table 1. Base enclosure dimensions and weight

Dimension	Value
Weight (fully populated)	41.7 kg (92 lbs)
Vertical size	Two NEMA units
Height	8.64 cm (3.4 in)
Width	44.45 cm (17.5 in)
Depth	79.5 cm (31.3 in)

Dimensions and weight for the PowerStore 500T

Table 2. Base enclosure dimensions and weight

Dimension	Value
Weight (fully populated)	37.4 kg (82.4 lbs)
Vertical size	Two NEMA units
Height	8.64 cm (3.4 in)
Width	44.45 cm (17.5 in)

Table 2. Base enclosure dimensions and weight (continued)

Dimension	Value
Depth	79.5 cm (31.3 in)

NOTE: The weight does not include mounting rails. Allow 3.6 kg (8 lbs) for a rail set.

Dimensions and weight for the SAS expansion enclosure

Table 3. SAS expansion enclosure dimensions and weight

Dimension	Value
Weight (fully populated)	34.98 kg (77.11 lb)
Vertical size	Two NEMA units
Height	8.64 cm (3.4 in)
Width	44.45 cm (17.5 in)
Depth	34.29 cm (13.5 in)

Dimensions and weight for the NVMe expansion enclosure

Table 4. NVMe expansion enclosure dimensions and weight

Dimension	Value
Weight (fully populated)	26.08 kg (57.5 lb) (not including cable management arms or mounting rails)
Vertical size	Two NEMA units
Height	8.89 cm (3.5 in)
Width	43.18 cm (17 in)
Depth	65.30 cm (25.71 in)
Depth with cable management arms	84.86 cm (33.41 in)

Power requirements for the base enclosure

Power requirements vary depending on system configuration, loading, and environmental conditions. The table below describes the maximum expected power draw. To estimate power consumption values for your specific environment, use the Dell Power Calculator.

Table 5. Power requirements for x000 models

Requirement	1000T	3000T	5000T	7000T	9000T
Maximum input power	240 VAC ± 10%, single phase For 100-120V, a customer-supplied step-up transformer is required.				
AC Line Current (operating maximum at 200 VAC)	6.7 A	8.1 A	9.0 A	9.3 A	10.4 A
Power Consumption (operating maximum at 200 VAC)	1385 VA (1316 W)	1629.6 VA (1597 W)	1792.9 VA (1757 W)	1868.4 VA (1831 W)	2088.8 VA (2047 W)
Heat Dissipation (operating maximum)	4.73 x 10^6 J/hr, (4,490 Btu/hr)	5.74 x 10^6 J/hr, (5,449 Btu/hr)	6.32 x 10^6 J/hr, (5,995 Btu/hr)	6.59 x 10^6 J/hr, (6,248 Btu/hr)	7.37 x 10^6 J/hr, (6,985 Btu/hr)
AC Inlet type	IEC320-C14 or IEC320-C20 appliance coupler per power zone			IEC320-C20 appliance coupler per power zone	
Normal input frequency	47 Hz–63 Hz				
Maximum inrush current	45 Apk "cold" per line cord at any line voltage				
AC protection	20 A fuse on each power supply, single line				
Ride-through time	10 ms min				
Current sharing	± 5 percent of full load between power supplies				
Startup Surge Current	120 Apk "hot" per line cord, at any line voltage				

Table 6. Power requirements for x200 models

Requirement	1200T	3200T	3200Q	5200T	9200T
Maximum input power	240 VAC ± 10%, single phase For 100-120V, a customer-supplied step-up transformer is required.				
AC Line Current (operating maximum at 200 VAC)	6.5 A	7.1 A	7.7 A	8.8 A	9.8 A
Power Consumption (operating maximum at 200 VAC)	1297.2 VA (1271.3 W)	1422 VA (1393.6 W)	1535.8 VA (1505.1 W)	1769.8 VA (1734.4 W)	1958.6 VA (1919.4 W)
Heat Dissipation (operating maximum)	4.58 x 10^6 J/hr, (4,338 Btu/hr)	5.02 x 10^6 J/hr, (4,755 Btu/hr)	5.42 x 10^6 J/hr, (5,136 Btu/hr)	6.24 x 10^6 J/hr, (5,918 Btu/hr)	6.91 x 10^6 J/hr, (6,549 Btu/hr)

Table 6. Power requirements for x200 models (continued)

Requirement	1200T	3200T	3200Q	5200T	9200T
AC Inlet type	IEC320-C14 or IEC320-C20 appliance coupler per power zone				IEC320-C20 appliance coupler per power zone
Normal input frequency	47 Hz–63 Hz				
Maximum inrush current	45 Apk "cold" per line cord at any line voltage				
AC protection	20 A fuse on each power supply, single line				
Ride-through time	10 ms min				
Current sharing	± 5 percent of full load between power supplies				
Startup Surge Current	120 Apk "hot" per line cord, at any line voltage				

Table 7. High ambient temperature shutdown

Ambient temperature	Hardware fault	Consequence
Above 45° C (113° F)	None	Noncritical warning generated.
Above 50° C (122° F)	None	Critical alert generated. The system shuts down after five minute timer expires. If the temperature returns to less than 45° C (113° F) , the system powers on.
Any	Three hottest drives have an average temperature of 50° C (122° F)	The system shuts down after five minute timer expires.
Any	Two fans fault	The system shuts down after five minute timer expires.

Power requirements for PowerStore 500T

Power requirements vary depending on system configuration, loading, and environmental conditions. The table below provides worst case data. To estimate power consumption values for your specific environment, use the Dell Power Calculator.

Table 8. Power requirements for AC power

Requirement	PowerStore 500T
Maximum input power	100 to 240 VAC ± 10%, single phase
AC line current (operating maximum)	10 A max at 100 VAC
	5 A max at 200 VAC
Power consumption (operating maximum at 200 VAC)	1004.1 VA (984 W)
Heat dissipation (operating maximum at 200 VAC)	3.54 x 10^6 J/hr (3,358 Btu/hr)
AC inlet type (high line)	IEC320-C14 appliance coupler per power zone (200 VAC)
AC inlet type (low line)	IEC320-C20 appliance coupler per power zone (100 VAC)
Normal input frequency	47 Hz–63 Hz
Maximum inrush current	45 Apk "cold" per line cord at any line voltage
AC protection	20 A fuse on each power supply, single line
Ride-through time	10 ms min
Current sharing	± 5 percent of full load between power supplies
Startup surge current	120 Apk "hot" per line cord, at any line voltage

Table 9. Power requirements for DC power

Requirement	PowerStore 500T
DC line voltage	-39 to -72 DC
DC line current (operating maximum)	28.2 max at -39 VDC
	22.9 max at -48 VDC
	15.3 max at -72 VDC
Power consumption (operating maximum)	1100 W
Heat dissipation (operating maximum at 200 VAC)	3.96 x 10^6 J/hr (3,753 Btu/hr)
DC inlet type	Positronics PLBH3W3M4B0A1/AA
Maximum inrush current	40 A peak
DC protection	50 A fuse in each power supply
Ride-through time	1 ms min at -50 V input
Current sharing	± 5 percent of full load between power supplies

Power requirements for the SAS expansion enclosure

Power requirements vary depending on system configuration, loading, and environmental conditions. The table below describes the maximum expected power draw. To estimate power consumption values for your specific environment, use the Dell Power Calculator.

Table 10. Power requirements

Requirement	Description
AC line voltage	100 to 240 VAC ± 10%, single-phase, 47 to 63 Hz
AC line current (operating maximum)	3.32 A max at 100 VAC
	1.66 A max at 200 VAC
Power consumption (operating maximum)	308 VA (319 W) max at 100 VAC
	332 VA (315 W) max at 200 VAC
Power factor	0.95 minimum at full load, 100V/200V
Heat dissipation (operating maximum)	1.11 x 10^6 J/hr. (1,088 Btu/hr.) max at 100 VAC
	1.20 x 10^6 J/hr, (1,075 Btu/hr) max at 200 VAC
In-rush current	30 A max for 1/2 line cycle per line cord at 240 VAC
Startup surge current	40 Amps peak max per line cord at any line voltage.
AC protection	15 A fuse on each power supply, both Line and Neutral
AC inlet type	IEC320-C14 appliance coupler, per power zone
Ride-through time	12-millisecond minimum
Current sharing	± 5% of full load between power supplies

Power requirements for the NVMe expansion enclosure

Power requirements vary depending on system configuration, loading, and environmental conditions. The table below describes the maximum expected power draw. To estimate power consumption values for your specific environment, use the Dell Power Calculator.

Table 11. Power requirements

Requirement	Description
AC line voltage	100 to 240 VAC +/- 10%, single-phase, 47 to 63 Hz
AC line current (operating maximum)	6.49 A max at 100 VAC
	3.31 A max at 200 VAC
Power consumption (operating maximum at 200 VAC)	663 VA (630 W)
Power factor	0.92 minimum at full load 100V/200V
Heat dissipation (operating maximum at 200 VAC)	2.27 x 10^6 J/hr (2,150 Btu/hr)
In-rush current	82A max for 1/2 Line cycle per line cord at 200 VAC
Startup surge current	100A Max for up to 125uSec
AC protection	15 A fuse on each power supply, both Line and Neutral
AC inlet type	IEC320-C14 appliance coupler, per power zone
Ride-through time	10-millisecond minimum
Current sharing	+/- 5% of full load between power supplies

Operating environment limits

Table 12. Operating environment limits

Limit Type	Limit
Temperature	5°C through 35°C normal, 35°C through 40°C for 10% of the time
Humidity	-12°C DP and 8% to 85% RH (non-condensing)
Temperature Gradient (disk)	20°C/hr
Altitude Compensation	Normal: Lower temp 1°C per 300 M above 950 M
	Improbable: Lower temp 1°C per 175 M above 950 M

Shipping and storage requirements

CAUTION: Systems and components must not experience changes in temperature and humidity that are likely to cause condensation to form on or in that system or component. Do not exceed the shipping and storage temperature gradient of 45°F per hr (25°C per hr).

Table 13. Shipping and storage requirements

Requirement	Description
Ambient temperature	-40° F to 149°F (-40°C to 65°C)
Temperature gradient	45°F per hr (25°C per hr)
Relative humidity	10% to 90% noncondensing
Elevation	-50 ft to 35,000 ft (-16 m to 10,600 m)
Unpowered storage time	Do not exceed six consecutive months of unpowered storage.

Base enclosure airflow

The base enclosure uses an adaptive cooling algorithm that increases or decreases fan speed as the unit senses changes to the external ambient temperature. Exhaust increases with ambient temperature and fan speed, and is roughly linear within recommended operating parameters. Note that the information in the table below is typical, and was measured without cabinet front/rear doors that would potentially reduce front-to-back air flow.

Table 14. Base enclosure airflow

Max Airflow CFM	Min Airflow CFM	Max Power Usage (Watts)
165 CFM	50 CFM	850 W

Environmental recovery

If the system exceeds the maximum ambient temperature by approximately 10°C (18°F), the nodes in the system begin an orderly shutdown that saves cached data, and then shut themselves down. Link control cards (LCCs) in each expansion enclosure in the system power down drives but remain powered on.

If the system detects that the temperature has dropped to an acceptable level, it restores power to the base enclosures and the LCCs restore power to their drives.

Air quality requirements

The products are designed to be consistent with the requirements of the American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE) Environmental Standard Handbook and the most current revision of Thermal Guidelines for Data Processing Environments, Second Edition, ASHRAE 2009b.

Cabinets are best suited for Class 1 datacom environments, which consist of tightly controlled environmental parameters, including temperature, dew point, relative humidity and air quality. These facilities house mission-critical equipment and are typically fault-tolerant, including the air conditioners.

The data center should maintain a cleanliness level as identified in ISO 14664-1, class 8 for particulate dust and pollution control. The air entering the data center should be filtered with a MERV 11 filter or better. The air within the data center should be continuously filtered with a MERV 8 or better filtration system. In addition, efforts should be maintained to prevent conductive particles, such as zinc whiskers, from entering the facility.

The allowable relative humidity level is 20 to 80% non condensing, however, the recommended operating environment range is 40 to 55%. For data centers with gaseous contamination, such as high sulfur content, lower temperatures and humidity are recommended to minimize the risk of hardware corrosion and degradation. In general, the humidity fluctuations within the data center should be minimized. It is also recommended that the data center be positively pressured and have air curtains on entry ways to prevent outside air contaminants and humidity from entering the facility.

For facilities below 40% relative humidity, it is recommended to use grounding straps when contacting the equipment to avoid the risk of Electrostatic discharge (ESD), which can harm electronic equipment.

As part of an ongoing monitoring process for the corrosiveness of the environment, it is recommended to place copper and silver coupons (per ISA 71.04-1985, Section 6.1 Reactivity), in airstreams representative of those in the data center. The monthly reactivity rate of the coupons should be less than 300 Angstroms. When monitored reactivity rate is exceeded, the coupon should be analyzed for material species and a corrective mitigation process put in place.

Storage time (unpowered) recommendation: do not exceed 6 consecutive months of unpowered storage.

Fire suppressant disclaimer

Fire prevention equipment in the computer room should always be installed as an added safety measure. A fire suppression system is the responsibility of the customer. When selecting appropriate fire suppression equipment and agents for the data center, choose carefully. An insurance underwriter, local fire marshal, and local building inspector are all parties that you should consult during the selection of a fire suppression system that provides the correct level of coverage and protection.

Equipment is designed and manufactured to internal and external standards that require certain environments for reliable operation. Compatibility claims and recommendations on fire suppression systems are not provided through Dell. It is not recommended to position storage equipment directly in the path of high-pressure gas discharge streams or loud fire sirens to minimize the forces and vibration adverse to system integrity.

NOTE: The previous information is provided on an as-is basis and provides no representations, warranties, guarantees, or obligations on the part of our company. This information does not modify the scope of any warranty set forth in the terms and conditions of the basic purchasing agreement between the customer and the manufacturer.

Shock and vibration

Products have been tested to withstand the shock and random vibration levels.

The levels apply to all three axes and should be measured with an accelerometer on the equipment enclosures within the cabinet and shall not exceed any of the values in this table.

Table 15. Platform Response Levels

Platform condition	Response measurement level
Nonoperational shock	25 Gs for 3-milliseconds
Operational shock	6 Gs for 11-milliseconds
Nonoperational random vibration	0.40 Grms at 5-500 Hz for 30 minutes
Operational random vibration	0.21 Grms at a frequency range between 5-500 Hz for 10 minutes

Systems that are mounted on an approved package have completed transportation testing to withstand shock and vibrations in the vertical direction only. The levels shall not exceed the values in this table.

Table 16. Packaged System Measurement Levels

Packaged system condition	Response measurement level
Transportation shock	10 Gs for 12-milliseconds
Transportation random vibration	0.28 Grms at a frequency range between 1-100 Hz for 4 hours

3

Licensing and Workstation Requirements

This chapter includes the following topics:

Topics:

PowerStore licensing

PowerStore license is automatically obtained and installed on all the appliances in your cluster during initial configuration. It includes access to all features available with PowerStore.

To obtain licenses automatically during and after initial configuration, ensure that the port 443 is open. The cluster communicates with the Dell Electronic Licensing Management System (ELMS) using port 443 to obtain the license file. If there is an issue obtaining the license file, your cluster will operate in a 30-day trial period. The system attempts to obtain a license automatically every 24 hours. To review the status of your license, in PowerStore Manager, go to **Settings** > **Licensing**. An **Active** status indicates that all the appliances in the cluster have a valid license.

If you do not have an active license yet, you can click **Refresh** on the **PowerStore Licensing** page to try obtaining the license automatically. Or, click **Install License** to manually install the license.

NOTE: You do not need a separate PowerStore license when installing PowerStore operating environment software and firmware upgrades.

Workstation requirements

Once you complete the physical installation process, use a Windows-based workstation or virtual machine to discover the appliances and begin the initial configuration. For workstation and virtual machine requirements, see the *PowerStore Simple Support Matrix*, which can be downloaded from the PowerStore Info Hub.

4

Support Connectivity

This chapter includes the following topics:

Topics:

Operational description of Support Connectivity

The following features are available with a warranty or ProSupport Enterprise Suite coverage:

NOTE: Secure Remote Services and SupportAssist Enterprise capabilities are now part of secure connect gateway.

- Proactive, automated issue detection, case creation and notification
- Accelerated issue resolution with remote support and secure, two-way communication between your service provider and your storage environment
- Analytics-based recommendations for support and services

NOTE: It is strongly recommended that you enable Support Connectivity to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. If you do not enable Support Connectivity, you may need to collect appliance information manually to assist your service provider with troubleshooting and resolving problems with your appliance. Also, Support Connectivity must be enabled on the appliance for data to be sent to APEX AIOps Observability and to enable use of the Cybersecurity application.

Support Connectivity enablement precheck

With PowerStoreOS version 4.0 or later versions, Support Connectivity runs a precheck as part of its enablement process. The precheck proactively confirms whether it is ready to be enabled. This precheck feature identifies common misconfigurations. The precheck determines the following:

- The DNS configuration on the appliance can properly resolve required hostnames.
- For Connect directly, the required network ports are open so that the appliance can contact the backend servers.
- For Connect via Secure Connect Gateway, the required network ports are open for the appliance to contact the backend servers.
- The appliance can copy and store valid certificates from the Dell backend servers or Secure Connect Gateway servers to establish an SSL connection.
- The appliance has sufficient available space and is not running an instance of Support Connectivity.
- The appliance has the required credentials that are installed to enable a successful connection.
- When adding an appliance to a cluster with Support Connectivity enabled, the precheck runs on the new appliance to verify that the new appliance can enable Support Connectivity as well.
- When modifying the existing Support Connectivity configuration, a subset of the defined tests are run to verify that the new configuration will be successful.

If the precheck determines that enabling Support Connectivity will fail, it remains disabled. Also, notifications are provided along with actionable steps to take to remedy issues that are discovered during the precheck.

The Support Connectivity precheck is implemented as a profile within the system health checks. The **System Checks** tab on the **Monitoring** page in PowerStore Manager has an added label and value pair that show the profile of the last system check results based on the respective profile. **Run System Check** only triggers the Service Engagement profile. However, other profiles can be triggered by other operations or actions within PowerStore Manager. For example, when a user enables Support

Connectivity from PowerStore Manager from the **Settings** page or through the Initial Configuration Wizard (ICW), the **System Checks** tab on the **Monitoring** page shows the results of the system check. The profile reflects Support Connectivity.

When **Run System Check** is selected, the values for **Profile** and **Last Run** change and reflect that a system check is running. Once the results are available, both values are updated to reflect the Service Engagement profile, and the last run value. The **Job Details** for PowerStore Manager reflect the output of the invoked system check. If there were failures during the check, they are shown in the output of the **Job Details**.

NOTE: The precheck can also be invoked from the `svc_health_check` service script. Also, the `remote_support` REST API includes a `precheck_override` option that allows users to skip the Support Connectivity precheck.

Support Connectivity and security

Support Connectivity employs multiple security layers throughout each step in the remote connectivity process to ensure that you and your service provider can use the solution with confidence:

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

Support Connectivity management

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

Support Connectivity communication

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

NOTE: Access to a DNS server is required for Support Connectivity to work.

The connection status of Support Connectivity indicates both the state of the connection between PowerStore and the backend Support services of your service provider and the quality of service of the connection. The connection state is determined over five minute periods, and the quality of service of the connection is determined over 24-hour periods. The connection status can appear as one of the following based on any of the appliances in the cluster:

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

The connection status can appear as one of the following based on the average of all the appliances in the cluster when PowerStore is connected to your service provider backend Support services:

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

Support Connectivity remote support

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

Enabling the remote support feature allows support engineers who are authorized by your service provider to securely access and troubleshoot your system. This feature allows your service provider's support personnel to remotely log in to the system to address issues that may occur. Support personnel can remotely log in to your system through SSH or PowerStore Manager. Your support contract determines what and when support personnel are allowed to do. By enabling this feature, you grant access to your system so that troubleshooting and fixing issues can happen as they occur. For example, if a call home, data unavailable or loss, or any otherwise abnormal event occurs, this feature allows your service provider's support personnel to respond faster to correct issues.

Support Connectivity options

The Support Connectivity options that are available by which to send appliance information to your service provider for remote troubleshooting are:

- **Connect via Secure Connect Gateway**—This option is for centralized Support Connectivity where secure connect gateway software runs on a customer-supplied gateway server with two-way file transfer, which includes:
  - Call-homes
  - APEX AIOps Observability and Cybersecurity support
  - Software notifications
  - Operating environment and firmware download from your service provider to the cluster

  It also includes remote access for the support personnel of your service provider. The gateway server is the single point of entry and exit for all IP-based Support activities for the appliances that are associated with the gateway.
- **Connect Directly**—This option is for distributed Support Connectivity where secure connect gateway software runs on individual appliances with the same two-way file transfer as connecting through a gateway server.

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

Support Connectivity using the Secure Connect Gateway option

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

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

To configure your appliance to use the **Connect via Secure Connect Gateway** option for Support Connectivity, you need to provide the IP address for each gateway server. Port number 9443 is the default and cannot be changed. Also, ensure that the port is open between the gateway server and the appliance.

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

Requirements for Support Connectivity using the Secure Connect Gateway

The following requirements are applicable to the **Connect via Secure Connect Gateway** Support Connectivity implementation:

- Network traffic (HTTPS) must be permitted on port 9443 between the appliance and the secure connect gateway server. Allow access to ports 22, 443, and 8443 between PowerStore and the secure connect gateway server for PowerStore Manager and SSH accessing. Also, set a reject rule between the appliance and outbound access for ports 443 and 8443 to ensure that the PowerStore appliance directs traffic to the secure connect gateway server.
- The secure connect gateway server must be version 5.00.06.xy or later.
- Ensure that the PowerStore cluster is running PowerStoreOS version 3.0 or later.

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

Support Connectivity using the Connect Directly option

For the **Connect Directly** option, secure connect gateway software runs directly on each appliance. In a cluster, each appliance establishes its own connection to your service provider. Traffic is not routed through the primary appliance in a cluster. However, Support Connectivity can only be managed at the cluster level, that is, all changes are applied to every appliance in the cluster.

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

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

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

Requirements for Support Connectivity using Connect Directly

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

- Network traffic (HTTPS) must be permitted on ports 443 and 8443 (outbound) to your support provider. Failure to open port 8443 results in significant performance impact (30–45 percent). Failure to open both ports may result in a delay in resolving issues with the end device. Also, if the connection uses a Proxy server, port 3128 is the default used when the port is not specified and **Support Connectivity** is enabled with **Connect Directly** and a firewall is employed between the storage system and the Proxy server. If the default or user-specified port is closed, communication with the storage system through the port will be unavailable.

Configuring Support Connectivity

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

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

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

Configure the initial setup of Support Connectivity

Prerequisites

NOTE: Support Connectivity cannot be enabled on a PowerStore appliance or cluster that has STIG enabled.

To enable Support Connectivity for either the **Connect Directly** or **Connect via Secure Connect Gateway** option, unrestricted access to Dell Support (esrs3-core.emc.com and esrs3-coredr.emc.com) over the Internet using HTTPS (for nonproxy environments) is required.

When configuring Support Connectivity, if your firewall is configured to inspect TLS certificates for verification, the associated Certificate Authority certificate files must be added to the list of trusted authorities in your firewall. The following required certificate files can be downloaded from their respective link:

- Download the DellSecureRemoteServicesRootCA.crt certificate file from Dell.
- Download the ESRS2CA.cer certificate file from Dell.

About this task

NOTE: Do not use this procedure if the feature has been initially configured and the associated End User License Agreement (EULA) has been accepted.

Use PowerStore Manager to configure the initial setup of Support Connectivity by doing the following:

NOTE: With PowerStoreOS version 2.1 and later releases, this feature cannot be enabled unless the **Primary Contact** information with the required values is provided under **Support Contacts**. Also, after a successful non-disruptive upgrade, you must either refresh or close and reopen your browser tab to see and use the new functionality; otherwise, you will still see and use the older functionality.

Steps

1. Click **Settings** and under **Support** select **Support Connectivity**.
   The Support Connectivity page appears with **Support Contacts** selected.
2. Type in the required information.

   NOTE: The **First Name** and **Last Name** of the **Primary Contact** are mandatory, and the **Email** or **Phone** (at least one of these two entries) is required) of the **Primary Contact**. Providing information for the **Secondary Contact** is optional. Your Support Connectivity contact information is critical for a quick response to support issues and must be accurate and current. Also, you can view the **Privacy Policy** and the **Telemetry Notice** by selecting the related link in the **Support Contacts** introductory text.

3. Click **Apply** to save the information.

   NOTE: You must click **Apply** before you can navigate from **Support Contacts** and select **Connection Type**; otherwise, a prompt appears asking whether to cancel the navigation move or to discard the information that you typed in.

4. Select **Connection Type**.

   NOTE: When the initial setup of Support Connectivity has not been configured, the status is shown as Disabled.

5. Click the **Enabled/Disabled** control to begin enabling Support Connectivity.

   NOTE: With PowerStoreOS version 4.0 or later versions, Support Connectivity runs a precheck as part of its enablement process to proactively confirm that it is ready to be enabled. If the precheck determines that enabling Support Connectivity will fail, it remains disabled. Also, notifications are provided along with actionable steps to take to remedy issues that are discovered during the precheck. See Support Connectivity enablement precheck for more information about the Support Connectivity precheck.

   The End User License Agreement (EULA) appears.
6. Click **Accept** to accept the EULA and enable Support Connectivity.
   Support Connectivity can be disabled, however, it is not recommended. Also, if the EULA is not accepted, Support Connectivity cannot be enabled.

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

NOTE: Each gateway server must be up and running before you configure your appliance to use it.

- Port 9443 is the default port and cannot be changed.

- For the **Connect Directly** option:
  - If your network connection uses a proxy server, specify the IP address of the proxy server.

    NOTE: The proxy server must be up and running before you configure your appliance to use it.

  - Use the controls to select the number of the port that will be used to connect to the proxy server in your network.

    NOTE: Port 3128 is the default that is used when the port is not specified and Support Connectivity is enabled with **Connect Directly** and a firewall is employed between the appliance and a Proxy server. If the default or user-specified port is closed, communication with the appliance through the port is not available.

9. Depending on which type of Support Connectivity option you select, do one of the following:
   - For the **Connect Directly** option, go to the next step.
   - For the **Connect via Secure Connect Gateway** option, select **Test Connection** for each configured gateway server to check the status of the connection to the gateway server.

   NOTE: If the connectivity status appears to remain as `Transitioning` and does not change after several minutes (the time it should take to test connectivity), contact your service provider.

10. The **Connect to APEX AIOps Observability** checkbox is selected by default; if you do not want to send files to APEX AIOps Observability and be able to use the Cybersecurity application, clear the checkbox; otherwise, leave the checkbox selected.
11. The **Remote Support** checkbox is selected by default; if you do not want to allow support engineers who are authorized by your service provider to securely troubleshoot your system, clear the checkbox; otherwise, leave the checkbox selected.
12. Select **Send Test Alert** to send a test alert to your service provider to ensure end-to-end connectivity.
13. Select **Apply** to retain the Support Connectivity configuration information.

Manage Support Connectivity settings

Prerequisites

Support Connectivity has been initially configured and the associated End User License Agreement (EULA) has been accepted.

About this task

You can change the **Support Contacts** and **Connection Type** configuration settings, view the status of the feature, test the connection to your service provider, and send a test alert to your service provider.

Steps

1. In PowerStore Manager, select **Settings** and, under **Support**, select **Support Connectivity**.
   The Support Connectivity page appears.
2. To modify the configuration settings of Support Connectivity, do one or more of the following actions as needed:

   NOTE: You must click **Apply** before you can navigate from either **Support Contacts** or **Connection Type** after changes have been made under either tab; otherwise, a prompt appears asking whether to cancel the navigation move or to discard the information that you typed in.

   - Change or delete the information for the **Primary Contact** or **Secondary Contact**, or both.

     NOTE: With PowerStoreOS version 2.1 and later releases, this feature cannot be enabled unless the **Primary Contact** information with the required values is provided. Also, the **Primary Contact** information can only be deleted when the feature is disabled. The **First Name** and **Last Name** of the **Primary Contact** are mandatory, as well as the **Email** or **Phone** (at least one is required) of the **Primary Contact**. Providing information for the **Secondary Contact** is optional. Your Support Connectivity contact information is critical for quick response to support issues and must be accurate and current. Also, you can view the **Privacy Policy** and the **Telemetry Notice** by selecting the related link in the **Support Contacts** introductory text.

- Click the **Enabled/Disabled** control to enable or disable Support Connectivity.

  NOTE: The connection status will not change until after you click **Apply**.

  NOTE: With PowerStoreOS version 4.0 or later versions, Support Connectivity runs a precheck as part of its enablement process to proactively confirm that it is ready to be enabled. If the precheck determines that enabling Support Connectivity will fail, it remains disabled. Also, notifications are provided along with actionable steps to take to remedy issues that are discovered during the precheck. See Support Connectivity enablement precheck for more information about the Support Connectivity precheck.

- Change the **Connection Type** option that you intend to use and provide any related information that is required.
  - For the **Connect via Secure Connect Gateway** option:
    - Specify the IP address of each gateway server, the primary server and, if available, the backup server.

      NOTE: Each gateway server must be up and running before you configure your appliance to use it.

    - Port 9443 is the default port and cannot be changed.
  - For the **Connect Directly** option:
    - If your network connection uses a proxy server, specify the IP address of the proxy server.

      NOTE: The proxy server must be up and running before you configure your appliance to use it.

    - Use the controls to select the number of the port that will be used to connect to the proxy server in your network.

      NOTE: Port 3128 is the default that is used when the port is not specified and Support Connectivity is enabled with **Connect Directly** and a firewall is employed between the storage system and a Proxy server. If the default or user-specified port is closed, communication with the storage system through the port is unavailable.

- For the **Connect via Secure Connect Gateway** option, select **Test Connection** for the configured gateway servers to check the status of the connection to the gateway servers.

  NOTE: If the connectivity status appears to remain as `Transitioning` and does not change after several minutes (the time it should take to test connectivity), contact your service provider.

- Send a test alert to your service provider to ensure end-to-end connectivity.
- Change the **Connect to APEX AIOps Observability** setting.

  NOTE: To send files to APEX AIOps Observability and be able to use the Cybersecurity application, select the checkbox; otherwise, clear the checkbox.

- Change the setting for **Remote Support**.

  NOTE: If you want to allow support engineers who are authorized by your service provider to securely troubleshoot your system, select the checkbox; otherwise, clear the checkbox.

3. Select **Apply** to retain the Support Connectivity configuration information.

APEX AIOps Observability

APEX AIOps Observability is a cloud-based application that allows users to monitor system performance in near real-time across multiple PowerStore clusters and perform basic service actions. APEX AIOps Observability uses logs, system configuration, alerts, power and temperature metrics, performance metrics, capacity metrics, and capacity forecast data that Support Connectivity collects from PowerStore clusters. APEX AIOps Observability provides dashboard views of all connected clusters, showing key information such as performance, capacity trending, and capacity predictions. APEX AIOps Observability also provides proactive serviceability that informs the user about issues before they occur and provides the user with simple, guided remediation.

NOTE: Support Connectivity must be enabled on the cluster to send data to APEX AIOps Observability.

Users can enable APEX AIOps Observability during the configuration of Support Connectivity on a PowerStore cluster. APEX AIOps Observability support is enabled by default when any Support Connectivity option is enabled. When Support Connectivity and APEX AIOps Observability are enabled, APEX AIOps Observability can be launched directly from PowerStore Manager.

NOTE: Once APEX AIOps Observability is enabled, it is possible to disable Support Connectivity without changing the APEX AIOps Observability setting. Without Support Connectivity, data is not collected and sent to APEX AIOps Observability, but if Support Connectivity is re-enabled, the system remembers the APEX AIOps Observability setting and immediately resumes sending data to APEX AIOps Observability. Disabling APEX AIOps Observability support does not disable the transfer of service-related telemetry data and data proactive collections that are provided through Support Connectivity.

System Health

NOTE: This feature is only applicable when Support Connectivity is enabled on the cluster and a bi-directional connection exists between PowerStore and APEX AIOps Observability.

System Health is shown in the **Overview** tab of the **Dashboard** page in PowerStore Manager. The health score provides an insight into how the system is performing. The health score is based on PowerStore alerts that are sent in the telemetry data. **System Health** also includes five attributes that appear as icons for Components, Configuration, Capacity, Performance, and Data Protection, respectively, along with issues and their associated remediation steps.

Cybersecurity

NOTE: Support Connectivity and APEX AIOps Observability must be enabled on the storage system to enable use of the Cybersecurity application.

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

A

Port usage

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

Topics:

Appliance network ports

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

Table 17. Appliance network ports

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
22	SSH client	TCP	User workstation	Cluster IP, or appliance IP, or node IP	Inbound	Used for SSH access (if enabled). If closed, management connections using SSH are not available. ● Remote access (call home)–Both appliance IP and cluster IP are registered; appliance IP is used to access specific appliance (if management connection is up). ● Support or field engineer–Node IP to access specific node.
25 or 587	SMTP	TCP	Node IP	SMTP server IP that is assigned by the user.	Outbound	Used by the appliance to send email. If closed, email notifications cannot be sent.
26	SSH client	TCP	User workstation	Cluster IP, or appliance IP, or node IP	Inbound	SSH access to port 22 is redirected to this port. If closed, management connections using SSH are not available.
53	DNS	TCP or UDP	Node IP	DNS server IP	Outbound	Used for transmitting DNS queries to the DNS server. If closed, DNS name resolution does not work.
80, 8080, 3128	Support Connectivity	TCP	Node IP	Proxy server IP that is assigned by the user.	Outbound	Used for Support Connectivity Proxy connection.
123	NTP	TCP or UDP	Node IP	NTP server IP that is assigned by the user.	Outbound	NTP time synchronization. If closed, time is not synchronized among appliances.
162 or between 1024–49151	SNMP	UDP	Node IP	SNMP server IP that is assigned by the user.	Outbound	SNMP communications. If closed, storage system alert mechanisms which rely on SNMP are not sent. The default port set for SNMP is 162.
443	● HTTPS ● Block replication ● Remote backup	TCP	Node IP	Cluster IP	Bi-directional	Secure HTTP traffic to PowerStore Manager. Also used for block replication management communication between clusters and remote backup management communication between PowerStore and PowerProtect Data Domain. If closed, communication with the appliance is not available.
514	Remote Logging	UDP	Node IP	Remote Syslog server IP	Outbound	Used by the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.

Table 17. Appliance network ports (continued)

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
1468	Remote Logging	TCP	Node IP	Remote Syslog server IP	Outbound	Used by the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.
2049	DD Boost/NFS	TCP	Storage IP set with replication purpose	DD Boost interface IP of PowerProtect Data Domain system	Outbound	The main port used by DD Boost for remote backup.
2051	DD Boost	TCP	Replication source Data Domain IP	Replication endpoint or destination Data Domain	Outbound	Used by the DD Boost protocol if replication is configured.
2052	DD Boost/NFS	TCP	Storage IP set with replication purpose	DD Boost interface IP of PowerProtect Data Domain system	Outbound	Used by the DD Boost protocol for remote backup.
3033	Import	TCP or UDP	Import–Storage IP of the FE port set with replication purpose	Import - Management address of remote system	Outbound	Required for storage import from legacy EqualLogic Peer Storage and Dell Compellent Storage Center systems.
3260	iSCSI	TCP	Replication and Import–Storage IP of the FE port set with replication purpose	• Inbound host access–Storage IP of the FE port set with iSCSI purpose through which the host access • Replication–Storage IP of the FE port set with replication purpose	• Inbound for Host and ESXi host access • Bi-directional for replication • Outbound storage for import	Required to provide the following access to iSCSI services: • External host iSCSI access • External or PowerStore embedded ESXi host iSCSI access • Inter-cluster access for replication • Storage import access from legacy EqualLogic Peer Storage, Dell Compellent Storage Center, Unity, and VNX2 systems If closed, iSCSI services are not available. Used by Data mobility to support reasonable replication performance on low-latency connection.

Table 17. Appliance network ports (continued)

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
				• Import–Storage IP of the FE port set for inbound host access and set in the remote system of import.		
3261	iSCSI/Data mobility	TCP	Replication–Storage IP of the FE port set with replication purpose	Replication–Storage IP of the FE port set with replication purpose	Bi-directional for replication	Used by Data mobility to support reasonable replication performance on high latency connection.
4420	NVMe over TCP I/O Controller	TCP	Host IP	Inbound host access–Storage IP of the FE port set with NVMe/TCP purpose through which the host access	Inbound for Host and ESXi host access	Required to provide the following access to NVMe/TCP I/O Controller services: • External host NVMe/TCP access • External or PowerStore embedded ESXi host NVMe/TCP access If closed, NVMe TCP I/O Controller services are not available.
5353	Multicast DNS (mDNS)	UDP	All storage IPs with NVMe/TCP purpose **NOTE:** Applicable for IPs from storage network configured with NVMe discovery = 'Auto Discovery of CDC'	Destination address is multicast IP address 224.0.0.251	Bi-directional	Multicast DNS query. If closed, mDNS name resolution does not work.

Table 17. Appliance network ports (continued)

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
			or 'Advertise DDC'.			
5555	RSA SecurID Authentication	TCP	Cluster IP	RSA SecurID server IP	Outbound	Used to communicate with an RSA Authentication server when the RSA SecurID Authentication feature is enabled. If closed, authentication using the RSA SecurID Authentication server does not function. The default port set for RSA SecurID Authentication is 5555.
8009	NVMe over TCP Discovery Controller	TCP	Inbound host access– Storage IP of the FE port set with NVMe/TCP purpose through which the host access	Host IP	Inbound for Host and ESXi host access	Used for NVMe of Discovery. If closed, NVMe TCP Discovery services are unavailable.
8443	• VASA • Support Connectivity	TCP	• vCenter IP • ClusterIP or Appliance IP	• Appliance IP • Dell Global Access Servers	• Inbound for VASA • Outbound for Support Connectivity	• Required for the VASA Vendor Provider for VASA 3.0. • Required for the related Support Connectivity Connect Home functions.
8443, 50443, 55443, or 60443	• Windows import host agent • Linux import host agent • VMware import host agent	TCP	Storage IP	• Windows import host agent IP • Linux import host agent IP • VMware import host agent IP	Outbound	One of these ports must be open when importing data storage from legacy storage systems.
9443	Support Connectivity	TCP	Appliance IP	SupportAssist Gateway IP	Outbound	Required for Support Connectivity REST API related to Connect Home.
13333	Data mobility	TCP	Storage IP set with	Storage IP from remote PowerStore with	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: Low

Table 17. Appliance network ports (continued)

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
			replication purpose	replication purpose		
13334	Data mobility	TCP	Storage IP set with replication purpose	Storage IP from remote PowerStore with replication purpose	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: Low_Medium
13335	Data mobility	TCP	Storage IP set with replication purpose	Storage IP from remote PowerStore with replication purpose	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: Medium
13336	Data mobility	TCP	Storage IP set with replication purpose	Storage IP from remote PowerStore with replication purpose	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: Medium_High
13337	Data mobility	TCP	Storage IP set with replication purpose	Storage IP from remote PowerStore with replication purpose	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: High

Appliance network ports related to file

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

NOTE: Outbound ports are ephemeral.

Table 18. Appliance network ports related to file

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
20	FTP (data traffic)	TCP	NAS server production interface	Any IP	Inbound	Port used for FTP data transfers. This port can be opened by enabling FTP. Authentication is performed on port 21 and defined by the FTP protocol.
21	FTP (management traffic)	TCP	Production network IP	NAS server production interface IP	Inbound	Port 21 is the control port on which the FTP service listens for incoming FTP requests.
22	SFTP	TCP	Production network IP	NAS server file interface IP configured by user.	Inbound	Allows alert notifications through SFTP (FTP over SSH). SFTP is a client/server protocol. Users can use SFTP to perform file transfers on an appliance on the local subnet. Also, it provides an outgoing FTP control connection. If closed, FTP is not available.
53	DNS	TCP or UDP	NAS server production interface	DNS server IP	Outbound	Used to transmit DNS queries to the DNS server. If closed, DNS name resolution does not work. Required for SMB v1.
88	Kerberos	TCP or UDP	NAS server production interface	NAS server Kerberos IP	Outbound	Required for Kerberos authentication services.
111	RPC bind (for file services namespaces; otherwise, host service)	TCP or UDP	Production network IP	NAS server file interface IP configured by user.	Bi-directional	Opened by the standard portmapper or rpcbind service and is an ancillary appliance network service. It cannot be stopped. By definition, if a client system has network connectivity to the port, it can query it. No authentication is performed.
123	NTP	UDP	NAS server production interface	NTP server IP	Outbound	NTP time synchronization. If closed, time is not synchronized among appliances.
135	Microsoft RPC	TCP	Production network IP	NAS server production interface	Inbound	Multiple purposes for Microsoft Client.
137	Microsoft Netbios WINS	UDP; TCP or UDP	Production network IP	NAS server file interface IP configured by user.	Inbound; Outbound	The NetBIOS Name Service is associated with the appliance SMB file sharing services and is a core component of that feature (Wins). If disabled, this port disables all SMB-related services.
138	Microsoft Netbios BROWSE	UDP	• Inbound: Production network IP • Outbound: NAS server	Inbound: NAS server file interface IP configured by user.	Inbound	The NetBIOS Datagram Service is associated with the appliance SMB file sharing services and is a core component of that feature. Only the Browse service is used. If disabled, this port disables Browsing capability.

Table 18. Appliance network ports related to file (continued)

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
			production interface			
139	Microsoft SMB	TCP	Inbound: Production network IP	Inbound: NAS server file interface IP configured by user.	Bi-directional	The NetBIOS Session Service is associated with appliance SMB file sharing services and is a core component of that functionality. If SMB services are enabled, this port is open. It is required for SMB v1.
162 or between 1024-49151	SNMP	UDP	NAS server production interface	SNMP server IP	Outbound	SNMP communications. If closed, storage system alert mechanisms which rely on SNMP are not sent. The default port set for SNMP is 162.
389	LDAP	TCP or UDP	NAS server production interface	LDAP server IP	Outbound	Unsecure LDAP queries. If closed, Unsecure LDAP authentication queries are not available. Secure LDAP is configurable as an alternative.
445	Microsoft SMB	TCP	Production network IP	Inbound: NAS server file interface IP configured by user.	Inbound	SMB (on domain controller) and SMB connectivity port for Windows 2000 and later clients. Clients with legitimate access to the appliance SMB services must have network connectivity to the port for continued operation. Disabling this port disables all SMB-related services. If port 139 is also disabled, SMB file sharing is disabled.
464	Kerberos	TCP or UDP	NAS server production interface	Kerberos IP	Outbound	Required for Kerberos authentication services and SMB.
514	Remote Logging	UDP	NAS server production interface	Remote Syslog server IP	Outbound	Allows the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.
636	LDAPS	TCP or UDP	NAS server production interface	LDAP server IP	Outbound	Secure LDAP queries. If closed, secure LDAP authentication is not available.
1234	NFS mountd	TCP or UDP	Production network IP	NAS server file interface IP configured by user.	Bi-directional	Used for the mount service, which is a core component of the NFS service (versions 2, 3, and 4).
1468	Remote Logging	TCP	NAS server production interface	Remote Syslog server IP	Outbound	Allows the appliance to send log messages to remote syslog servers. If closed, log messages cannot be sent to remote syslog servers.

Table 18. Appliance network ports related to file (continued)

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
2000	SSHD	TCP	Service container IP	NAS service interface at node	Inbound	SSHD for serviceability (optional)
2049	NFS I/O	TCP or UDP	Production network IP	NAS server file interface IP configured by user.	Bi-directional	Used to provide NFS services.
3268	LDAP	UDP	NAS server production interface	LDAP server IP	Outbound	Unsecure LDAP queries. If closed, Unsecure LDAP authentication queries are not available.
3269	LDAPS	UDP	NAS server production interface	LDAP server IP	Outbound	Secure LDAP queries. If closed, Secure LDAP authentication queries are not available.
4000	STATD for NFSv3	TCP or UDP	Production network IP	NAS server file interface IP configured by user.	Bi-directional	Used to provide NFS statd services. statd is the NFS file-locking status monitor and works with lockd to provide crash and recovery functions for NFS. If closed, NAS statd services are not available.
4001	NLMD for NFSv3	TCP or UDP	Production network IP	NAS server file interface IP configured by user.	Bi-directional	Used to provide NFS lockd services. lockd is the NFS file-locking daemon. It processes lock requests from NFS clients and works with the statd daemon. If closed, NAS lockd services are not available.
4002	RQUOTAD for NFSv3	TCP or UDP; UDP	Production network IP	NAS server file interface IP configured by user.	Inbound; Outbound	Used to provide NFS rquotad services. The rquotad daemon provides quota information to NFS clients that have mounted a file system. If closed, NAS rquotad services are not available.
4003	XATTRPD (extended file attribute)	TCP or UDP	Production network IP	NAS server file interface IP configured by user.	Inbound	Required for managing file attributes in a multi-protocol environment.
5086	File replication (replication management traffic)	TCP	Node IP	Node IP	Bi-directional	Used by management communication for file services file replication between clusters.
10000	NDMP	TCP	Production network IP	NAS server file interface IP configured by user.	Inbound	• Enables you to control the backup and recovery of a Network Data Management Protocol (NDMP) server through a network backup application, without installing third party software on the server. In an

Table 18. Appliance network ports related to file (continued)

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
						appliance, the NAS Server functions as the NDMP server. ● If NDMP tape backup is not used, the NDMP service can be disabled. ● The NDMP service is authenticated with a username and password pair. The username is configurable. The NDMP documentation describes how to configure the password for various environments.
[10500,10531]	NDMP reserved range for NDMP dynamic ports	TCP	Production network IP	NAS server file interface IP configured by user.	Inbound	For three-way backup/restore sessions, NAS Servers use ports 10500–10531.
12228	Antivirus checker service	TCP	NAS server production interface	Virus checker service IP	Outbound	Required for the Antivirus checker service.
13333	Data mobility	TCP	Storage IP set with replication purpose	Storage IP from remote PowerStore with replication purpose	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: Low
13334	Data mobility	TCP	Storage IP set with replication purpose	Storage IP from remote PowerStore with replication purpose	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: Low_Medium
13335	Data mobility	TCP	Storage IP set with replication purpose	Storage IP from remote PowerStore with replication purpose	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: Medium
13336	Data mobility	TCP	Storage IP set with replication purpose	Storage IP from remote PowerStore with replication purpose	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: Medium_High
13337	Data mobility	TCP	Storage IP set with	Storage IP from remote PowerStore with	Bi-directional	Used by iBasic replication data traffic on block replication network interfaces for latency setting: High

Table 18. Appliance network ports related to file (continued)

Port	Service	Protocol	Source Device IP	Destination Device IP	Access Direction	Description
			replication purpose	replication purpose		

B

Rack Space Planning Worksheets

This appendix includes the following worksheets:

Topics:

Sample worksheet for rack space planning

Table 19. Sample worksheet for rack space planning

40 (1U)	Management Switch (PowerStore T Model Only)	
39 (1U)	**Ethernet Switch 2**	
38 (1U)	**Ethernet Switch 1**	
35 / 36 (2U)		
33 / 34 (2U)		
31 / 32 (2U)		
29 / 30 (2U)		
27 / 28 (2U)		
25 / 26 (2U)		
23 / 24 (2U)	Base Enclosure 5 (BE5) Mgmt IP Address: xxx.xx.xxx	**Appliance 5** (2 expansion enclosures in the stack, alternating order)
21 / 22 (2U)	Expansion Enclosure (BE5-EE1)	
19 / 20 (2U)	Expansion Enclosure (BE5-EE2)	
17 / 18 (2U)	Expansion Enclosure (BE4-EE2)	**Appliance 4** (2 expansion enclosures in the stack, alternating order)
15 / 16 (2U)	Expansion Enclosure (BE4-EE1)	
13 / 14 (2U)	Base Enclosure 4 (BE4) Mgmt IP Address: xxx.xx.xxx	
11 / 12 (2U)	Base Enclosure 3 (BE3) Mgmt IP Address: xxx.xx.xxx	**Appliance 3** (1 expansion enclosure in the stack)
09 / 10 (2U)	Expansion Enclosure (BE3-EE1)	
07 / 08 (2U)	Expansion Enclosure (BE2-EE1)	**Appliance 2** (1 expansion enclosure in the stack)
05 / 06 (2U)	Base Enclosure 2 (BE2) Mgmt IP Address: xxx.xx.xxx	
03 / 04 (2U)	Base Enclosure 1 (BE1) Mgmt IP Address: xxx.xx.xxx	**Appliance 1** (No expansion enclosure in the stack)
01 / 02 (2U)	**Reserved for Serviceability**	

Blank worksheet for rack space planning

Table 20. Blank worksheet for rack space planning

40 (1U)	Management Switch (PowerStore T Model Only)	
39 (1U)	**Ethernet Switch 2**	
38 (1U)	**Ethernet Switch 1**	
35 / 36 (2U)		
33 / 34 (2U)		
31 / 32 (2U)		
29 / 30 (2U)		
27 / 28 (2U)		
25 / 26 (2U)		
23 / 24 (2U)		
21 / 22 (2U)		
19 / 20 (2U)		
17 / 18 (2U)		
15 / 16 (2U)		
13 / 14 (2U)		
11 / 12 (2U)		
09 / 10 (2U)		
07 / 08 (2U)		
05 / 06 (2U)		
03 / 04 (2U)		
01 / 02 (2U)	**Reserved for Serviceability**	