Dell PowerStore Manager Overview

May 2024

H18150.9

White Paper

Abstract

This white paper introduces and describes Dell PowerStore Manager. PowerStore Manager is a web-based solution that provides an easy-to-use interface for management actions and monitoring operations which are crucial to an organization’s needs.

Copyright

Contents

Executive summary....4
Introduction....5
Appliance discovery....7
PowerStore Manager user interface....12
PowerStore CLI....53
PowerStore REST API....53
Conclusion....54
References....55

Executive summary

Overview

This white paper provides an overview of the Dell PowerStore platform user interface, PowerStore Manager, which enables management and monitoring of PowerStore clusters and associated appliances.

For hardware and high-level software details about PowerStore appliances, see the white paper Dell PowerStore: Introduction to the Platform.

Audience

This white paper is intended for IT administrators, storage architects, partners, and Dell Technologies employees. It is also intended for any other individuals that are involved in the evaluation, acquisition, management, operation, or design of a Dell Technologies networked storage environment using PowerStore.

Revisions

Date	Part number/ revision	Description
April 2020	H18150	Initial release: PowerStoreOS 1.0
December 2020	H18150.1	Updated for PowerStoreOS 1.0.3; AD/LDAP section added
April 2021	H18150.2	Updated for PowerStoreOS 2.0
January 2022	H18150.3	Updated for PowerStoreOS 2.1; template update
July 2022	H18150.4	Updated for PowerStoreOS 3.0
October 2022	H18150.5	Updated for PowerStoreOS 3.2
May 2023	H18150.6	Updated for PowerStoreOS 3.5
October 2023	H18150.7	Updated for PowerStoreOS 3.6
November 2023	H18150.8	Updated the section Compute: Hosts & Host Groups, Initiators
May 2024	H18150.9	Updated for PowerStoreOS 4.0 Removed references to PowerStore X

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Authors: Robert Weilhammer, Ryan Meyer, Andrew Sirpis, Louie Sasa

Note: For links to other documentation for this topic, see the PowerStore Info Hub.

Introduction

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. PowerStore is a versatile platform with a performance-centric design that 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. It also offers predictive analytics to easily 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 Manager

For most technology products available today, simplicity and ease of use are some of the top priorities. For PowerStore appliances, PowerStore Manager addresses these priorities by providing an easy-to-use and simplified management interface for IT generalists, while simultaneously providing advanced features for storage administrators. PowerStore Manager allows administrators to easily configure storage resources from their PowerStore appliances to meet the needs of their applications, hosts, and users.

The PowerStore Manager provisioning workflows simplify management by using best practices and recommended default values. These abilities help optimize system performance and minimize the overall costs of using and maintaining the system. Manage provisioned resources easily by using the intuitive filtering options to sort and view data to the user. PowerStore Manager can easily identify failed and faulted components through graphical representations of the system. PowerStore Manager also offers a wide range of Dell Technologies support options, directly from the user interface, to assist troubleshooting.

Terminology

The following table provides definitions for some of the terms that are used in this document.

Table 1. Terminology

Term	Definition
Appliance	Solution containing the base enclosure and any attached expansion enclosures.
Base enclosure	Enclosure containing both nodes (node A and node B) with 25 x NVMe drive slots in the front.
Cluster	One or more appliances in a single grouping and management interface. Clusters are expandable by adding more appliances to the existing cluster, up to the allowed amount for a cluster.
Expansion enclosure	Enclosures that can be attached to a base enclosure to provide additional storage.
NVMe over Fibre Channel (NVMe/FC)	Protocol used to perform Non-Volatile Memory Express (NVMe) commands over a Fibre Channel network.

Term	Definition
NVMe over TCP (NVMe/TCP)	Protocol used to perform Non-Volatile Memory Express (NVMe) commands over an Ethernet network.
Fibre Channel protocol	Protocol used to perform Internet Protocol (IP) and SCSI commands over a Fibre Channel network.
File system	Storage resource that can be accessed through file-sharing protocols such as SMB or NFS.
Internet SCSI (iSCSI)	Provides a mechanism for accessing block-level data storage over network connections.
Network attached storage (NAS) server	File-level storage server used to host file systems. A NAS server is required to create file systems that use SMB or NFS shares.
Network File System (NFS)	Access protocol that allows data access from Linux or UNIX hosts on a network.
Node	Component within an appliance that contains processors and memory. Each appliance consists of two nodes.
PowerStore Q	Container-based storage system that is running on purpose-built hardware. This storage system supports unified (block and file) workloads, or block-optimized workloads. The PowerStore Q model supports Quad-Level Cell (QLC) NVMe SSDs for data storage.
PowerStore T	Container-based storage system that is running on purpose-built hardware. This storage system supports unified (block and file) workloads, or block-optimized workloads. The PowerStore T model supports Triple-Level Cell (TLC) NVMe SSDs for data storage.
Representational State Transfer (REST) API	Set of resources (objects), operations, and attributes that provide interactive, scripted, and programmatic management control of the PowerStore cluster.
Server Message Block (SMB)	Network file-sharing protocol, sometimes referred to as CIFS, used by Microsoft Windows environments. SMB provides access to files and folders from Windows hosts on a network.
Snapshot	Point-in-time view of data stored on a storage resource. A user can recover files from a snapshot or restore a storage resource from a snapshot.
VMware vSphere Virtual Volumes (vVols)	A VMware storage framework which allows VM data to be stored on individual Virtual Volumes. This ability allows for data services to be applied at a VM-level of granularity and according to SPBM. Virtual Volumes can also refer to the individual storage objects that are used to enable this functionality.

Appliance discovery

Introduction

When the PowerStore system base enclosure and optional expansion enclosures are installed and powered on for the first time, configure the system in one of the following ways:

- **Direct connection:** This is the recommended procedure and requires that you are physically present in the data center or lab where the base enclosure is installed.
- **Remote connection:** Use this procedure if you do not have physical access to the base enclosure. This method uses a predefined static IP address to discover and configure the system.

For more information about network configuration, see the *PowerStore Planning Guide* and *PowerStore Installation and Service Guide* at dell.com/powerstoredocs.

Discovery with service port

The preferred method for configuration is to physically connect a workstation to the service port on node B of the PowerStore appliance. A static IP of 128.221.1.249 and subnet mask 255.255.255.0 is set on the workstation. You can log in to PowerStore and begin the Initial Configuration Wizard by directing a browser to 128.221.1.251. PowerStore systems running on versions previous to PowerStoreOS 3.0 require a connection to node A service port and directing the browser to 128.221.1.250.

For instructions and prerequisites for the direct-connect method, see the *PowerStore Quick Start Guide* at dell.com/powerstoredocs.

Discovery with static IP address

If not using the recommended direct-connect method, you can discover PowerStore appliances running PowerStoreOS 1.0.3 and higher using a predefined static IP address. The user must set their workstation to an IP address in the 169.254.0.x/16 range which has access to the same network (untagged/native VLAN) that the PowerStore management ports are plugged into. After an IP on the workstation is set, the user can navigate using a browser to one of the predefined Static IP addresses below to start the Initial Configuration Wizard.

https://169.254.0.10
https://169.254.0.20
https://169.254.0.30
https://169.254.0.40
https://169.254.0.50

For more information about static IP discovery, see the documents PowerStore: Networking Guide and Dell PowerStore: Introduction to the Platform.

Initial Configuration Wizard

When you launch the Initial Configuration Wizard either through the direct-connect or remote-connect options, a browser window tab automatically appears in the default Internet browser asking the user to log in to PowerStore. When you log in for the first time, enter the default credentials of **admin** for the **Username** and **Password123#** for the **Password**. Figure 1 shows an example of the login screen.

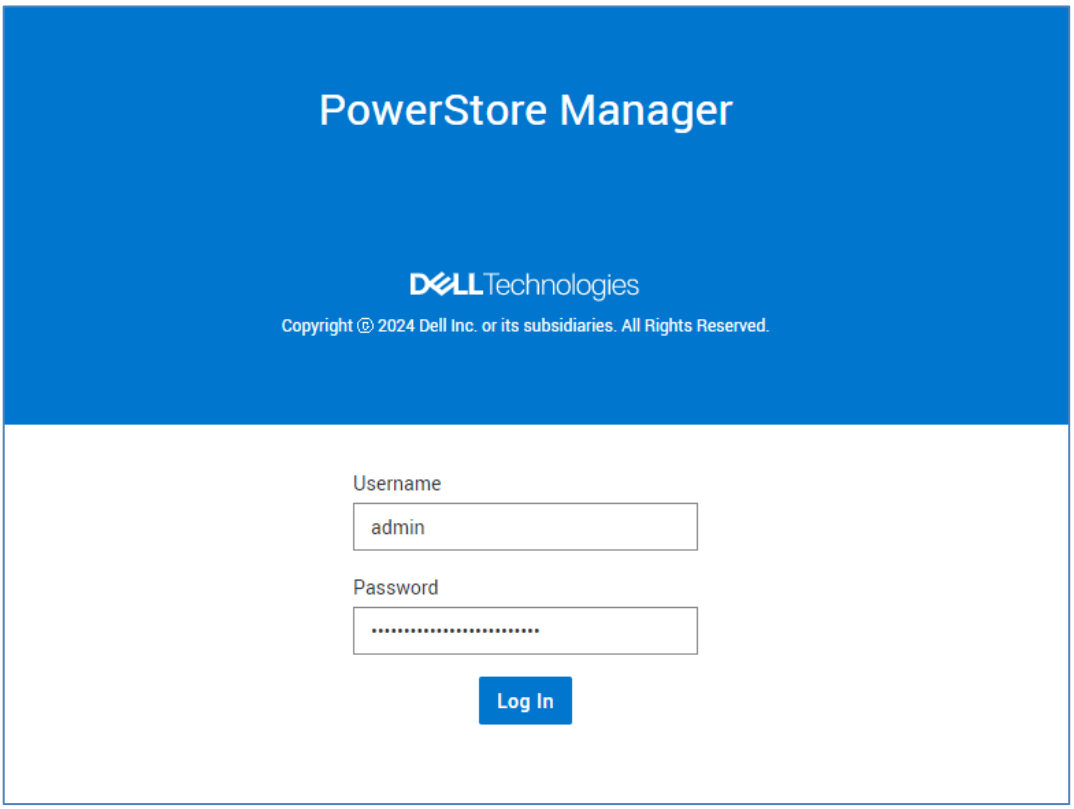

Figure 1. PowerStore Manager login screen

After you log in, the Initial Configuration End User License Agreement (EULA) appears, as shown in Figure 2. You must scroll to review the text, check the box next to **I accept this agreement**, and click **Accept**. The following figure shows an example of the EULA screen.

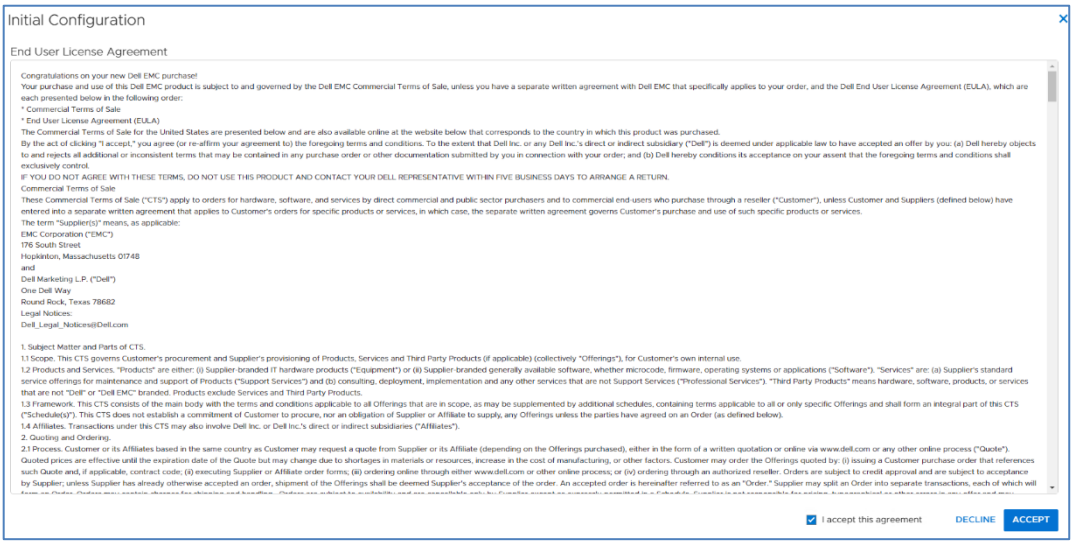

Figure 2. PowerStore Discovery Utility > EULA

After you accept the EULA, the **Infrastructure Telemetry Notice** appears. If you choose to accept the notice, click **Next**.

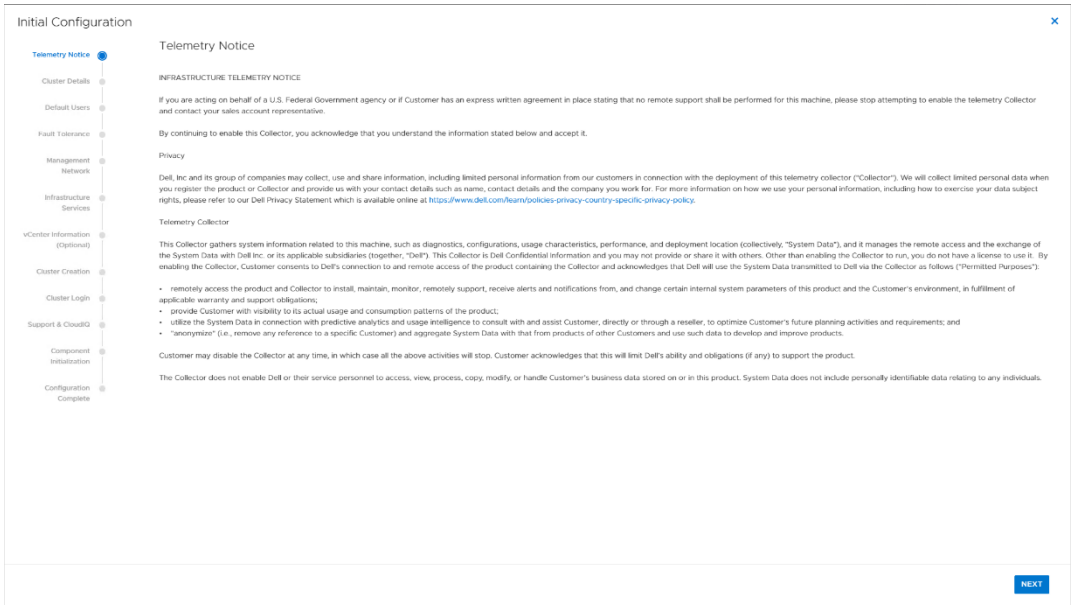

Figure 3. PowerStore Discovery Utility > Infrastructure Telemetry Notice

The Initial Configuration Wizard steps you through the following pages to configure the PowerStore appliances for the first time:

- **Telemetry Notice:** Provides information about the Dell Telemetry collector and privacy policy information.
- **Cluster Details:** Enables you to configure the friendly name of the cluster that appears in the upper-left side of PowerStore Manager and choose the deployment mode, either the default of **Unified** (SAN and NAS) or **Block Optimized** (SAN only). You can optionally add appliances to the cluster if wanted.
- **Default Users:** Enables you to configure the admin and service user passwords. The password requirements are listed below. By default, the service password will match the configured admin password. The user is required to change the default password for security reasons. Click the **Update** button after the passwords are defined, and the UI issues a notification that the passwords have been set. The password requirements are as follows:
  - Must be 8 to 40 characters
  - Must contain at least one upper case letter and one lower case letter
  - Must contain at least one numeric character
  - Must contain at least one special character (! , @ # $ % ^ ~ ? _)
  - Cannot include the single quote ('), ampersand (&), space, or non-English characters
- **Fault Tolerance:** Allows you to select the fault-tolerance level for each appliance. This determines the number of drives that can fail concurrently on an appliance without incurring data loss. You can choose single or double drive failure. For the PowerStore 3200Q model, double drive failure fault tolerance is enforced and cannot be changed.

- **Management Network:** Enables you to enter the IP addresses and network information for the management network. For systems running PowerStoreOS 2.0 and higher, the Storage Network configuration was removed from the Initial Configuration Wizard. PowerStore Manager recommends that you set up a Storage Network upon first login. PowerStore Manager access is only available using the more-secure HTTPS protocol. You can check the optional box to **Enable HTTP redirect to HTTPS for Cluster IP.** This will redirect any HTTP request to the more secure HTTPS protocol.
- **Infrastructure Services:** Allows you to configure DNS and NTP servers, and optionally configure the physical top-of-rack or out-of-band management switch credentials for network validation.
- **vCenter Information (Optional):** Enables you to configure integration with an existing VMware vCenter cluster and the PowerStore as a VASA storage provider.
- **Cluster Creation:** Allows you to review the chosen configuration information, validate the configuration, and initiate the cluster creation. You can also export the configuration details from this page. The validation process is automatically performed as part of the cluster creation process, but you may **Validate** before clicking **Configure**, if wanted. If there are any issues, the wizard notifies you of the errors and provides guidance to resolve them. The Initial Configuration Wizard sets up the services to bring up the PowerStore cluster.
- **Cluster Login:** Once the cluster creation completes, this step allows you to log in again with your newly created password. Then, you return to the Initial Configuration Wizard.
- **Support & APEX AIOps Infrastructure Observability:** Allows you to proceed with the default enablement of **Support Connectivity** and Infrastructure Observability or clear the options if you do not want to enable them. Support Connectivity allows you to stay ahead of disruptions with effortless support and richer insights. Infrastructure Observability requires Support Connectivity to be enabled. Infrastructure Observability is a single pane of glass for proactive monitoring, machine learning, and predictive analytics. You must provide contact information for support (names, email messages, phone numbers). You are also prompted for the connection type (Connect Directly or Connect using Secure Connect Gateway). Remote support is also checked by default, which allows authorized technical support agents to remotely troubleshoot issues over a secure connection.
- **Component Initialization:** Allows you to show the components such as **Create Cluster** and **File Services** that must be completed before the PowerStore cluster is ready. The message **All PowerStore components have initialized successfully** is displayed with a green checkmark when this process is completed.
- **Configuration Complete:** Provides the notification **The PowerStore cluster is fully configured**, and allows you to close the wizard or click **Go to PowerStore Manager**.

For more information about the initial discovery process and Initial Configuration Wizard, see the *PowerStore Quick Start Guide* and *PowerStore: Network Planning Guide* at dell.com/powerstoredocs.

Licensing

Before you can use the software features on PowerStore appliances, you must install a proper license. PowerStore provides two options for licensing: Automatic Licensing and Manual Licensing.

The default option is Automatic Licensing which requires port 443 to be open. If you have the network port 443 open for the system management ports, the system automatically connects to Dell Technologies, acquires the appropriate license that is based on the system service tag, and installs it without any user intervention.

The other option is Manual Licensing. To obtain a license manually, go to the **Settings** menu > **Licensing** page. On the page, the **Install License** button opens a window which provides instructions on how to retrieve and upload a license file as shown in Figure 4.

If a license is not installed, the system uses a 30-day free-trial license while the administrator works to obtain a license. If the 30-day trial period ends before a license is installed, you are not able to perform management operations. For example, you cannot create a volume, take snapshots, upgrade software, or modify NAS servers. However, users still have access to storage data if there is an expired license.

Here are some considerations for licensing:

- The license file is all-inclusive, and all features are enabled automatically.
- To license the whole cluster, only one license file is required.
- If an appliance is reimaged or removed from the cluster, a license must be reapplied for that appliance upon initial configuration.
- The VMware ESXi host license is separate from the PowerStore license.

For more information, see the white paper Dell PowerStore: Virtualization Integration.

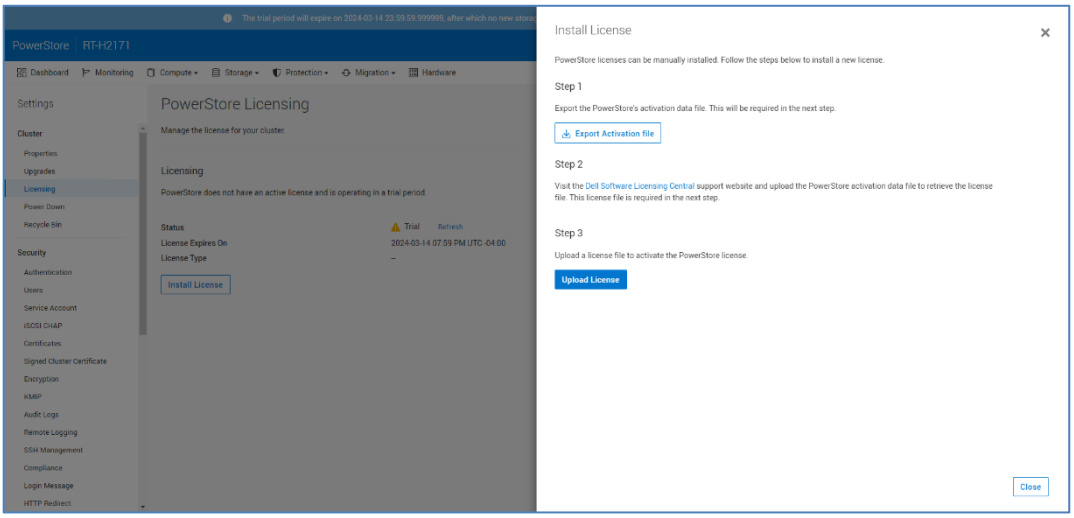

Figure 4. Settings page > PowerStore Licensing

PowerStore Manager user interface

Overview

PowerStore Manager provides an optimal user experience using an HTML5-based web interface that allows you to manage and monitor the cluster and all associated appliances. This modern interface has been designed with simplicity and ease-of-use in mind for all storage-management needs. The top navigation menu includes several categories, most of which include cards that you can select for more information. The menu includes resources and system settings that are used on a frequent basis by administrators. The categories and subcategories in the main menu are described in the following table.

Table 2. Navigation menu options

Category	Subcategories	Description
Dashboard	None	View a comprehensive summary of cluster status, overall capacity, and system performance
Monitoring	None	Consolidated view of system alerts, events, jobs, and system checks
Compute	Host Information, Virtual Machines, vCenter Server Connection	View and configure hosts, virtual machines, and the cluster vCenter Server Connection
Storage	Volumes, Volume Groups, Storage Containers, File Systems, NAS Servers, Quality of Service (QoS), Recycle Bin	View, configure, delete, prioritize, and recover storage resources for the cluster
Protection	Replication, Metro, Metro Witness, Remote Backup, Remote Systems, Protection Policies	View and configure replication, Metro and Metro Witness, remote clusters, Remote backup to PowerProtect DD and protection policies including snapshot, replication, and remote backup rules
Migration	Internal Migrations, Import External Storage	View and configure internal cluster migrations between appliances and imports to PowerStore from supported external systems
Hardware	None	View and monitor hardware related to the cluster including drives and attached expansion enclosures

Dashboard

The dashboard is the first page that is displayed when you log in to PowerStore Manager. The page provides a status view of various system details, including system capacity, system health, storage health, and overall system performance. Different system details and information appear in the **Overview**, **Capacity**, and **Performance** tabs.

- The **Overview** tab includes high-level cluster information, including the number of configured storage and host resources, a user-selected resource watchlist, alerts, and system health metrics imported from Infrastructure Observability (available in PowerStoreOS versions 4.0 and later). This high-level information provides quick insight into the overall usage of the systems in the cluster, and it

highlights important issues that require the immediate attention of the administrator.

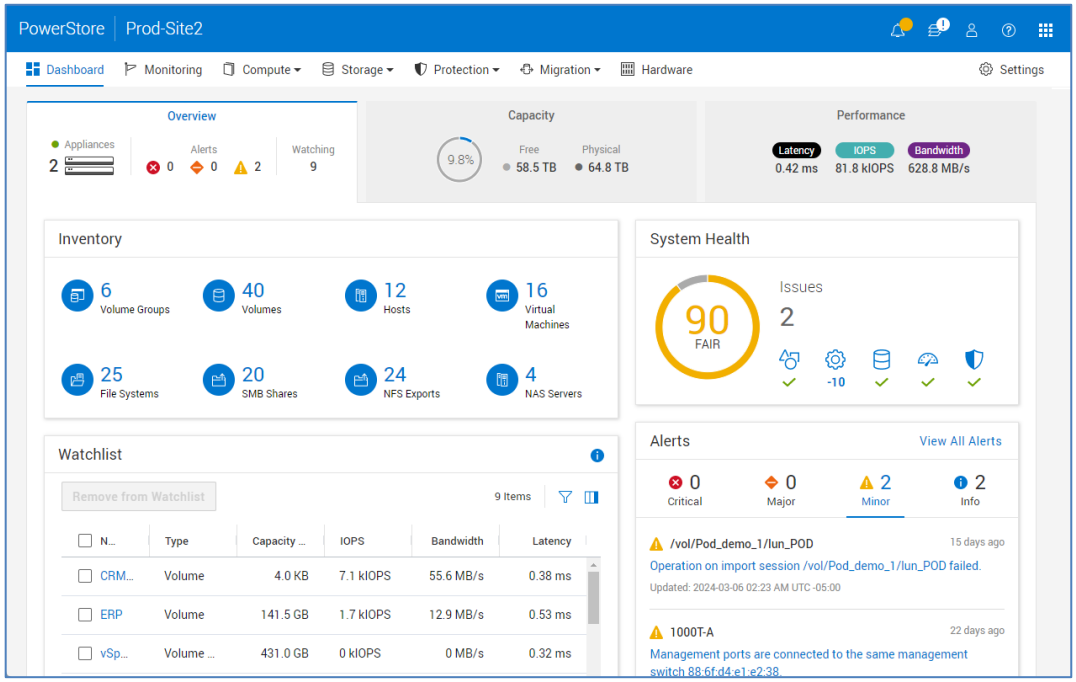

Figure 5. PowerStore Manager dashboard > Overview tab

The **Capacity** tab, as shown in Figure 6, includes information about the overall capacity of the systems in the cluster. The tab also shows a historical graph of usage which helps determine a capacity forecast over time. It might take several days for the capacity forecast to be displayed with a new system. PowerStoreOS versions 4.0 and later display the Overall DRR, Reducible DRR, and Unreducible Data metrics on the system when hovering over the **Data Savings** graphic. The **Capacity** tab also includes information about data savings and top storage consumers that are related to configured storage resources.

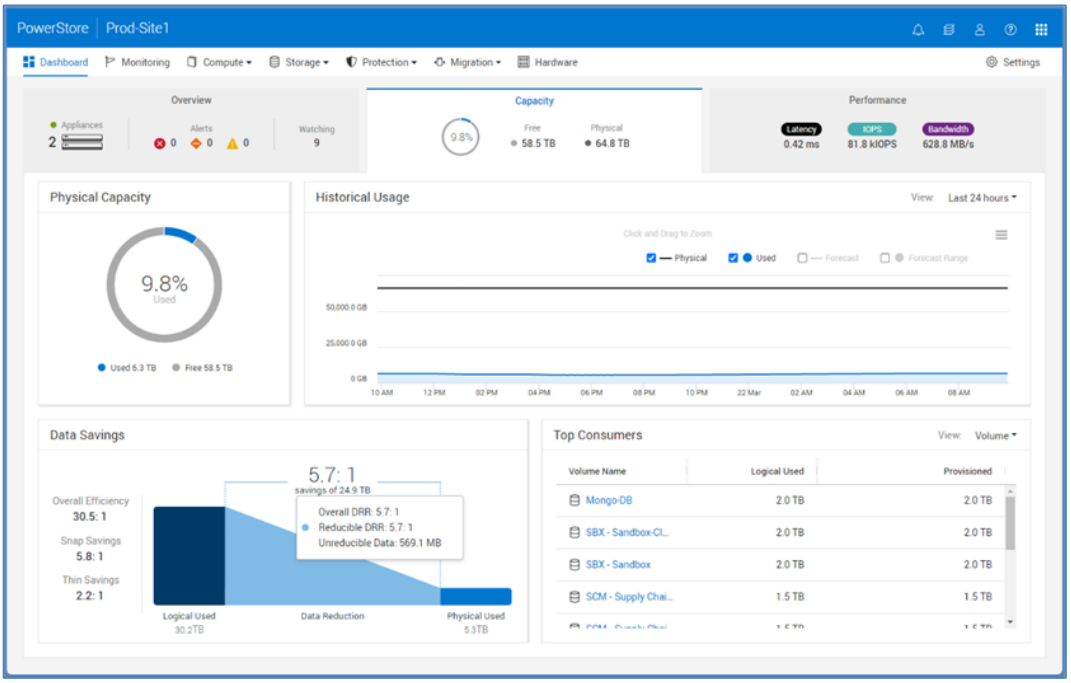

Figure 6. PowerStore Manager dashboard > Capacity tab

The **Performance** tab includes an overall cluster performance chart which shows top-level performance metrics including latency, IOPS, I/O size, and bandwidth. Also included on the performance chart are graphed system alerts at the time they were identified, which is useful when troubleshooting performance anomalies. The performance chart itself can be exported in different formats including .jpeg, .pdf, .png, and .csv formats.

The following table shows the performance-metric retention periods and associated sampling intervals.

Table 3. Sampling intervals and retention periods

Time range setting	Sampling interval
Last 1 Hour	20 Seconds
Last 24 Hours	5 Minutes
Last 1 Month	1 Hour
Last 2 years	24 Hours

Monitoring

The Monitoring page is the consolidated area of all appliance alerts, events, and jobs for the cluster. Events provide information about changes to the system, but do not rise to the level of an alert that indicates a problem with the system. Alerts, as shown in Figure 7, are categorized by severity which indicates the urgency of the alert. On the Jobs tab, you can monitor the status of user and system-created jobs. In PowerStoreOS version 2.0 and later, jobs that have completed with a warning status will be displayed. When the user clicks a job, they can view each individual job step for details about the warning.

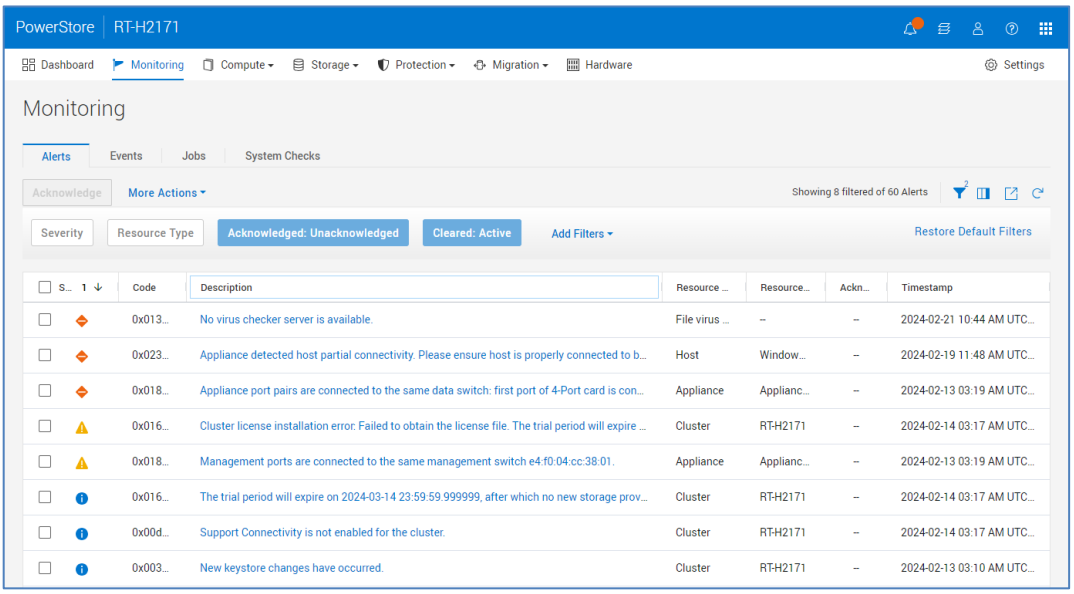

Figure 7. Monitoring page > Alerts tab

The following table shows the supported alert severities and their descriptions.

Table 4. Alert severity levels

Icon	Label	Indicates
	Information	An event has occurred that does not impact system functions. No action is required.
	Minor	An error has occurred that you should be aware of, but it does not have a significant impact on the system. For example, a component is working, but its performance may not be optimal.
	Major	An error has occurred that has a major impact on the system and should be remedied but may not have to be fixed immediately. For example, a component is failing and some or all functions may be degraded or not working.
	Critical	An error has occurred that has a significant impact on the system, and it should be remedied immediately. For example, a component is missing or has failed, and recovery may not be possible.

In the details of each alert, more information is displayed including the System Impact, Repair Details, and Associated Events as shown in Figure 8. This information is useful in troubleshooting scenarios and allows users to remediate issues seen on the system.

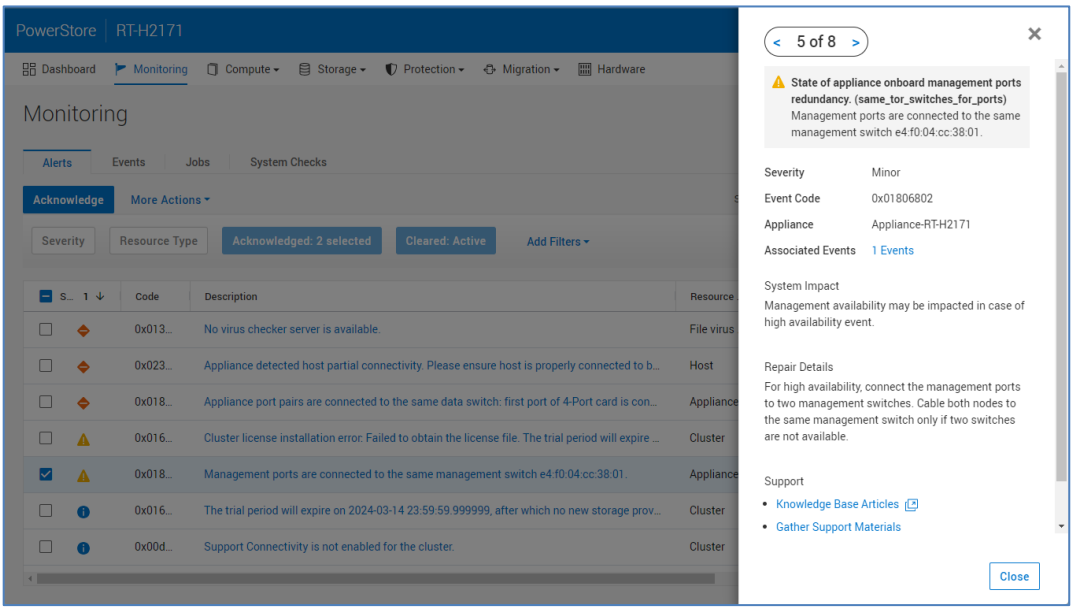

Figure 8. Monitoring page > Alert details

When alerts are no longer relevant or are resolved, the system automatically clears the alerts with no user intervention. This action ensures that cleared alerts are hidden from the default view so that only relevant issues are displayed to administrators. Cleared alerts can be optionally displayed through table filtering options. Alerts can also be acknowledged which removes the alert from default view. Acknowledging an alert does not indicate that the issue is resolved. You can view acknowledged alerts through the table-filtering options. You can also configure PowerStore Manager to send alert notifications to a specified email or SMTP server through the **Settings** menu.

When a user logs in to PowerStore Manager, the system may display a global alert banner across the top of the menu buttons. Global banners inform users of specific events happening on the system by displaying three different banner styles: Informational (blue), Minor/Major (yellow), or Critical (red). Multiple global alerts are supported, and the color and message on the banner will always display the most severe alert. When a user clicks the global banner alert, the alert details will slide out from the right and the user may cycle through all active global alerts. Global alerts may include expiring license warnings, NDU in progress notifications, and critical issues such as a degraded system.

System checks

Introduced in PowerStoreOS 2.0, system checks can be run against your PowerStore cluster from the **Monitoring** > **System Checks** tab, see Figure 9. System checks can be run independently at any time to allow users to proactively check system health outside of the upgrade cycle. System Check jobs run the latest Health Check that has been installed on the system. Once the System Check job is complete, status information is displayed with a pass-to-fail ratio of the various components that were checked as shown in Figure 9.

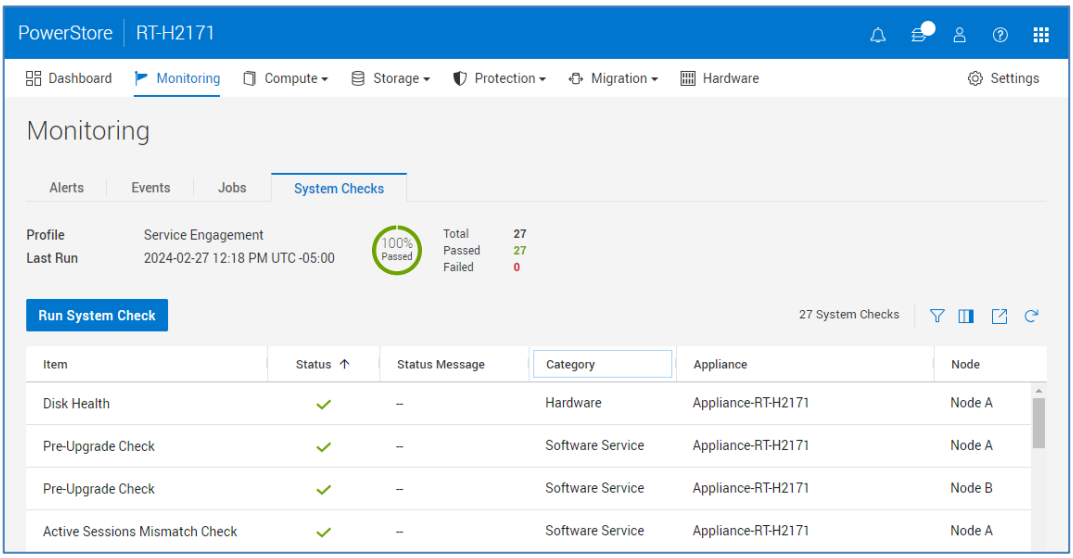

Figure 9. Monitoring page > System Checks

Compute: Hosts & Host Groups, Initiators

The Compute section contains multiple pages, one of which is the **Hosts Information** page as shown in Figure 10. The Host Information page defaults to the **Hosts & Hosts Groups** pane. It allows you to create and manage host configurations which are logical connections through which hosts or applications can access storage resources. When creating a host, the user must select an initiator type based off how the host will connect to the storage, either Fibre Channel, iSCSI, NVMe, or NVMe vVol.

You can pool individual hosts together into a host group. A host group is a collection of hosts that enables you to perform volume mapping operations across all the hosts in the group. For example, when you provision volumes for a host group, the volumes become available to all member hosts. A host group can only use one protocol. You cannot add a host to a host group that uses a different protocol.

NVMe host support is added in PowerStoreOS versions 2.0 and later to support end-to-end NVMe/FC configurations. In PowerStoreOS versions 2.1 and later, NVMe support is extended to also include end-to-end NVMe/TCP host configurations.

vVols can also be accessed using NVMeoF. PowerStoreOS 3.0 and later includes support for NVMe/FC for vVols. PowerStoreOS 3.6 and later includes support for NVMe/TCP for vVols.

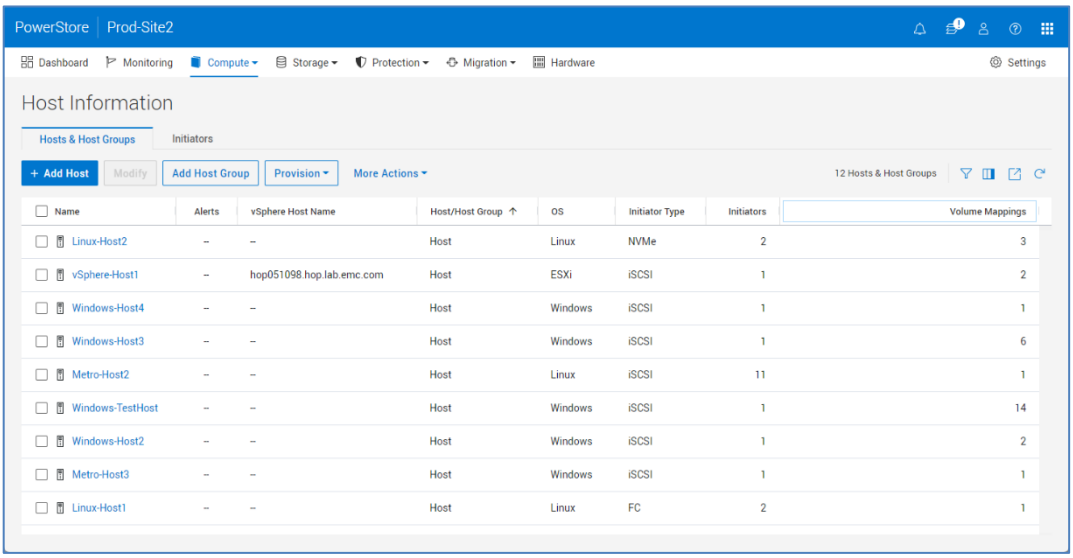

Figure 10. Compute > Host Information > Hosts & Host Groups

The **Host Information** section also contains the Initiators pane in PowerStoreOS versions 3.0 and later as shown in Figure 11. This list view table displays all the initiators and initiator paths in one pane of glass for all supported protocols (iSCSI, FC, NVMe/FC, NVMe/TCP). This makes configuration and troubleshooting much more efficient for users. Click one of the blue initiator links in the identifier column displays the connected paths section of the UI showing the number of connections to node A and B. The total paths displayed make up the number shown on the main initiator pane under the Active Sessions column.

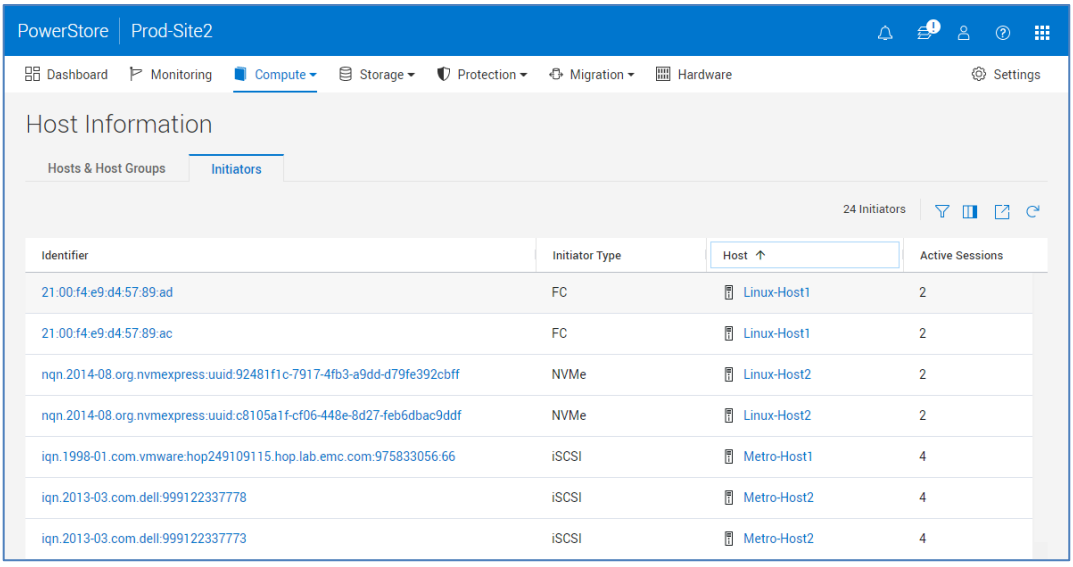

Figure 11. Compute > Host Information > Initiators

Compute: Virtual Machines

PowerStore Manager provides detailed monitoring capabilities for virtual machines (VMs). To access vCenter, launch the vSphere Web Client directly from PowerStore Manager. Under **Compute** > **Virtual Machines** (see Figure 12) you can view performance details, alerts, and connections for the VMs that are configured from the PowerStore cluster. In PowerStoreOS versions earlier than 3.0, you can view and manage data protection

policies. In PowerStoreOS versions 3.0 and later, you can no longer assign protection policies to Virtual Machines. For automatic snapshot creation, use VMware vSphere storage policies. Existing protection policies added to virtual machines on previous codes remain, and you can assign them at any time. The main view shows essential details for each VM, and you can filter, sort, refresh, and export the table data to a spreadsheet if required. VMs that are provisioned from the PowerStore cluster and on an associated ESXi host are added to the table automatically. Prior to PowerStoreOS 3.0, only VMs that are deployed on vVols can be viewed and managed in PowerStore Manager. PowerStoreOS versions 3.0 and later can also view and manage virtual machines on NFS and VMFS datastores. In PowerStoreOS versions 3.0 and later, you can add CPU and memory usage columns using the **Show/Hide Table Columns** icon as shown in Figure 12. This allows you to see whether particular VMs are consuming resources from within PowerStore Manager, to easily monitor and perform troubleshooting.

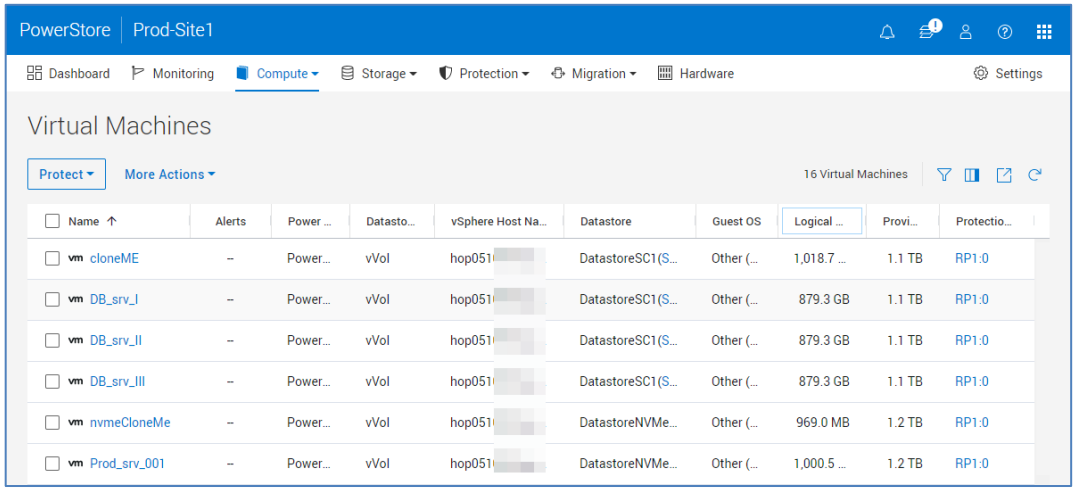

Figure 12. Compute > Virtual Machines

Compute: vCenter Server Connection

PowerStore can configure a vCenter server connection during the Initial Configuration Wizard. For PowerStore T model appliances, this step is optional, and you can configure it manually after initial configuration. To register or manage the vCenter Server connection, go to **Compute** > **vCenter Server Connection** as shown in Figure 13. Click **Launch vSphere** to start the vSphere Web Client and connect to the associated vCenter Server. You can also use this page to update the connection or disconnect as required. PowerStore T model appliances can also register the VASA provider from this page, which allows you to manage VMs that have been deployed on PowerStore storage volumes.

For more information about vSphere integration and registering the VASA provider, see the white paper Dell PowerStore: Virtualization Integration.

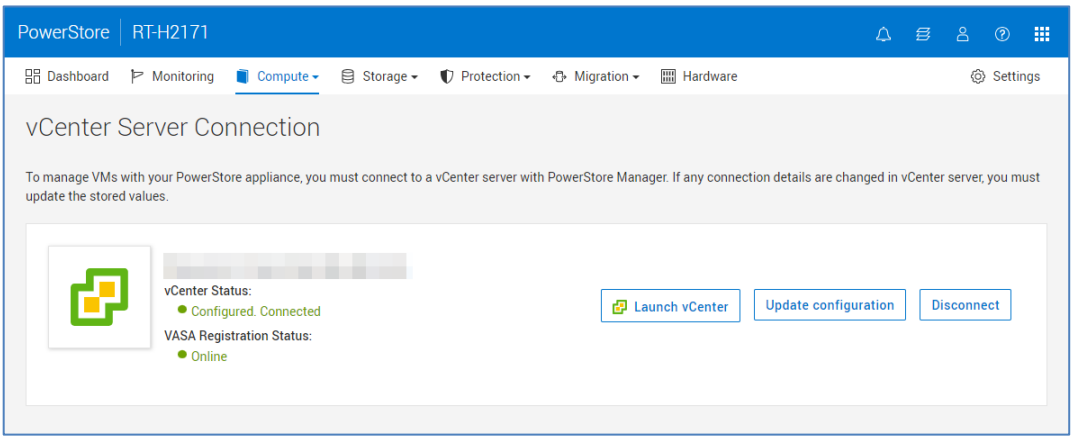

Figure 13. Compute > vCenter Server Connection

Storage: Volumes

In PowerStore Manager > **Storage** > **Volumes** (shown in Figure 14), you can create, view, manage, and delete volumes for the PowerStore appliances in the cluster. You can monitor detailed information about capacity, performance, alerts, protection status, and connectivity within the detailed view of a volume. Thin clones are also created and managed from this page.

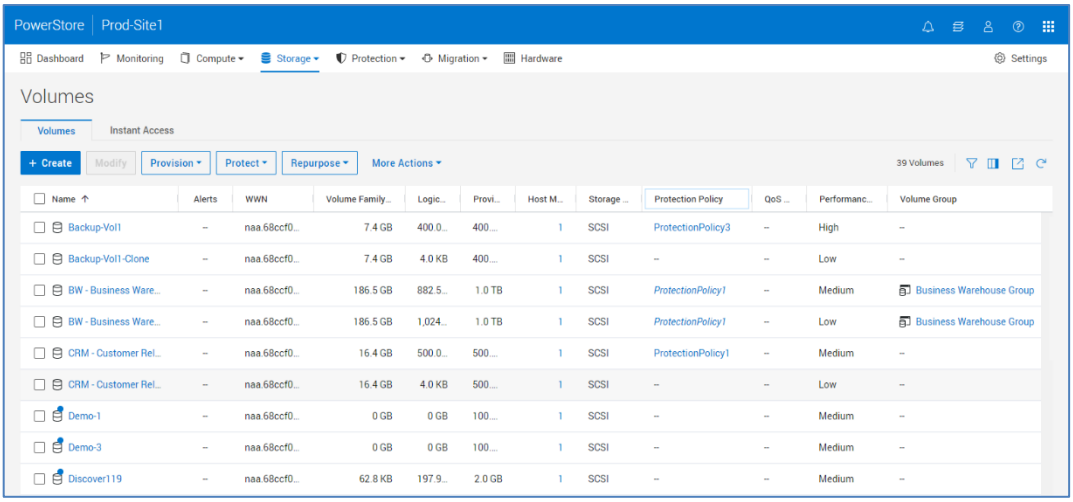

Figure 14. Storage > Volumes

PowerStoreOS 3.0 introduces the Snapshots column to the Volumes, Volume Groups, File Systems, and Virtual Machines list view tables. You can add it to the view by using the Show/Hide Table Columns icon and selecting the **Snapshots** item. This enables you to see how many snapshots are associated with a particular object. You can also click the Snapshots number, which opens the **Protection** pane for the object and shows the specific snapshot details including name, type, or creation time.

PowerStoreOS 4.0 introduces Data Efficiency metric columns such as Volume Family Unique Data, Family Overall DRR, Reducible DRR, and Unreducible Data. Figure 15 shows the new columns and the column options.

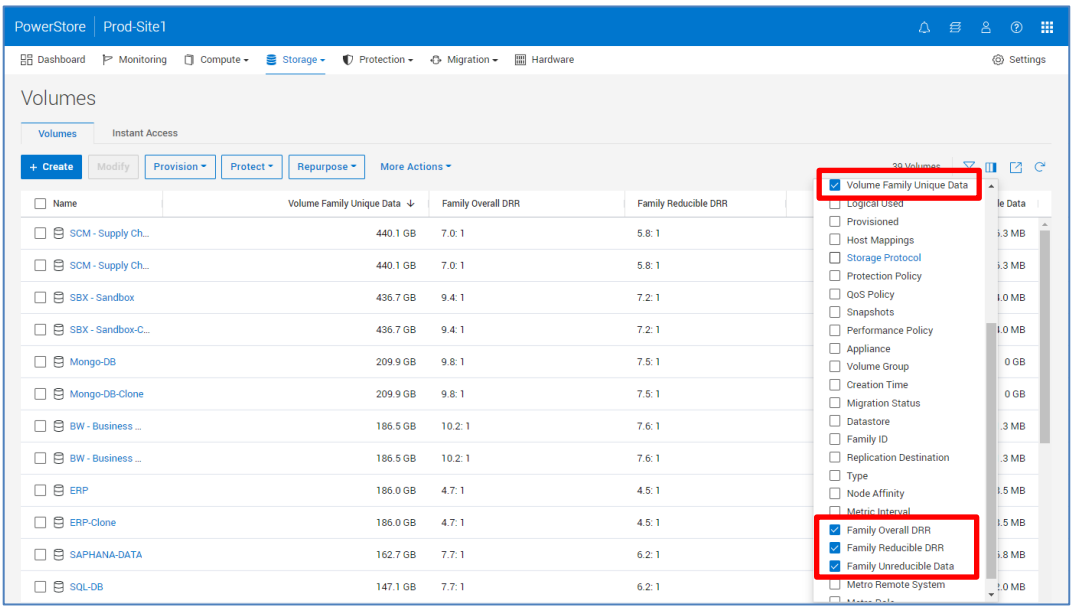

Figure 15. Storage > Volumes > Show/Hide Table Columns

Volume Application Tags

PowerStoreOS 2.1 introduced Volume Application Tags. A Volume Application Tag is specified during volume creation, allowing users to label their volumes with a specific category and application type based on the use case for those volumes (Figure 16).

You can use application-centric management to view and sort through the volumes by application type by adding the new **Application** column in the list view as seen in Figure 17. There are six different predefined categories, each with several different application types. If the application type is not listed, the user can manually enter their own application name. Finally, if the five categories do not match up with the application you are looking for, you can select the **Other** category and optionally enter the application type, up to 32 characters in length.

- **Relational Databases:** Oracle, SQL Server, PostgresSQL, MySQL, IBM DB2
- **Big Data & Analytics:** MongoDB, Cassandra, SAP HANA, Spark, Splunk, ElasticSearch
- **Business Applications:** ERP / SAP, CRM, Exchange, SharePoint
- **Healthcare:** EPIC, Meditech, Allscripts, Cerner
- **Virtualization:** Virtual Servers (VSI), Containers/Kubernetes, Virtual Desktop (VDI)
- **Other:** User specified application type

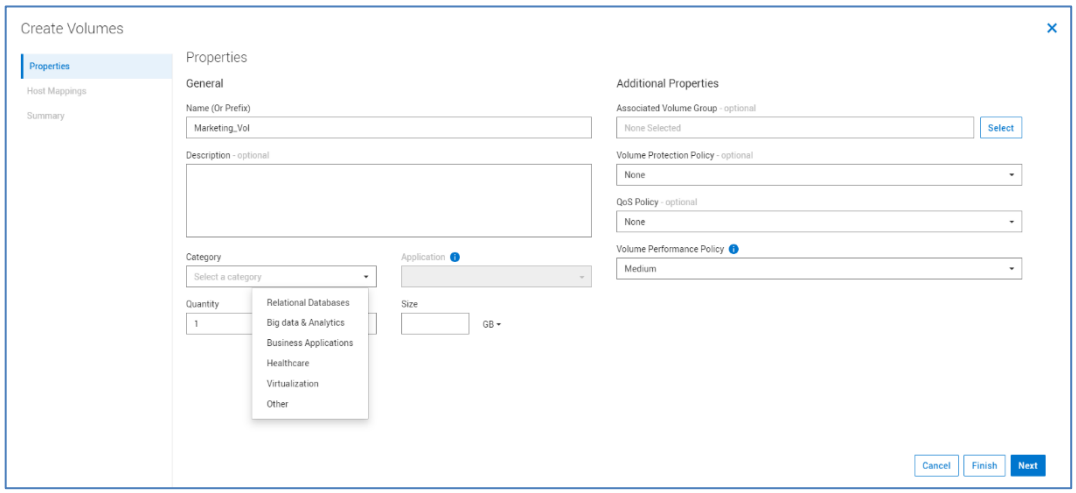

Figure 16. Create Volumes Wizard > Application Category

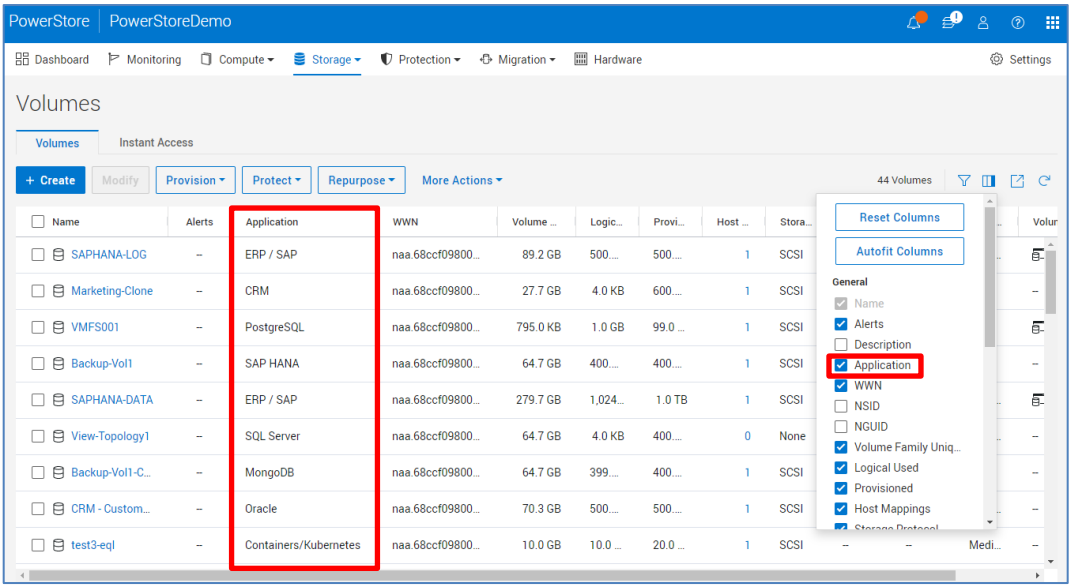

Figure 17. Storage > Volumes > Application Column

Application tags can be changed after a volume is created by modifying the volume properties and specifying a different application category and type. Any existing volumes created before PowerStoreOS 2.1 will not have any Application Tags configured. After upgrading to PowerStoreOS 2.1, the user can manually apply Application Tags to existing volumes. Once an Application Tag is applied to a volume, it cannot be removed, however it can be modified as needed. Application Tags can also be set and managed through the REST API or PowerStore CLI (pstcli).

Designed with interoperability in mind, Application Tags are applied at the volume level and cannot be applied to the Volume Group itself. However, Volume Groups support member volumes with Application Tags. If there are multiple member volumes with different Application Tags, the Volume Group will show as a **Mixed** application category.

Application Tags have also been designed with backwards compatibility in mind. When creating a Volume through REST API or pstcli, the Application Tag fields are not a required field. However, in PowerStore Manager, Application Tags must be specified to

continue the Create Volume Wizard. This is to prevent issues with pre-existing automation scripts or applications after upgrading to PowerStoreOS 2.1.

Consider the following points when applying and managing Application Tags:

- **Cloning Volumes**: Clones of a Volume with an application tag will inherit the tag of the parent volume.
- **Snapshots of Volumes**: Snapshots do not inherit the Application Tags of the source volume, and operations like refresh and restore do not affect the Application Tag of the source volume.
- **Internal Migration of Volumes**: The Application Tag will be migrated and retain the same value as the source volume.
- **Importing Volumes**: Imported Volumes will not have an Application Tag set and can be modified post-import to add an Application Tag.
- **Replication:** The Application Tags are always replicated to the destination volume.

View Topology

PowerStoreOS versions 3.0 and later allow you to view information about the topology of a volume or volume group. This feature provides a hierarchy as a graphical family tree between volumes, clones, and snapshots. This makes it efficient to visualize the family relationship with one click, as opposed to querying the data based on the family ID, which can be time-consuming. This feature is supported for volumes and volume groups. Figure 18 shows that after you select a volume, you can click **More Actions** > **View Topology** to see the topology.

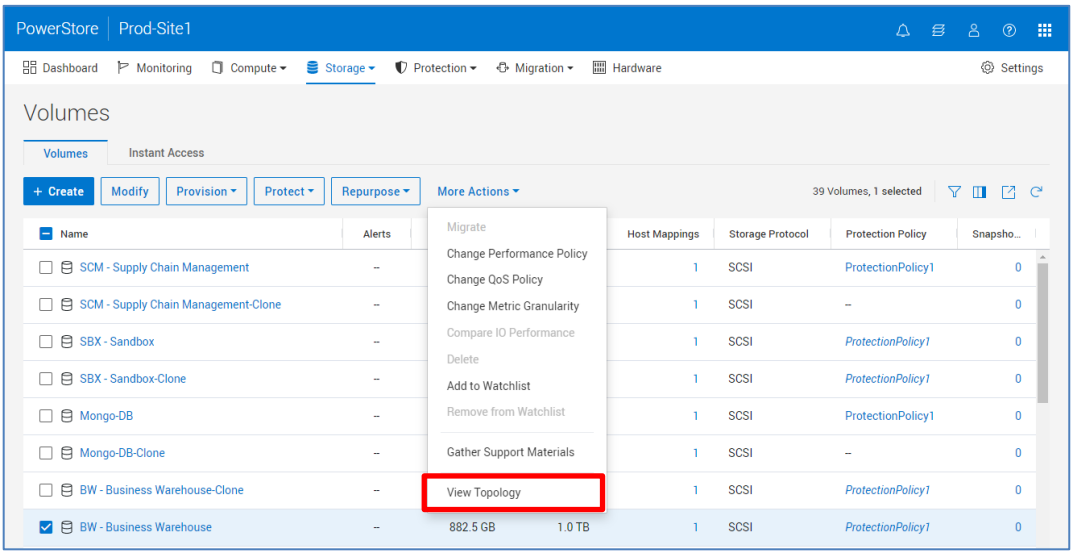

Figure 18. Storage > Volumes > View Topology

Figure 19 shows an example of the Topology for the volume **BW – Business Warehouse**. Notice that below the **Snapshots** icon, the volume has four snapshots created. There is also a clone created from snap5. You can click the different objects in the topology to show more detailed information about the panes on the right, such as the details, capacity, and hosts the volume is mapped to.

You can collapse and expand objects in the topology with the minus and plus signs, and you can also drag objects to reposition them as wanted. Any user changes to the view persist and remain intact, even after a logout. You can also use the search box to search for specific items. This new view allows you to understand impacts of your actions and avoid errors.

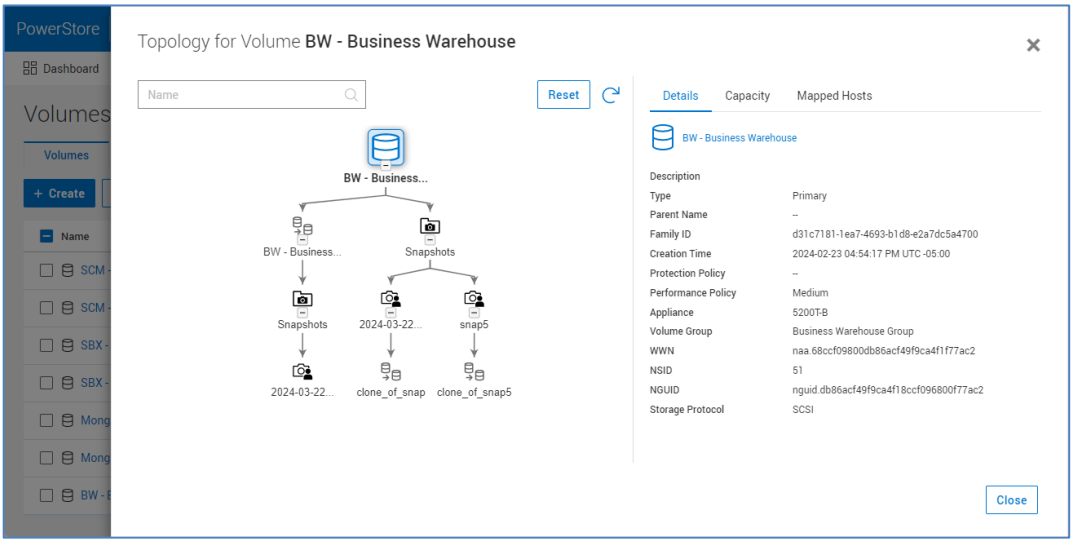

Figure 19. Storage > Volumes > Topology

Figure 20 shows the capacity and family capacity details on the capacity pane. The family capacity includes all space consumed by the base volume, and all clones and snapshots including internal system snapshots used for replication. The capacity shown may not always match the objects in the topology. In PowerStoreOS version 4.0 and later, Volume Family Unique Data, Overall DRR, Reducible DRR, and Unreducible Data metrics can be viewed from this pane as well.

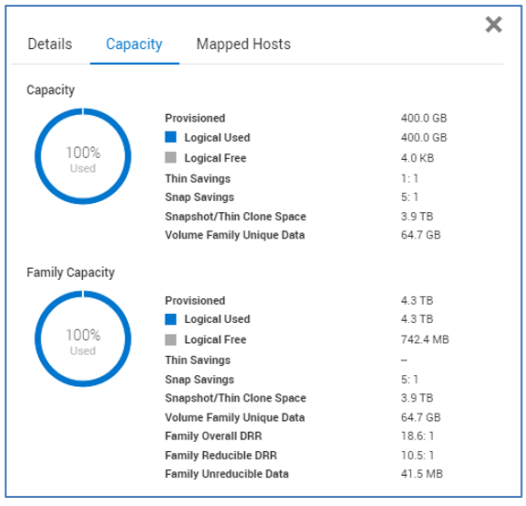

Figure 20. View Topology > Capacity Tab

Storage: Volume Groups

A volume group is a logical container for a group of volumes and provides a single point of management for multiple storage resources that work together as a unit. For example, you can use volume groups to monitor metrics and manage data protection for

development applications, user applications, and user storage resources. You can also use volume groups to separate the management of test environments from development environments.

To configure a volume group in PowerStore Manager, go to **Storage** > **Volume Groups** as shown in Figure 21. In this page, you can create, view, manage, and delete volume groups. On this page, you can also create and manage thin clones from volume groups. To monitor the capacity, performance, protection status, and view members of a volume group, click the name of the group to display it in the page table.

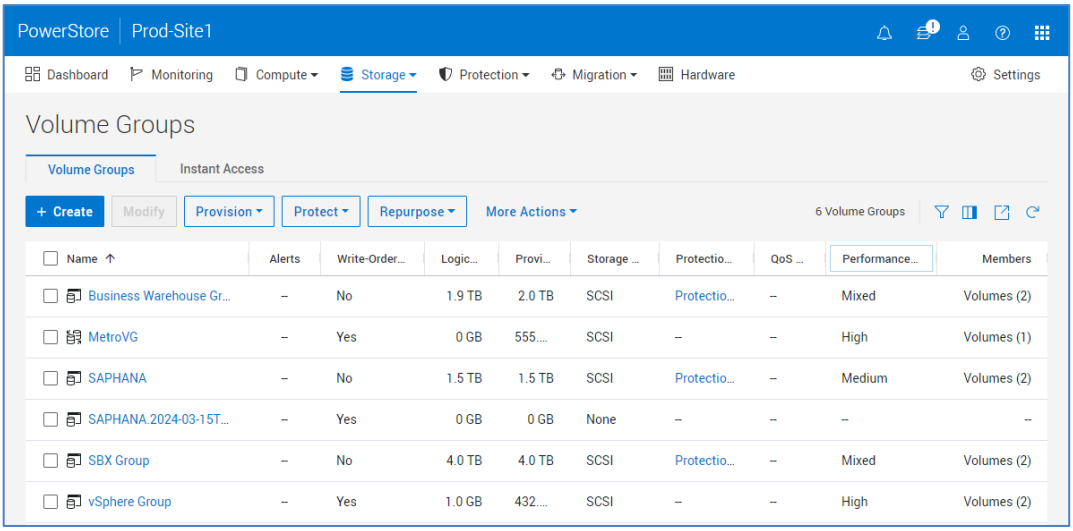

Figure 21. Storage > Volume Groups

Storage: Recycle Bin

In PowerStoreOS versions 3.5 and later, a recycle bin is supported for block volumes, volume groups, and clones. This allows users an additional way to prevent accidental deletion of block storage. When a resource is deleted in the GUI, it will be placed into the Recycle Bin by default. Users have the option to skip the recycle bin in the delete resource window, causing immediate deletion. Note that deleting a volume has the same prerequisites as previous PowerStoreOS versions.

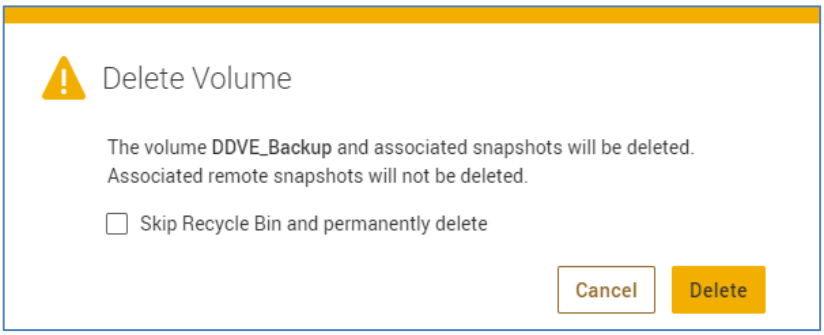

Figure 22. Delete Volume Window

When a block storage resource has been placed in the Recycle Bin, a user has two options: **Expire Now** or **Recover**. Expire Now will trigger expiration and immediately delete the object; the Recover option will restore the object back into the storage section for use. The expiration duration for resources in the Recycle Bin can be configured

between 0-30 days. The default setting is seven days. Setting the value to 0 days causes resources to expire immediately.

Important: The Recycle Bin expiration setting applies to the entire cluster. While resources are in the recycle bin, they still consume storage capacity and count against system limits.

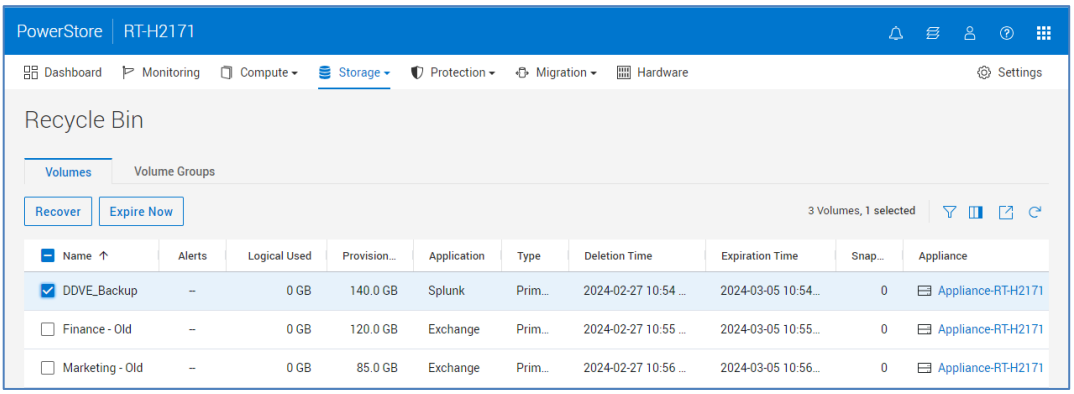

Figure 23. Recycle Bin

Storage: Storage Containers

You can use a storage container to present vVol storage from PowerStore to vSphere. vSphere mounts the storage container as a vVol datastore and makes it available for VM storage. In PowerStoreOS versions 3.0 and later, storage containers are classified as either SCSI or NVMe. This classification dictates the storage protocol that they support. In previous versions of PowerStoreOS, all storage containers were considered SCSI by default. A storage container spans all appliances in the cluster and uses storage from each. The specific appliance that a given vVol resides on is visible in PowerStore Manager, and you can migrate a vVol between appliances in the same cluster. Use the **Storage** > **Storage Containers** page (Figure 24) to create and manage storage containers within PowerStore Manager.

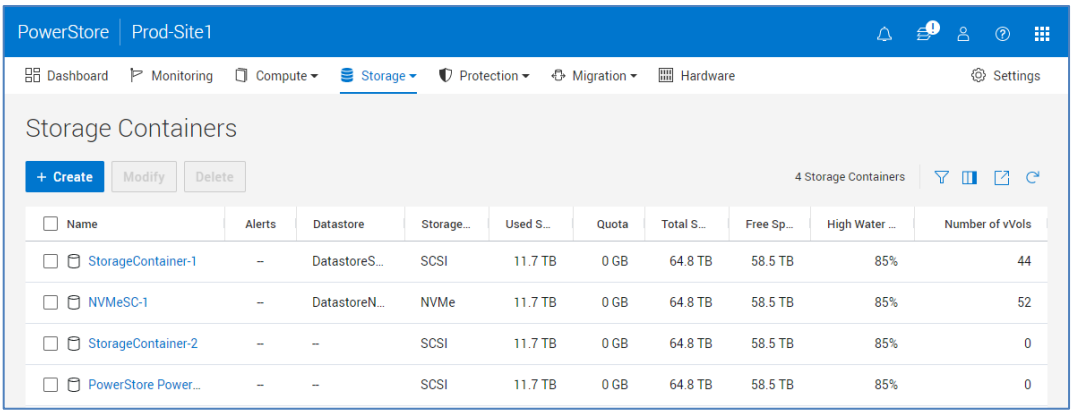

Figure 24. Storage > Storage Containers

Storage: NAS Servers

Before file systems on a Unified PowerStore appliance are configured, you must create a NAS server. A NAS server is a virtualized network-attached storage server that uses SMB, NFS, FTP, or SFTP protocols to catalog, organize, and transfer files within file-system shares and exports. A NAS server, the basis for multitenancy, must be created before you can create file-level storage resources. A NAS server is responsible for the

configuration parameters on the set of file systems that it serves. To create, view, manage, or delete NAS servers, use the **Storage** > **NAS Servers** page in PowerStore Manager, as shown in Figure 25.

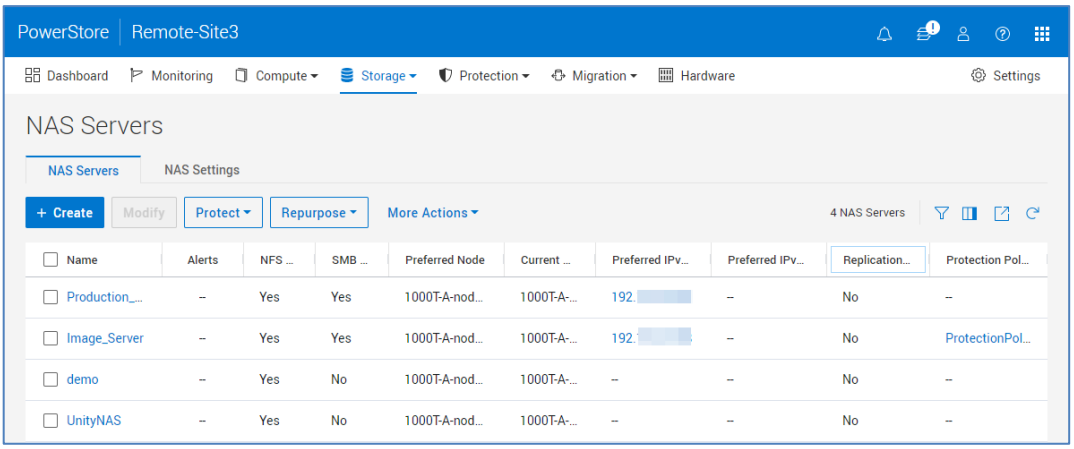

Figure 25. Storage > NAS Servers

Common Anti-Virus Agent (CAVA) enables third party software to identify and eliminate known viruses before they infect files on SMB shares. PowerStoreOS versions 4.0 and later allow users to manage and configure CAVA directly through PowerStore Manager, CLI, and REST API without any third-party tools.

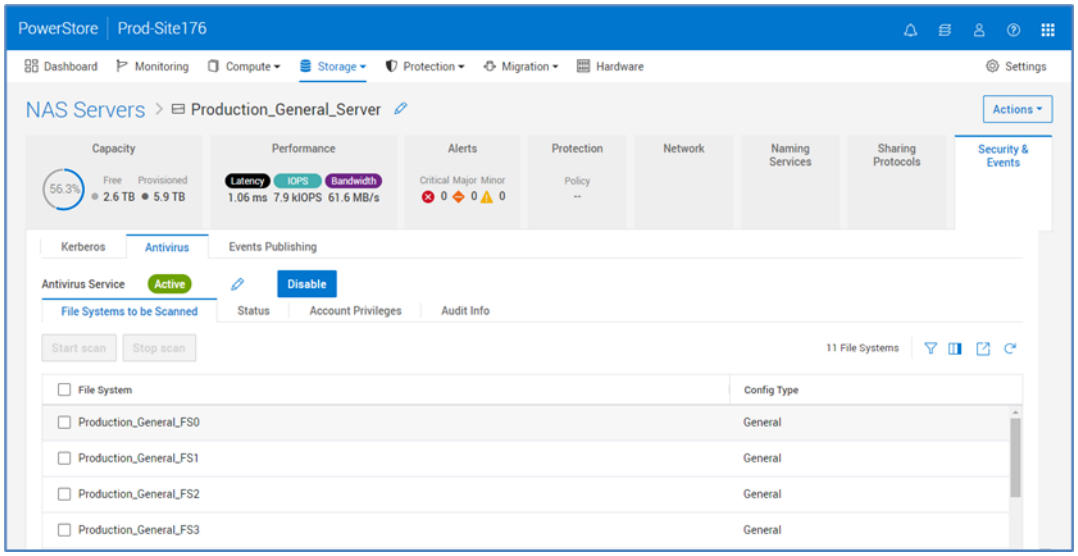

Figure 26. Storage > NAS Servers > Security & Events > Antivirus

Storage: File Systems

A file system represents a storage resource that provides network file storage. The types of file systems that you can create are determined by the file-sharing protocols (SMB, NFS, or multiprotocol) that are enabled for NAS servers on the PowerStore appliances in your cluster. You can create, view, manage, and delete file systems, SMB shares, and NFS exports from the **Storage** > **File Systems** page as shown in Figure 27.

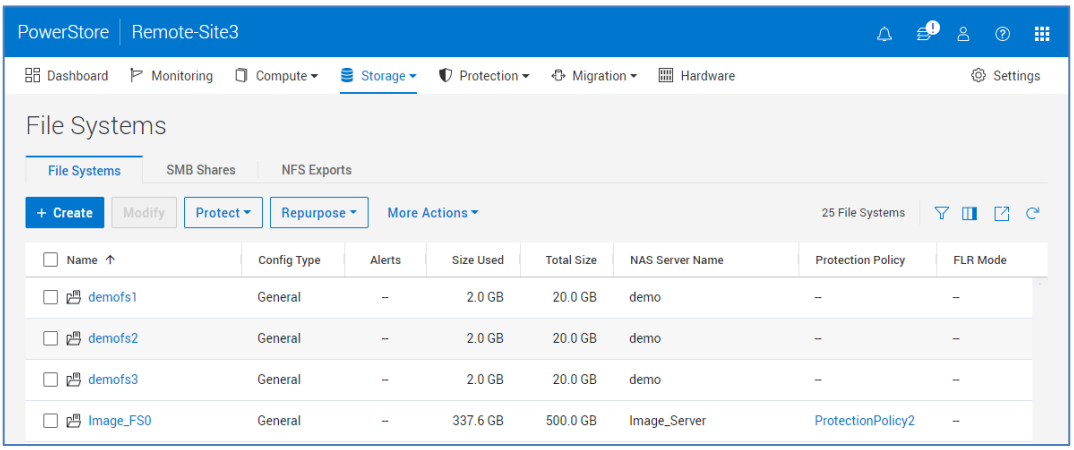

Figure 27. Storage > File Systems

Storage: Quality-of-Service (QoS) is the ability to limit the performance capabilities of a resource. This allows granular prioritization of I/O for storage resources to ensure administrators meet their SLAs within their organization. Limits can be placed on non-critical applications, which frees resources for other applications. PowerStoreOS versions 4.0 and later support QoS for block storage resources. To set QoS on a resource, a Block IO Limit Rule and QoS Policy must be created. The Block IO Limit rule object specifies the type of rule to implement and the metric to limit. Block IO limit rules support Absolute and Density based limits. I/O can be limited using an IOPs limit, bandwidth limit, or a combination of the two. QoS can be found by navigating to **Storage > Quality of Service (QoS)**. For more information about configuring Block QoS Policies and Block IO Limit Rules, see the Dell PowerStore Configuring Volumes guide.

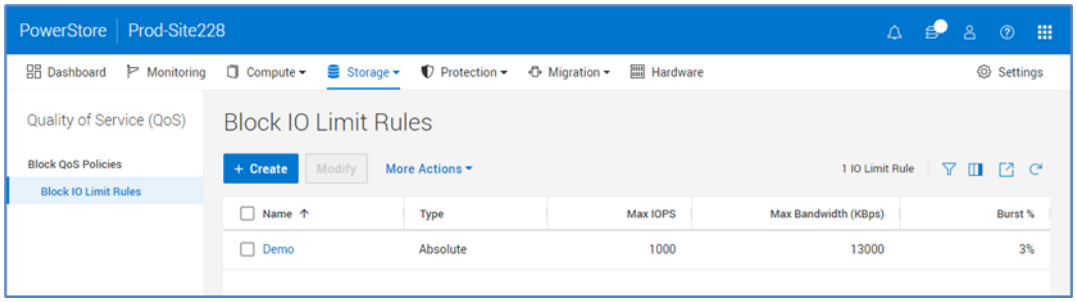

Figure 28. Storage > Quality of Service (QoS) > IO Limit Rules

Protection: Remote Systems

You can use the **Protection** > **Remote Systems** page (Figure 29) to configure remote system connections between source and destination PowerStore clusters to enable remote replication. For PowerStore, the remote system connection is associated with a replication rule which is applied to a supported storage resource. You can create remote system connections ahead of time in the **Remote Systems** page, or while creating a replication rule.

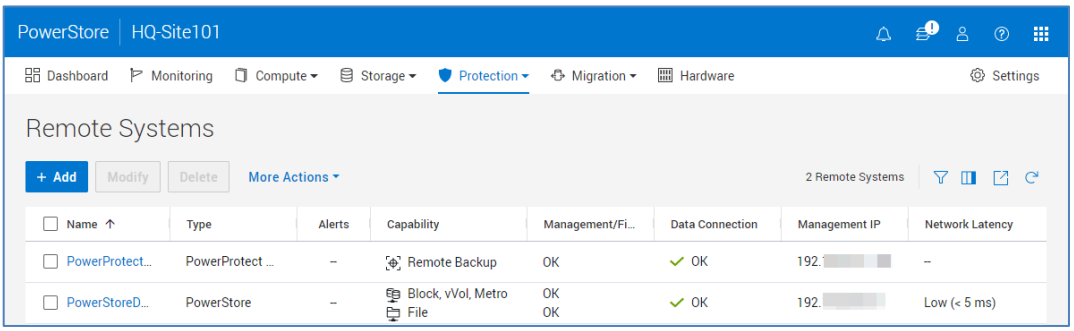

Figure 29. Protection > Remote Systems

Protection: Replication

Data replication is a process in which storage data is duplicated to a remote cluster, which provides an enhanced level of redundancy if the main storage system fails. Replication minimizes the downtime-associated costs of a system failure and simplifies the recovery process from a natural disaster or human error.

PowerStore has consistently provided asynchronous replication for block storage. However, with the introduction of PowerStoreOS 3.0, this feature was extended to file storage. As a result, all data types, whether housed in block or file volumes, or within volume groups, can be replicated in an asynchronous manner.

Asynchronous replication of vVol-based VMs is also supported with PowerStoreOS versions 3.0 and later with VMware SRM integration.

In PowerStoreOS versions 4.0 and later, native synchronous replication is supported. This is available for Network Attached Storage (NAS) servers along with their underlying file systems, volumes, and volume groups.

When a protection policy with a replication rule is applied to a volume, volume group, or NAS server, the related replication session that is created appears in **Protection** > **Replication** page (Figure 30). You can use this page to monitor, pause, or fail over replication sessions as needed.

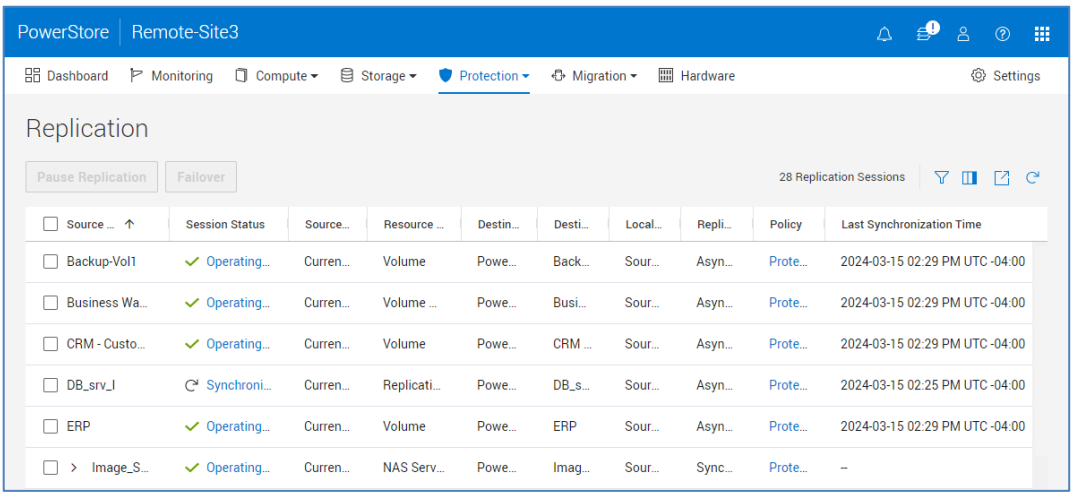

Figure 30. Protection > Replication

Protection: Metro

PowerStoreOS versions 3.0 and later support the Metro Volume implementation, which you can use for disaster avoidance, application load balancing, and migration scenarios. This feature provides active-active I/O to a Metro Volume across two PowerStore clusters. It supports FC/SCSI or iSCSI-connected VMware ESXi hosts. In PowerStoreOS version 4.0 and later, the system has expanded metro support to volume groups as well as Linux and Windows hosts. When Metro Volume is implemented, you can see the details in **Protection** > **Metro** page (Figure 31). You can use this page to monitor, end, pause, and to set the local preferred role.

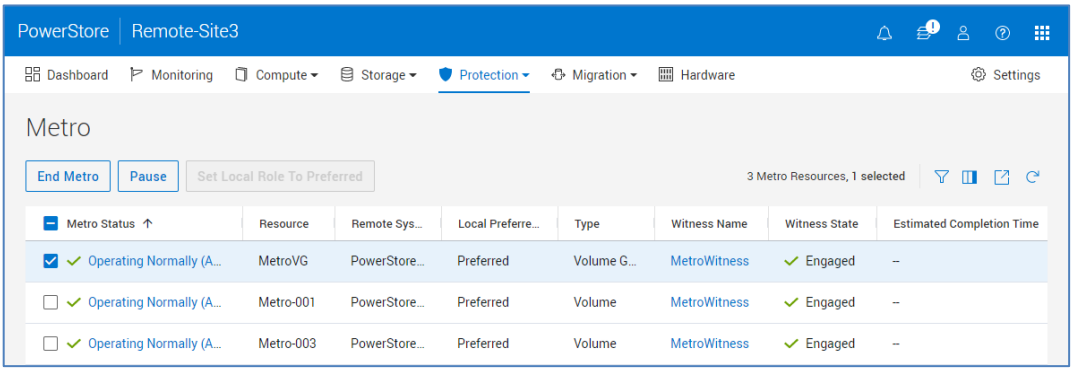

Figure 31. Protection > Metro

Protection: Metro Witness

Starting with PowerStore version 3.6, Metro Volume supports a witness server. The witness server is software that is installed on a host at a third site. The witness monitors the status of the local and remote PowerStore systems. When a failure occurs, the witness determines which system remains accessible to hosts and continues to service I/Os. This adds more resiliency and further mitigates the potential risk of split-brain scenarios.

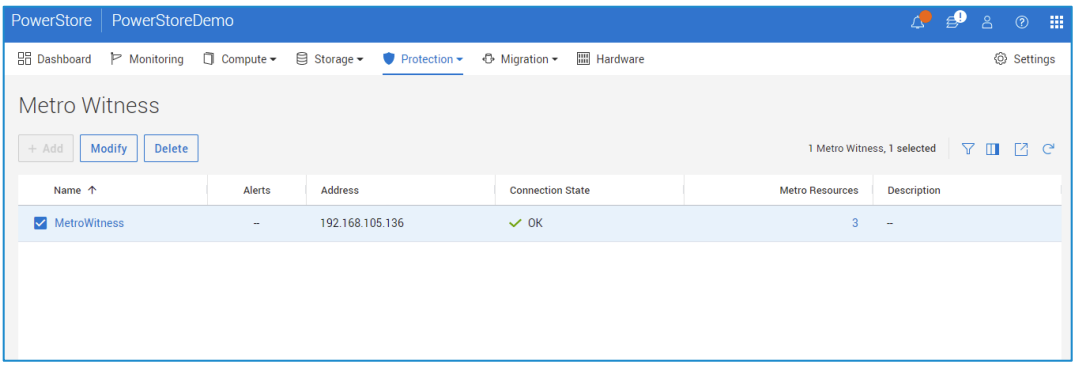

Figure 32. Metro Witness (Protection > Metro Witness)

Protection: Native PowerProtect DD Backup Integration

In PowerStoreOS version 3.5 and later, the system can complete backups directly to a PowerProtect Data Domain series appliance. A PowerProtect DD system would need to be added as a remote system under **Protection > Remote Systems**. This feature allows the backup traffic to be directly offloaded to the backup storage appliances, which eliminates the need for a backup host. PowerStore supports both physical and virtual edition (DDVE) PowerProtect appliances. Backups are supported on volumes and volume groups.

There are three primary functions when using the remote backup feature:

- **Backup Session** – Backs up data from a supported storage object to a PowerProtect DD system. The data is backed up in the form of a point-in-time snapshot on the PowerProtect appliance.
- **Retrieve Session** – Allows users to pull data from a PowerProtect appliance to a PowerStore appliance.
- **Instant Access** – Allows hosts connected to a PowerStore appliance to temporarily access the data residing on the PowerProtect DD series appliance.

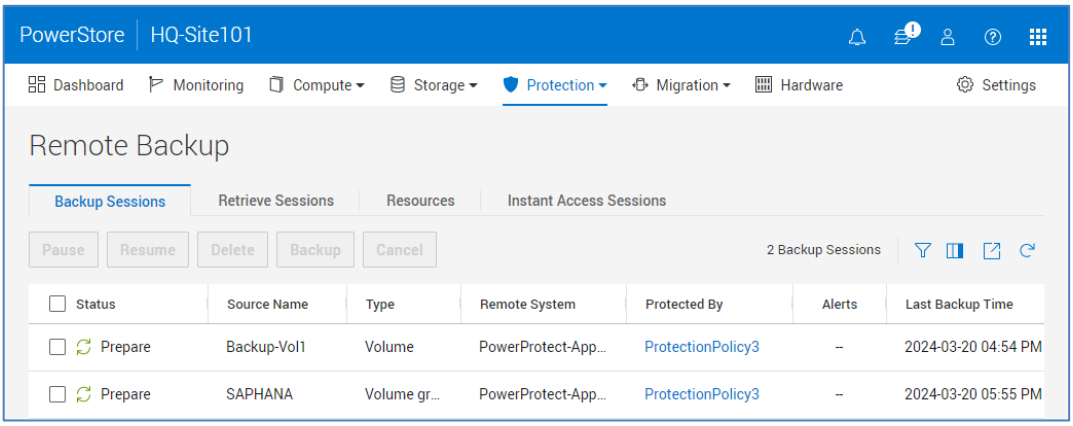

Figure 33. Protection > Remote Backup

Protection: Protection Policies

A protection policy consists of snapshot rules, a replication rule, a remote backup rule, or a combination of each that you create to establish consistent data protection across storage resources. After you configure a protection policy, you can associate new or existing storage resources with the protection policy. Remote backup rules are used with the native PowerProtect DD backup integration feature which was introduced in PowerStoreOS 3.5.

Protection policies automatically manage snapshot, replication, and backup operations that are based on the included rules. You can create policies with various rules to meet your local and remote protection needs and assign a policy to resources to provide identical protection to those resources.

Each protection policy can only include one replication rule, one remote backup rule, and up to four snapshot rules. To create and manage protection policies, go to **Protection** > **Protection Policies** as shown Figure 34.

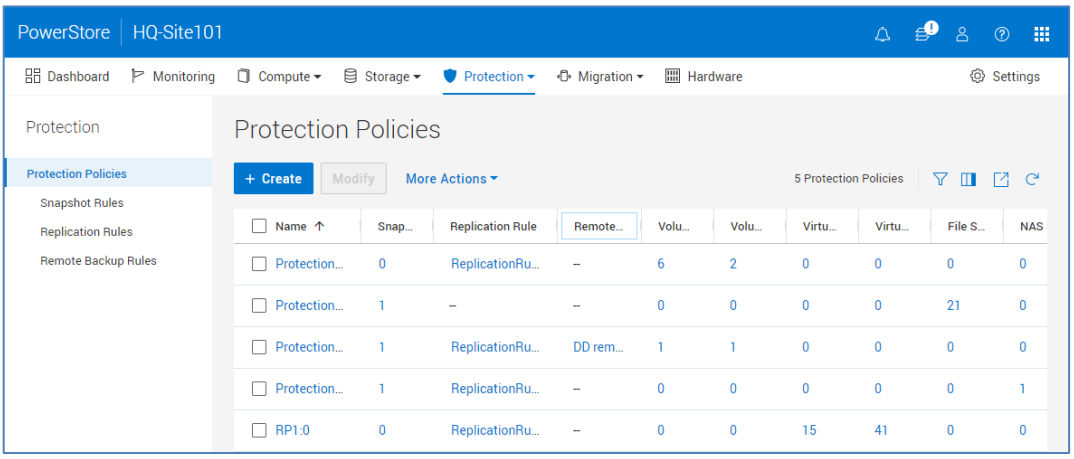

Figure 34. Protection > Protection Policies

Migration: Migration Actions

There are two ways to migrate storage resources in PowerStore Manager: manual migration and assisted migration. When a volume or volume group is provisioned on a specific appliance, you can choose to manually migrate the storage resource to another appliance in the cluster later. Assisted migrations are recommendations that are based on regular monitoring of storage resources across the appliances in the cluster. These recommendations are generated based on many factors including drive wear, appliance capacity, host connectivity, and health. Recommendations are shown under **Migration** > **Internal Migration** as shown in Figure 35. Before removing or shutting down an appliance for service, use this feature to migrate storage resources to another appliance and prevent disruption. When you migrate a volume or volume group, all associated snapshots and thin clones also migrate with the storage resource. To start a migration, select the associated migration action and click **Start Migration**.

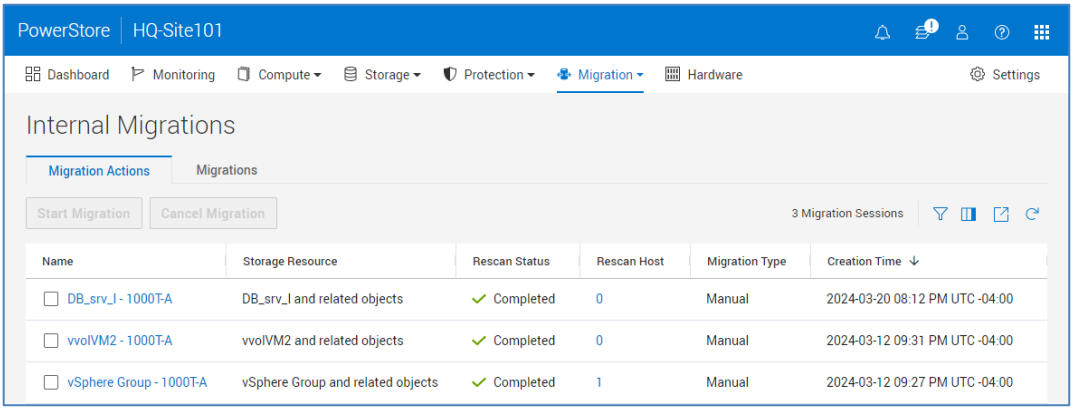

Figure 35. Migration > Internal Migrations

Migration: Internal Migrations

When a migration is initiated, all migration sessions are displayed under **Migration** > **Internal Migrations > Migrations** as shown in Figure 36. This page allows you to easily monitor migrations in the cluster and determine the status of each migration along with an estimation of completion time.

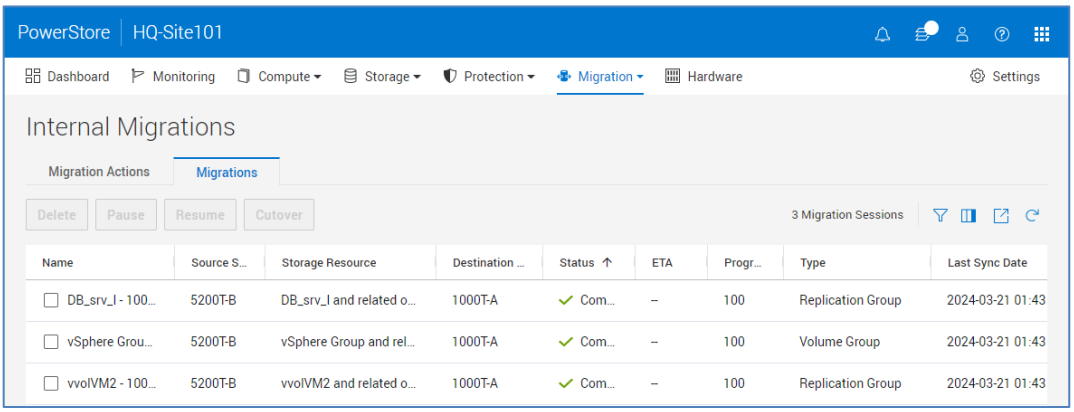

Figure 36. Migration > Internal Migration > Migrations

Migration: Import External Storage

PowerStore supports importing external storage from supported storage platforms. The PowerStore import feature supports the following block storage resources from other arrays: LUNs and volumes, consistency groups and volume groups, and thick and thin clones, depending on the source system. PowerStore can manage the import process non-disruptively with a host orchestrator called a host plug-in which is installed on all hosts that access the source data. Agentless import is also supported, but it is a disruptive process which requires application downtime. Go to **Migration** > **Import External Storage** (see Figure 37) to connect to supported storage platforms and enable a nondisruptive import. To connect to a remote system from PowerStore, you must have the management IP address, iSCSI IP addresses, and credentials. FC target WWNs are automatically discovered.

PowerStoreOS versions 3.0 and later support native file import. Dell VNX2 is supported with 3.0 and later, and Unity is supported with 4.0 and later. This capability includes support for both NFS and SMB file systems. Proper networking and configuration of the **File Import Interface** is required to use this import functionality.

PowerStoreOS versions 4.0 and later support import from universal remote systems, which allows the PowerStore to perform agentless imports for a wide range of block storage systems. FC and iSCSI backend connections are supported and the discovery does not require control path connectivity to the remote storage system.

For more information about imports and the import process, see the white paper Dell PowerStore: Migration Technologies.

Note: Ensure that all existing hosts and storage systems are referenced in the PowerStore Simple Support Matrix. If a system is not referenced, open an RPQ for support.

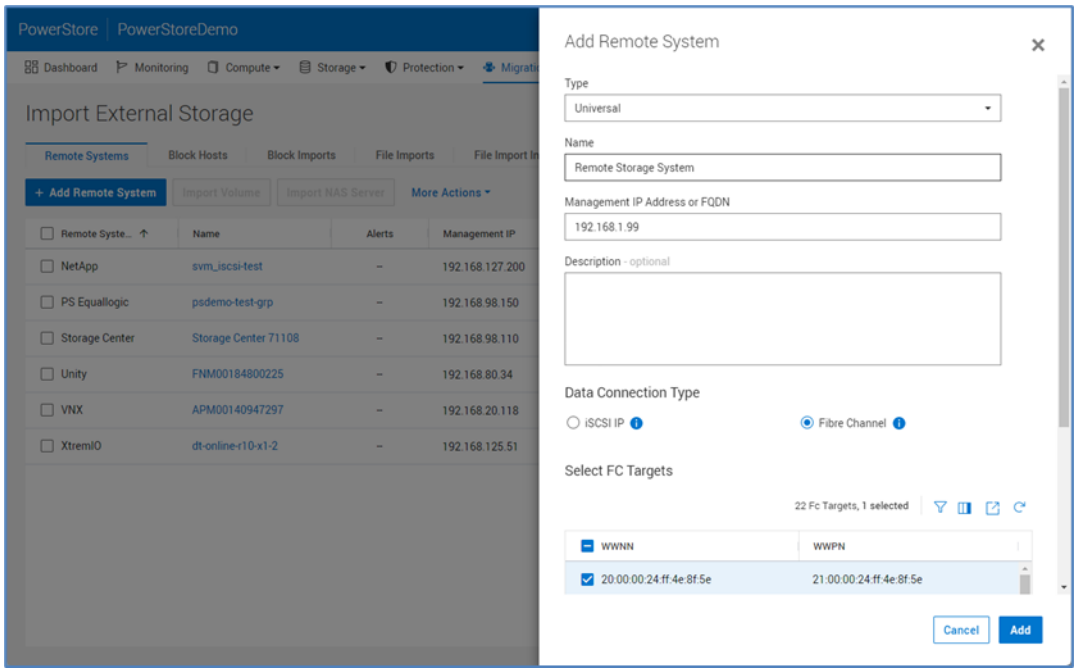

Figure 37. Migration > Import External Storage > Add Remote System

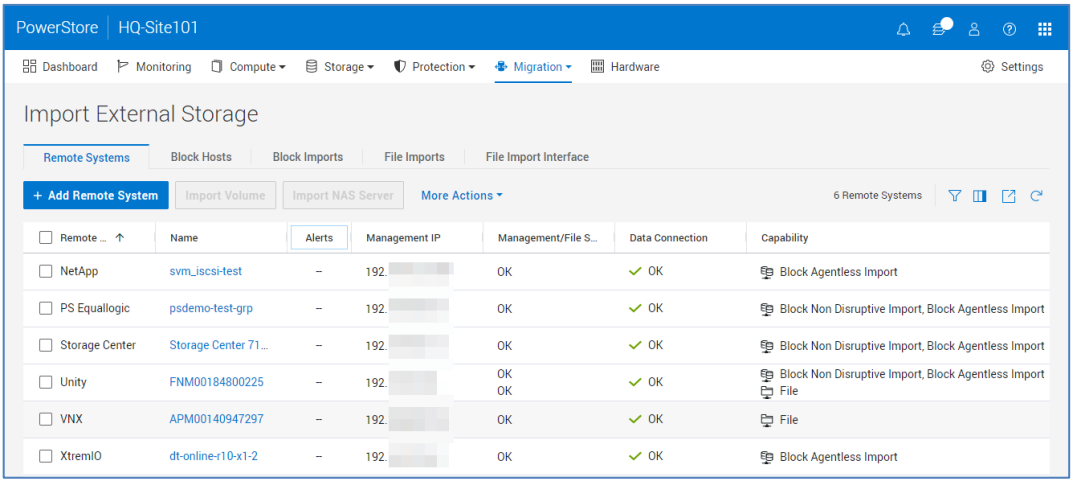

Figure 38. Migration > Import External Storage

Migration: Imports

After an import is successfully initiated, the import session displays under **Migration** > **Import External Storage** > **Block Imports or File Imports** (Figure 39). This page allows you to manage the import sessions as required including the following supported operations: Cancel, Cutover, Enable Destination Volume, Start Copy, Pause, Resume, and Cleanup. During an ongoing import, a cancel operation enables you to change the active path to the source storage resource. When a cutover operation is performed, the import session can no longer be canceled.

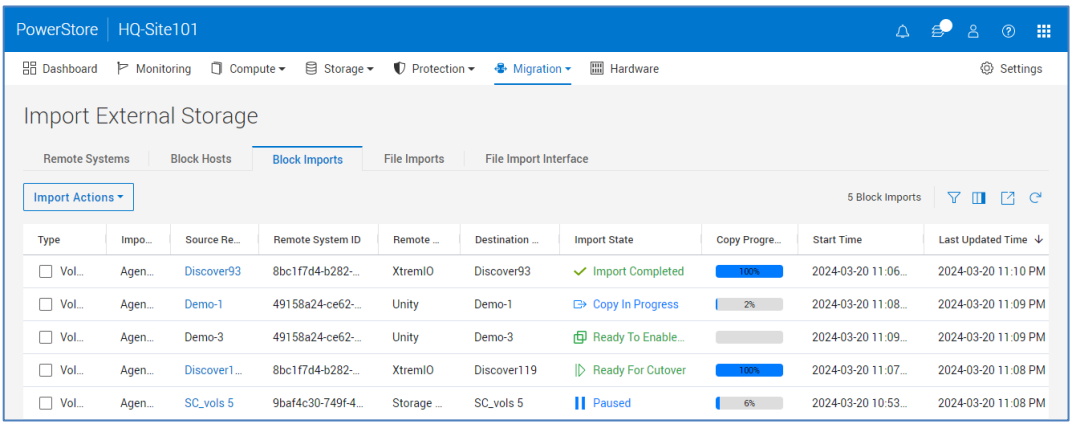

Figure 39. Migration > Import External Storage > Block Imports

Table 5 shows the actions available for import sessions along with the associated descriptions. An action depends on the import job current state.

Table 5. Import actions

Action	Overview
Cancel	• Cancels import session and goes back to source • Terminates a session that has not been cutover • Disables access to the destination volume • Deletes the destination volume or volume group associated with the import session
Cutover	• Cuts over the resource in PowerStore • Stops background copy and removes host mappings from source **Note**: After a cutover has been completed, it cannot be canceled, and it is not possible to revert to the source resource.
Pause	• Suspends a copy-in-progress import session • Only pauses the background copy; host I/O is still mirrored
Resume	• Resumes a paused session • Starts the background copy again from where it was paused and continues the host I/O mirroring
Cleanup	• Removes an import session in clean-up-required state • Removes an import session that had a failure

Actions applicable to Agentless Import	
Enable Destination Volume	**Note:** Before you select this action, ensure the host application accessing the source volume or volumes is shut down. Also, ensure the host mappings are removed from the volume or volumes in the source system. • Enables destination resource for writes • Connectivity with the source system goes into inactive state For each import session that is in the **Ready To Enable Destination Volume** state, select the import session, and select **Import Actions** > **Enable Destination Volume** to progress each import session to the **Ready to Start Copy** state.
Start Copy	**Note:** Ensure the host application has been reconfigured to access and use the destination volume or volumes in PowerStore. • Starts the background copy and continues the host I/O mirroring For each import session that is in the **Ready to Start Copy** state, select the import session, and select **Import Actions** > **Start Copy** to progress each import session to the **Copy In Progress** state

Hardware

For PowerStore, an appliance consists of a base enclosure and optional expansion enclosures. A base enclosure includes two nodes and slots for up to 25 drives, while expansion enclosures enable adding more drives and increasing the storage capacity of the appliance. To view the overall health of the physical hardware of appliances, go to **Hardware** > **Appliances** as shown in Figure 40. This page lists all appliances that are associated with the cluster. Click an appliance in the table to display the appliance details page to review more information.

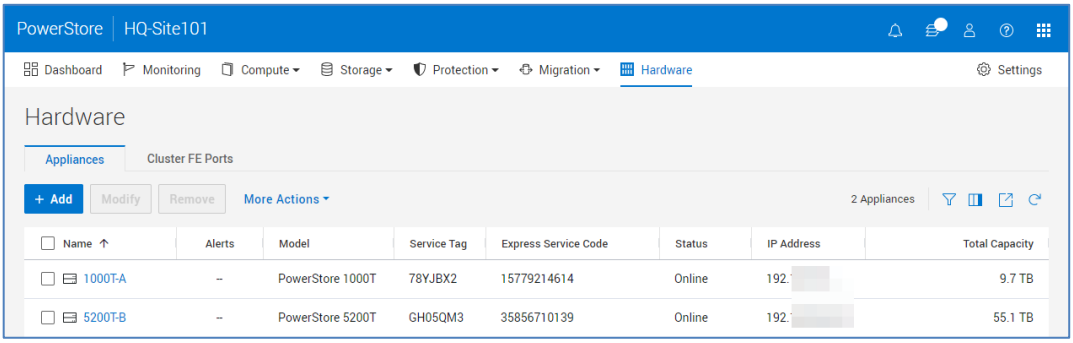

Figure 40. Hardware page

In the appliance details page, you can review the metrics, alerts, and health information for the selected appliance and its associated components (Figure 41). This information is similar to the Dashboard view, but is filtered for the selected appliance, which is useful in daily administrative tasks. In terms of physical hardware component health and status, click the **Components** card on the right side of the page. In the components view, you can see different views of the base enclosure including **Drives** (Figure 42), **Rear View**, and **Top View**. Each view has different components that can be selected for more information including the part number, health status, and other component-specific details. When a component has an issue or is faulted, the graphical figure indicates an alert, depending on the type of issue, to visually notify the user of an error.

On the **Drives** tab, there is an option to **Blink LED**. When the base enclosure is selected, click the button to blink all LEDs for the drives, the base-enclosure LED, and the rear-fault LED simultaneously. This action is useful when you are trying to identify a particular system in a rack of multiple appliances. Click the button again to stop the LEDs from blinking. When a specific drive is selected, click **Blink LED** to blink the LED of only that drive. This action is useful when an individual drive must be located in the data center.

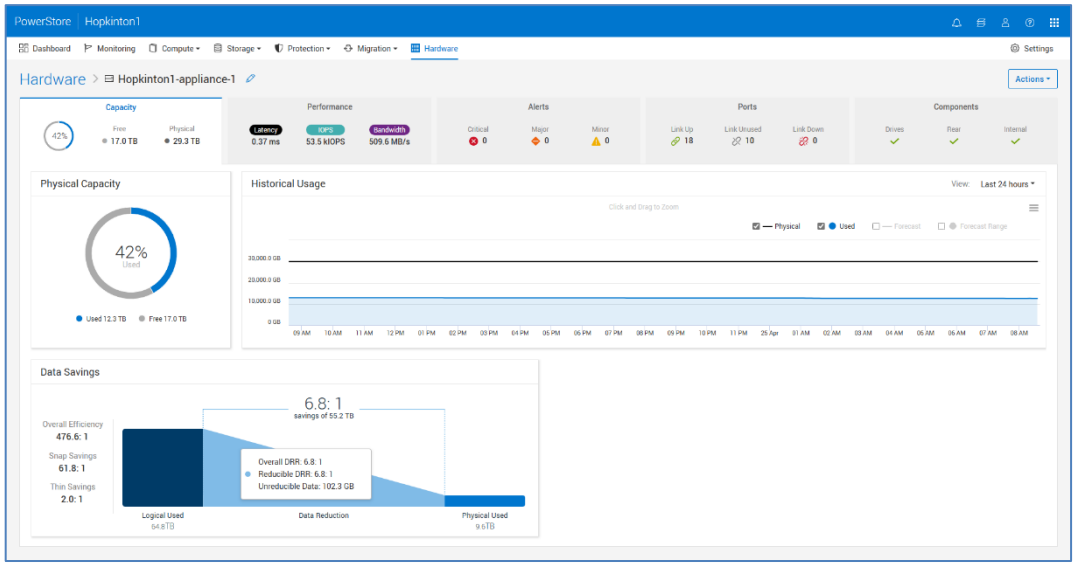

Figure 41. Hardware > [APPLIANCE] > Capacity tab

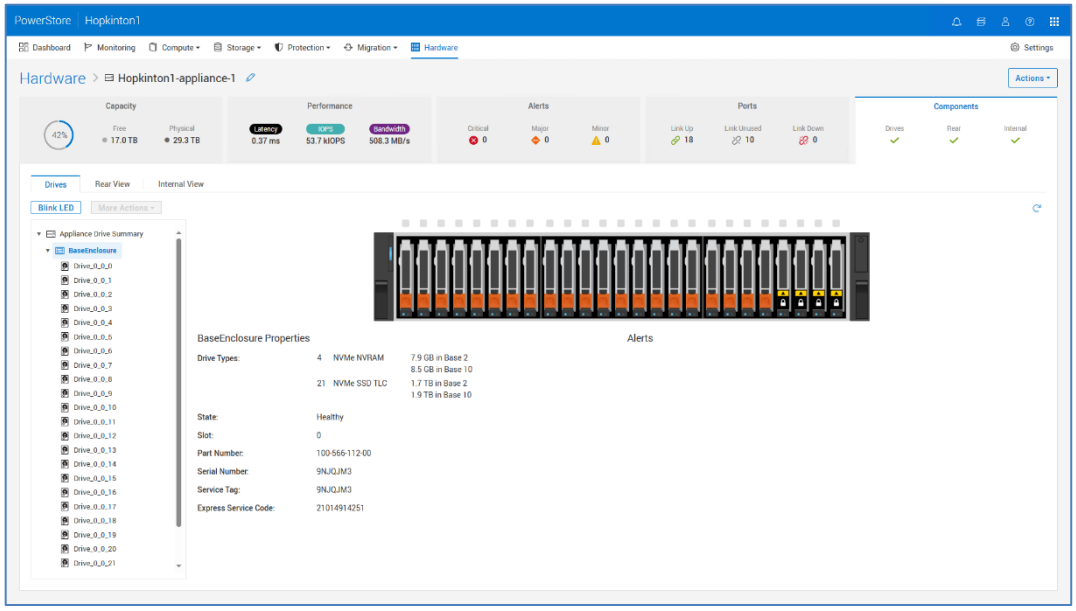

Figure 42. Hardware > [APPLIANCE] > Components > Drives

Appliance Performance

From the **Hardware > [APPLIANCE] > Performance** card, you can view performance metrics for the selected appliance. Performance data is polled every 20 seconds and rolled into timeline charts that update at different frequencies depending on the timeline selected.

- **Last hour** data is updated every 20 seconds.
- **Last 24 Hours** data is updated every 5 minutes.
- **Last 1 month** data is updated every 1 hour.
- **Last 2 years** data is updated every 24 hours.

You can select different performance categories from the drop-down menu on the left column. The following table shows the performance metric categories available from the drop-down menu.

Table 6. Appliance Performance Metrics

Category	Metrics	Description
Summary	Latency, IOPS, Bandwidth	Displays the Latency, IOPS, and Bandwidth performance metrics for the appliance.
Bandwidth details	Latency, Total Bandwidth, Read Bandwidth, Write Bandwidth	Amount of data that moved through the system within a specified period. The bandwidth metrics include average total bandwidth, average read bandwidth, and average write bandwidth. Bandwidth is calculated by multiplying the IOPS by the IO size.
IOPS details	Latency, Total IOPS, Read IOPS, Write IOPS	Number of read and write requests that the system serviced within a specified period. The IOPS metrics include average total IOPS, average read IOPS, and average write IOPS.
Latency details	Latency, Ready Latency, Write Latency	How fast the system responded to read and write requests within a specified period. The latency metrics include average total latency, average read latency, and average write latency.
CPU Utilization details	Latency, CPU Utilization	The percentage of CPU Utilization on the cores dedicated to servicing storage I/O requests (available only for Overall Performance metrics).
IO Size details	Latency, Avg. IO Size, Read IO Size, Write IO Size	Number of read and write requests' size that performed I/O operations within a specified period. The IO size metrics include average total size, average read size, and average write size.
Queue depth	Latency, Queue Depth	The number of pending IO requests.

In PowerStoreOS 2.0, node CPU stats were added to the **CPU Utilization details** category which allows you to monitor each node’s CPU utilization and latency metrics.

In PowerStoreOS 3.0 and higher, you can adjust the layout to show between one and three columns for easier viewing.

Note: Appliance performance metrics are also available over REST API.

Port IO Performance

From the **Hardware > [APPLIANCE] > Ports** card, you can view IO Performance details for Ethernet, and Fibre Channel ports by checking the chosen port and clicking the **IO Performance** button from the **More Actions** drop-down menu. From the port IO Performance page, you can view performance metric details for Host IO latency, IOPS, Bandwidth, IO Size, and Queue Depth for that specific port. The ports card also allows you to perform link aggregation, map storage networks, tag ports for replication, and compare performance metrics.

Other system status messages and settings

There are other status messages and settings in the upper-right corner of PowerStore Manager, as shown in Figure 43. Each icon provides different information to the administrator and is always available. The following sections provide more information about each icon.

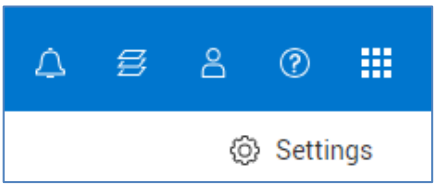

Figure 43. Other system status information and settings

CloudIQ/vCenter/metro node connection

The first icon in the top blue banner of PowerStore Manager provides quick links to **CloudIQ**, **VMware vSphere,** and **metro node,** respectively, as shown in Figure 44. To see PowerStore appliances in CloudIQ, you must configure SupportAssist and check the **Connect to CloudIQ** checkbox. Note, if a vCenter connection has not been configured in **Compute** > **vCenter Server Connection**, the quick link for **VMware vSphere** is not available. To configure a metro node connection, go to **Settings** > **Networking** > **Metro Node.**

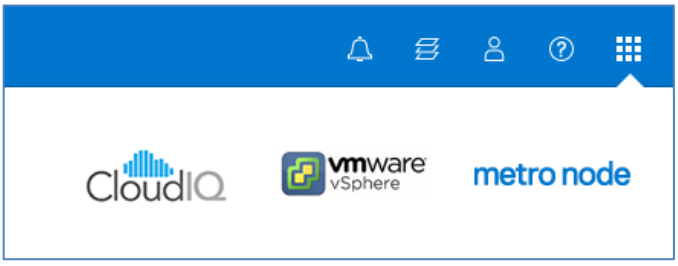

Figure 44. CloudIQ, VMware vSphere, and metro node quick links

Running jobs

To see active or recently completed jobs, click the **Jobs** (stacked squares icon) in the upper-right corner, and the window shown in Figure 45 appears. For recent and active jobs, this view also shows the percentage that is completed. When there are multiple PowerStore appliances in the cluster, the window includes a tab for **Required Actions**

which shows any assisted-migration recommendations on the system from the **Migration** > **Internal Migrations** > **Migration Actions** page. Lastly, The **View All Jobs** button takes you directly to **Monitoring** > **Jobs** for a full list of all jobs.

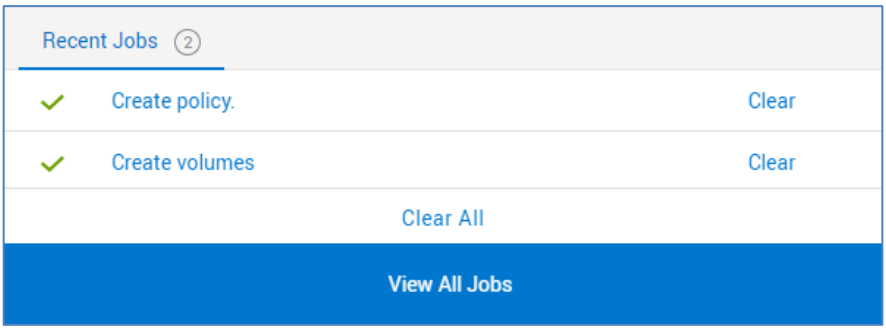

Figure 45. Jobs icon

Quick access alerts

PowerStore Manager enables you to quickly see relevant alerts on the system through the **Alerts** icon in the top menu bar (Figure 46). Links in the dialog lead to the **Alerts** page, which lists all alerts that are associated with the cluster. Here, users can get more details about the alerts and information about how to remedy the associated issues. Click an alert to go to the **Monitoring** page, with the alert automatically selected, to see more alert information and the suggested repair flow if applicable.

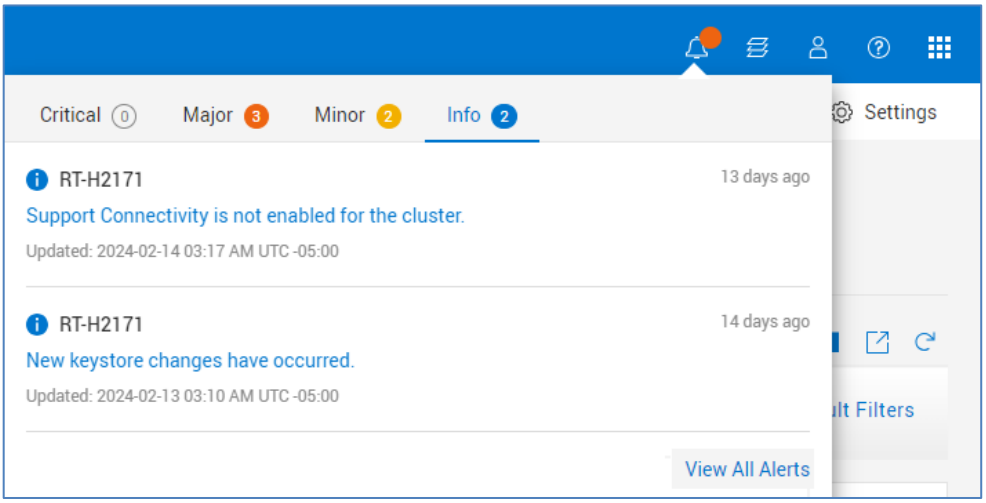

Figure 46. Quick access alerts

Logged-in user options

In the top blue banner, the Profile icon (Figure 47) includes various options including resetting user preferences, changing the password of the logged-in user, and a **Log out** option.

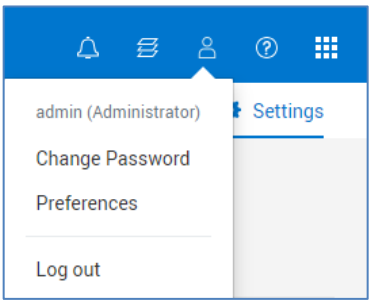

Figure 47. Logged-in user options

Online help

The next icon in the top menu bar is the context-sensitive help menu shown in Figure 47. The options for the corresponding dialog dynamically change based on the current page or wizard in PowerStore Manager. For example, if the user is on the **Volumes** page, the online help icon displays an option to go directly to online help for Volumes as shown in Figure 48. This feature helps you find the exact information to learn more about the system, instead of having to search through the various pages in the online help. The **Help** icon also provides a quick link to **Settings** > **Support** > **General Support**. It links to an **About** menu which includes the current software version, a **Gather Support Materials** button, and a **Configuration Recommendations** menu.

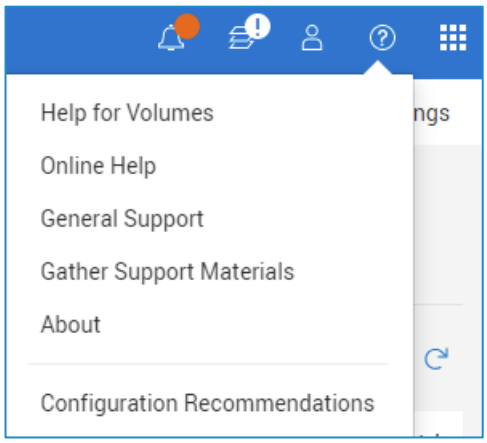

Figure 48. Online help icon

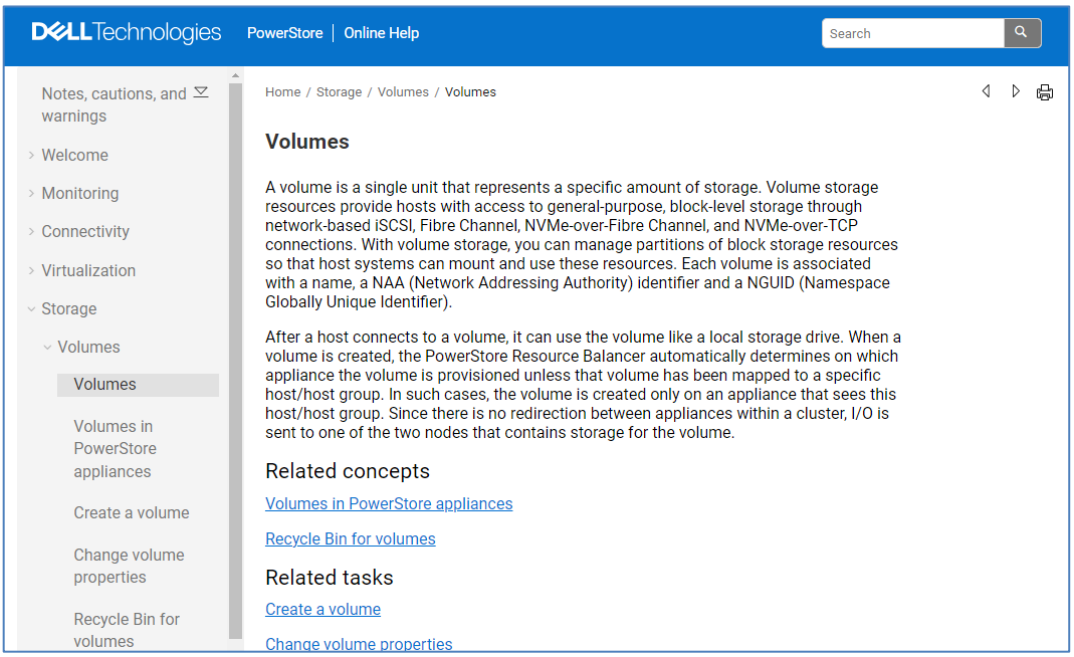

Figure 49. Online Help > Volumes

Settings menu

The **Settings** icon (gear symbol near the top menu bar) leads to the **Settings** menu. The **Settings** menu (Figure 50) enables administrators to set or configure many settings that are important to the cluster but are less frequently used. The menu lets you upgrade system software, configure support connectivity, configure infrastructure services, and enable SSH, among other actions.

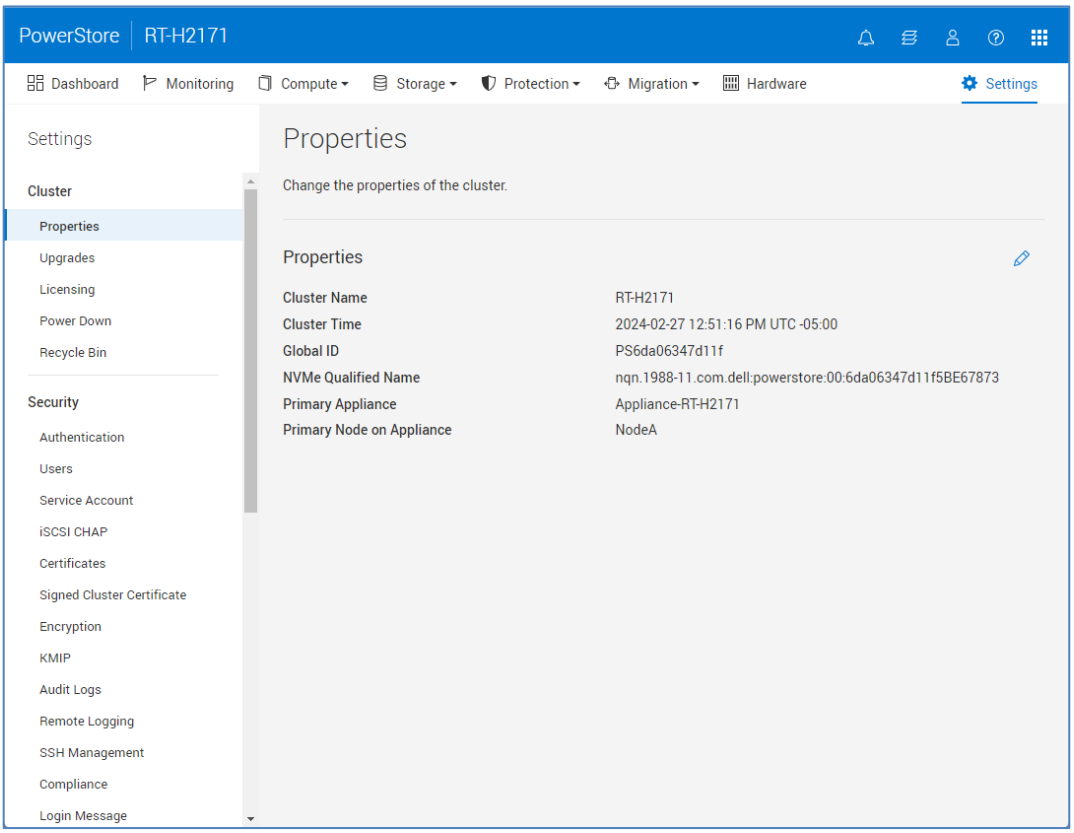

Figure 50. Settings page

The following table shows all available settings in the **Settings** menu.

Table 7. Settings menu options

Category	Settings	General description
Cluster	Properties, Upgrades, Licensing, Power Down, Recycle Bin	Update cluster-friendly name, manage system upgrades, manage system licensing, power down the system, and manage the expiration duration of the Recycle Bin.
Security	Authentication, Users, Service Account, ISCSI CHAP, Certificates, Signed Cluster Certificate, Encryption, KMIP, Audit Logs, Remote Logging, SSH Management, Compliance, Login Message, HTTP Redirect, VASA Certificate	Manage system settings related to security topics including authentication, authorization, encryption, and managing SSH access.
Networking	Cluster MTU, Network IPs, Infrastructure Services, SMTP Server, SNMP, Metro Node	Configure various system settings related to networking including system IPs, MTU size, DNS, NTP, physical switches, and metro node connection.
Support	Metric Collection Configuration, Support Connectivity, Gather Support Materials, Metrics Archives, General Support, Disable Support Notifications, Email Notifications	Configure Support Connectivity, support contacts, generate support materials for troubleshooting, and configure email addresses to which to send system alerts.

Cluster Power Down

A Power Down Cluster Wizard is available in PowerStoreOS version 4.0 and later. The wizard validates that the system is ready to be powered down, identifies any active storage objects on the system, and confirms with the administrator prior to proceeding.

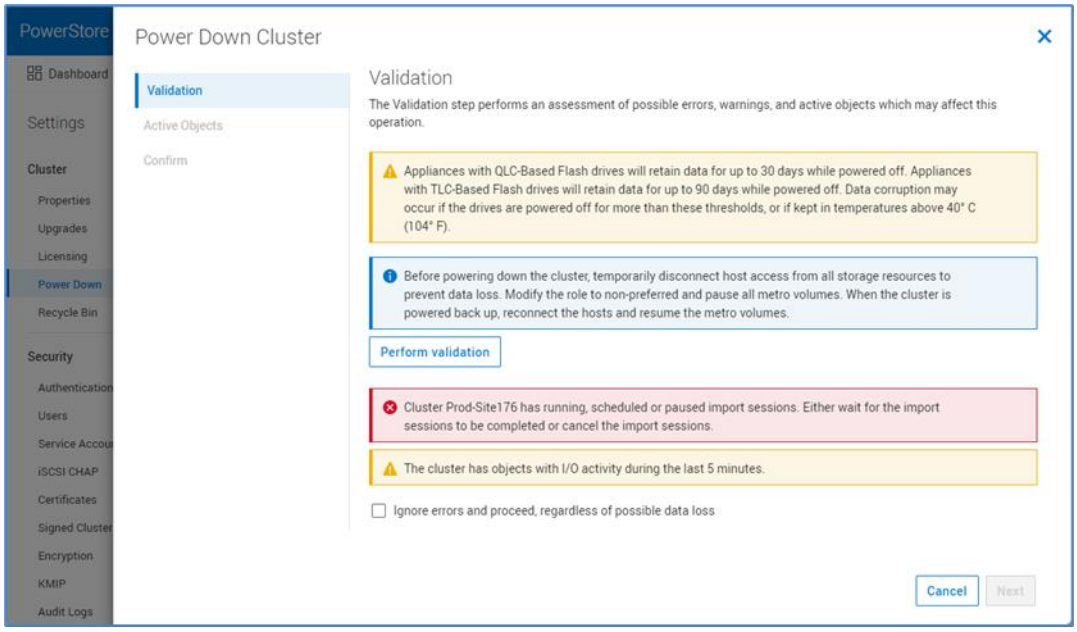

Figure 51. Settings > Power Down > Power Down Cluster

Support Connectivity

The **Settings** menu > **Support > Support Connectivity** category enables you to configure and manage Support Connectivity. The Support Connectivity feature provides an IP-based connection that enables Dell Support to receive error files and alerts from your appliance, and to perform remote troubleshooting that results in a fast and efficient time-to-resolution. Dell Technologies recommends that you enable the Support Connectivity feature to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. PowerStore offers the ability to connect directly or by using the Secure Connect Gateway. The ability to connect PowerStore to CloudIQ and enable remote support is also available to be enabled in this section. If you do not enable the Support Connectivity and remote support features, you may need to collect appliance information manually to assist Dell Support with troubleshooting and resolving problems with your appliance.

For more information about Support Connectivity and options for remote troubleshooting, see the PowerStore Security Configuration Guide.

Upgrades

From the **Settings** menu > **Cluster** > **Upgrades** page, users can manage, upload, and deploy various Non-Disruptive Upgrade (NDU) packages for the PowerStore cluster. Generally, NDU packages consist of two categories: Software Releases and Thin Packages. Software Releases are PowerStoreOS upgrades which contain the full operating system image or patch or hotfix images for a specific operating system version. Thin Packages contain a smaller and more targeted amount of functionality than regular PowerStoreOS packages. These packages may also consist of different package types

such as Disk Firmware or Health Check updates. Thin Packages are smaller in size, take less time to apply, and often do not require node reboots.

Since Health Check packages can be upgraded outside of the PowerStoreOS upgrade path, PowerStoreOS 2.1 provides users the ability to run an Upgrade Extensions System Check before a PowerStore NDU. When any PowerStore NDU package file besides a Health Check is selected with PowerStoreOS below version 3.0, the UPGRADE button is disabled (see Figure 52).

The button is enabled if the Upgrade Extensions have run within 60 minutes before and no further System Checks are performed after the Upgrade Extensions job completes. If any of these conditions are not met, a tooltip providing instructions to run Upgrade Extensions from Monitoring > System Checks is displayed as seen in Figure 52. The run Upgrade Extensions job runs any off-cycle Health Check packages that have been installed on the system. PowerStoreOS versions 3.0 and later do not require you to run the Upgrade Extensions job before running an NDU.

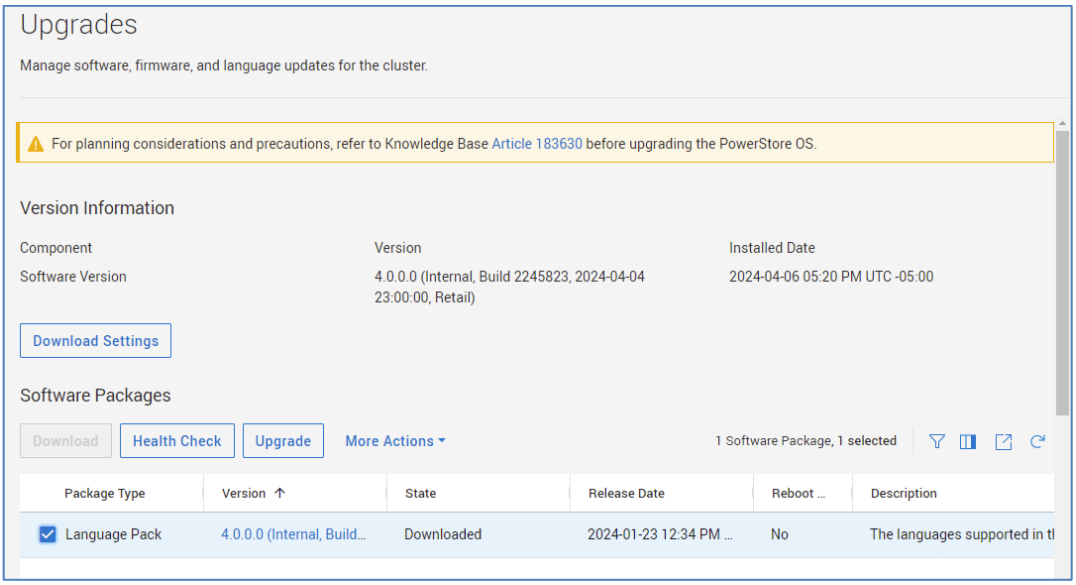

Figure 52. Upgrades

PowerStoreOS versions 3.0 and later offer the ability to automatically download software packages if support connectivity is enabled. Click on the **Download Settings** button in the Upgrades page to enable automatic download.

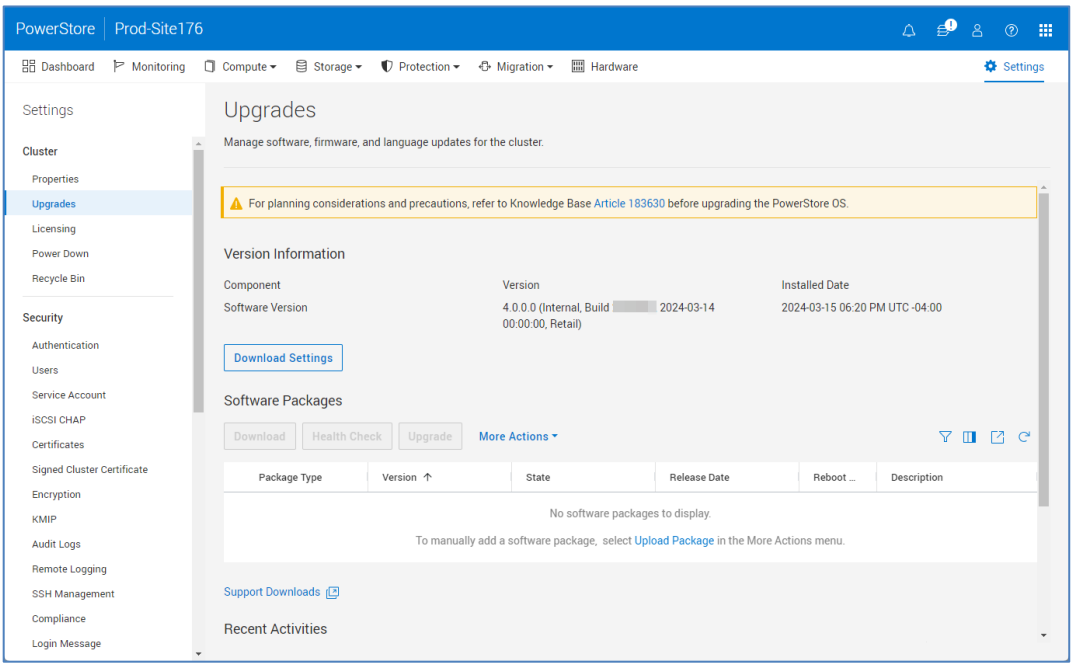

Figure 53. Automatic download

When enabling automatic download in PowerStoreOS versions 4.0 and later, users can select their **Software Release Package Preference**. Target is selected by default, which indicates the release has achieved runtime and stability requirements to make it the current target code. Latest provides the most recent software release with the latest and greatest feature set. Users with this guidance can directly download target or latest software packages to achieve specific requirements in their environment without having to download from a separate support site.

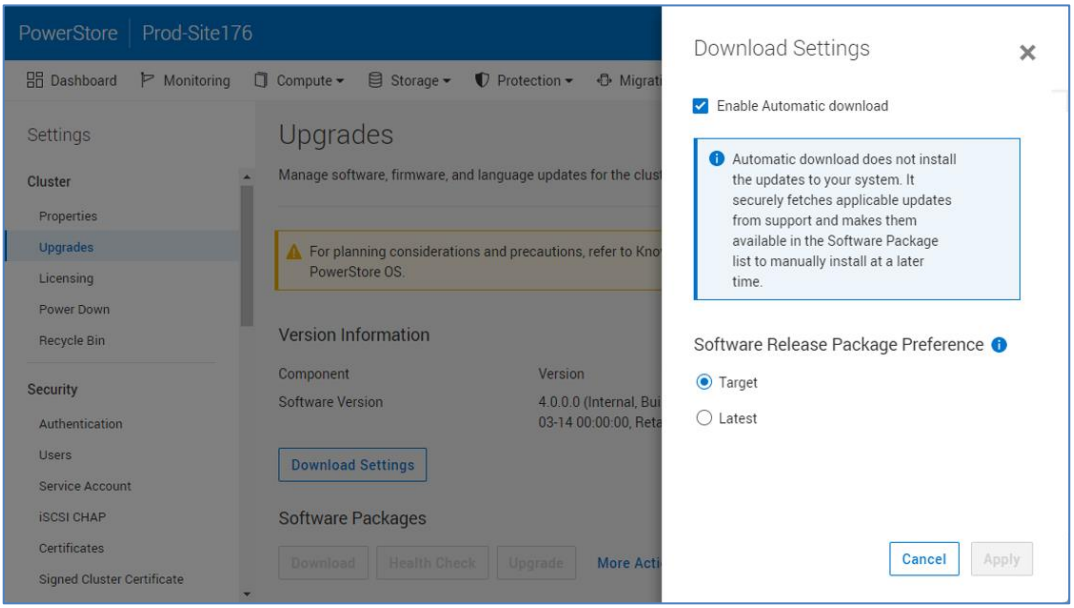

Figure 54. Download settings

Note: Users can manually check for software package updates even if automatic download is not enabled.

PowerStoreOS versions 3.0 and later supports the use of language packages within the upgrades menu of PowerStore Manager. The purpose of this feature is to adapt PowerStore to make it easier to use for users around the world. This involves translations of texts and adding specific local components for different regions. You can download language packs for supported languages from the Dell website and upload the package to PowerStore. After you complete this step, you can select your wanted language, date, and time format options from the user preferences menu item under the user icon (Figure 55).

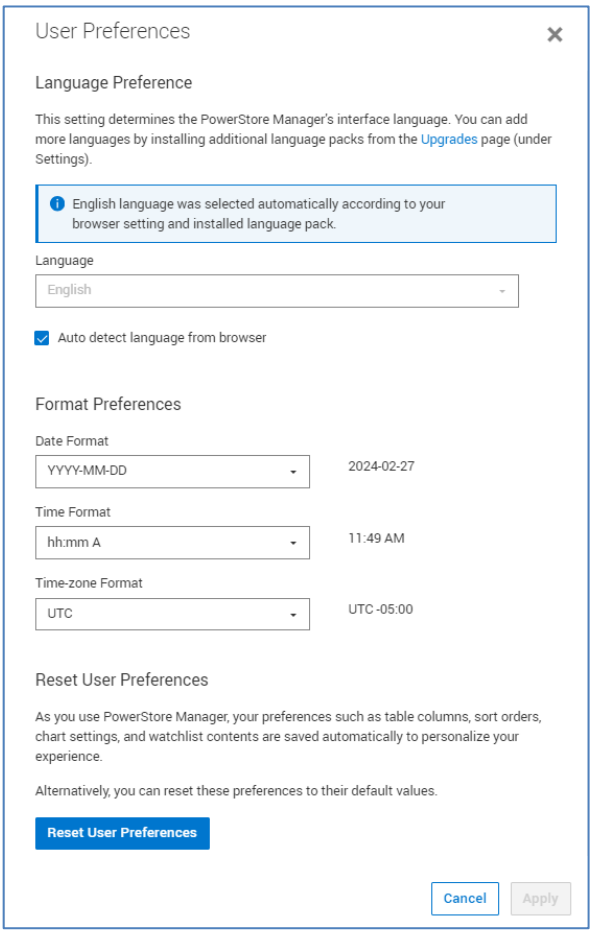

Figure 55. Language Option

Network IPs

From the **Settings** menu > **Networking** category, you can configure and manage the system's **Network IPs**. Each network consists of its own VLAN, Netmask, Gateway, and MTU size. Table 8 shows the various networks and a brief description of their function.

Table 8. Network IPs overview

Network	Function	General description
Management	Connects PowerStore cluster to management services	Connectivity to DNS, NTP, and vCenter, and enables external clients to access your cluster for management purposes

Network	Function	General description
Storage	Connects PowerStore cluster to an external storage network or creates a Storage network	Provides external clients or hosts network connectivity to the storage in your cluster
File Mobility	Connects traffic between PowerStore file clusters in replication and file import environments	Provides infrastructure needed for exchange of control traffic for file environments
Intra-cluster Management (ICM)	Internal management network	Provides continuous management connectivity between appliances within the PowerStore cluster
Intra-cluster Data (ICD)	Internal data network	Provides continuous storage connectivity between appliances within the PowerStore cluster

PowerStoreOS 2.0 added multitenancy and traffic isolation support to Storage networks. You can configure up to eight storage networks per interface, with up to a total of 256 different storage networks using IPv4 addresses, IPv6 addresses, or both in PowerStoreOS versions 4.0 and later. PowerStoreOS versions 3.0 and later added the **File Mobility** network to the Network IPs section of settings. The file mobility network is the pre-requisite infrastructure required for the exchange of control traffic between file clusters in replication and file import environments. It uses the same management network VLAN and subnet settings.

In PowerStoreOS 4.0, an enhancement to storage networks allows uses to create multiple storage networks with defined purposes. These purposes include Storage (iSCSI), Storage (NVMe/TCP), and Replication. This feature allows storage networks for host connectivity, and dedicated networks for replication. When configuring a network for replication, PowerProtect DD integration, and import, consult the Import, Protecting Your Data, and Best Practices guides for specific guidance.

User management

Besides email notification settings, the **Settings** menu > **Users** section enables you to manage local users and set up Active Directory or OpenLDAP Directory Services to authenticate users and map them to PowerStore roles. PowerStoreOS 1.0.3 and later support external user directories for authentication and authorization. Managing users in a centralized directory reduces the tasks to set up accounts on each system individually and might be a requirement to meet company rules and compliance.

Role-based access control

Role-Based Access Control (RBAC) allows for users to have different privileges, which provides a means to separate administration roles to better align with skill sets and responsibilities. To ensure an end-to-end secure environment, PowerStore systems have various roles that are assigned specific privileges to perform different tasks. These roles include, but are not limited to: Operator, VM Administrator, and Storage Admin. Dell Technologies recommends giving users the fewest privileges possible while still enabling them to meet their responsibilities. As an example, it is sufficient to give only **Operator** privileges to an account which is only responsible for monitoring instead of giving full privileges with the Administrator role. To get a more compressive list of the PowerStore

roles and privileges, see the PowerStore Security Configuration Guide at: dell.com/powerstoredocs.

Local User

By default, PowerStore has an integrated **admin** user which is assigned to the **Administrator** role to manage a PowerStore cluster. You can set up more users under **Settings** > **Users > Users** > **Local** tab. Security Administrators or Administrators can also reset a password, and lock or unlock existing users on the system.

For more information about local user management, see the PowerStore Security Configuration Guide at: dell.com/powerstoredocs.

Active Directory/OpenLDAP: Overview

The Active Directory/OpenLDAP feature requires PowerStoreOS 1.0.3 or later. You can manage the directory server settings in **Settings** > **Security > Authentication** . To individually map AD/LDAP users or groups to a role in PowerStore, go to **Settings** > **Security> Users** > **LDAP** tab. PowerStore supports one instance of a directory connection with one or multiple servers for redundancy.

The directory structure of Active Directory and OpenLDAP is similar, but the implementation of each directory server may use a different naming scheme and structure. A directory service is based on a hierarchical database that is referenced as a tree. Some implementations may represent the geographical structure of an organization, and other implementations show the organizational structure. Like a tree, the structure starts with a root which usually represents domain components (DC) of a computer network or organization and splits into multiple branches. Each branch starts with a structural object-like organizational unit (OU) or common name (CN). The tree can continue with more branches or end in leaf objects. Leaf objects can stand for individual items like a user, a group, or a computer. Within the tree, each leaf object is identified by a concatenated string of individual elements that are separated by commas and is called a distinguished name (DN). Each DN is unique in a directory. For example, a user and group can have the same leaf name, but the path to the object makes the leaf instance a unique DN. To find the right leaf object for a user or group that is used for authentication, you can limit a lookup to certain parts of the tree by using a search path. A search path is useful when the directory represents a company structure, when using a filter for attributes, or when using a combination of both.

Figure 56 shows the LDAP structure which is used for the following examples.

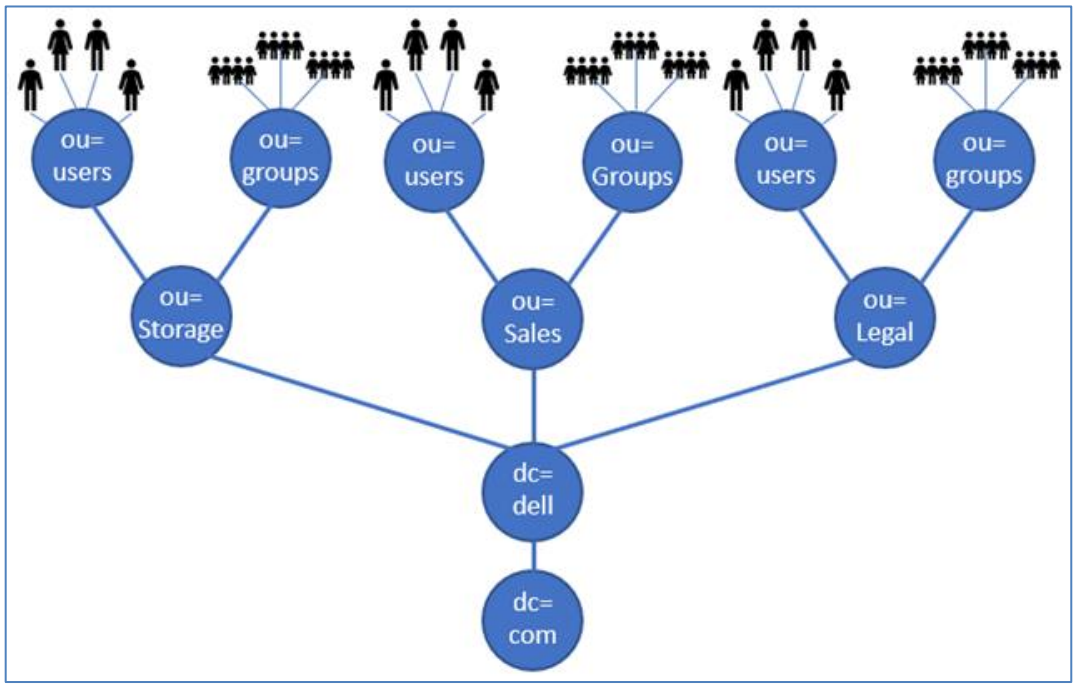

Figure 56. LDAP tree example

An example of a user object in a directory structured by the organization may look like this:

```
dn: cn=PowerStore User, ou=users, ou=Storage, dc=dell, dc=com
cn: PowerStore User
objectClass: person
sn: PowerStore
uid: pstuser
uidNumber: 1234
home: /home/pstuser
```

In this example, if the PowerStore users are only in the storage department, a good choice for the user search path would be: **ou=users, ou=storage, dc=dell, dc=com.** In the example, more information is used to narrow down the type of the object with a filter where objectClass is **person**.

The structure of groups is similar to users. The group might be as follows:

```
dn: cn=PowerStore Users, ou=groups, ou=Storage, dc=dell, dc=com
objectClass: Group
cn: PowerStore Users
member: cn=Powerstore User A, ou=users, ou=Storage, dc=dell,
dc=com
member: cn=Powerstore User B, ou=users, ou=Storage, dc=dell,
dc=com
member: cn=Powerstore User C, ou=users, ou=Storage, dc=dell,
dc=com
```

Similar to the user object above, it is possible in that structure to limit the lookup only to the branch: **ou=groups, ou=storage, dc=dell, dc=com**, and filter for the objectClass

Group to search for a group. The group example shows member attributes containing the distinguished name of each individual user. Other implementations may use the **memberUid** attribute where only the user UID is listed. In that case, the directory must ensure that UIDs are unique.

For security reasons, anonymous lookups are not allowed by the LDAP administrator, and an authentication against the directory server is required beforehand. PowerStore uses **Bind DN** and **Bind DN Password** to establish the directory server connection for initial lookups and role mapping.

To set up AD/LDAP authentication, request the following information from the directory administrator for PowerStore if not already known:

- Type of the directory: **Active Directory** or **OpenLDAP**
- **IP Address** of at least one directory server
- When **SSL** is used, the signing **CA cert** file must be uploaded to PowerStore

Note: When enabling SSL, it is mandatory that the server IP is configured as subjectAlternateName (SAN) in the directory server certificate.

- Domain name
- Bind DN and password
- Advanced configuration information:
- **ID Attribute**, which is usually samAccountName or uid
- **User objectClass** like a user or person
- **User search path**
- Group **member attribute**, which is usually a member or memberUid
- The mapped **ID attribute** to the group where **cn** is the default for PowerStore
- **Group objectClass**, which could be group or **groupOfNames**
- Group search path
- Number of Search levels for subtree- or nested search

AD/LDAP: Directory connection

You can set up an AD or OpenLDAP server connection in PowerStore Manager > **Settings** > **Users** > **Directory services**. When you select the **Server Type** in PowerStore Manager, the advanced settings use common default settings for the selected type. When the default values do not match your environment, you can change them accordingly. When a directory server connection is set up, PowerStore provides a **Verify connection** button to check if PowerStore Manager can access the directory server.

AD/LDAP: User to role mapping

After a directory connection is established, you can start mapping individual users or groups to a role in PowerStore. To perform this task, click **Settings** > **Users** > **Users in LDAP** tab. When you start to set up a mapping, PowerStore Manager requests the mapping type of **User** or **Group**, the **Domain**, and the **Account Name** that is used in AD/LDAP. The role is located in the drop-down menu for **Account Role**. This role selects

one of the PowerStore roles mapped to the AD/LDAP object after applying the **Add Account** dialog. When PowerStore is not able to look up the given **Account Name**, the system cannot look up the given name with the **ID attribute** as given in the directory connection configuration. The error message **Account does not exist in LDAP server!** appears in PowerStore Manager and requires a validation of the current configuration. For remediation, you must check if the Account Name matches with a corresponding user object or group object in AD/LDAP. It is also possible that a wrong attribute setting for **Directory Service** prevents the lookup.

Login Message

A **Login Message** provides the ability for storage administrators to create, enable, and disable a customizable login message starting in PowerStoreOS 2.1. The Login Message is displayed whenever you go to the PowerStore Manager login page from your browser. You can use Login Messages for a wide variety of use cases, such as informing you what system you are logged into or even provide a security warning. You can easily configure the Login message from PowerStore Manager through **Settings** > **Security** > **Login Message.** Here, you can enable the message, enter your text up to 2000 characters, and click the **Apply** button (Figure 57). After you enable the message, it is seen by all users from the PowerStore Manager login page as shown in Figure 58. You can also enable and configure Login Messages through REST API and PowerStore CLI. Only the Storage Administrator or Security Administrator roles can edit, enable, and disable Login Messages.

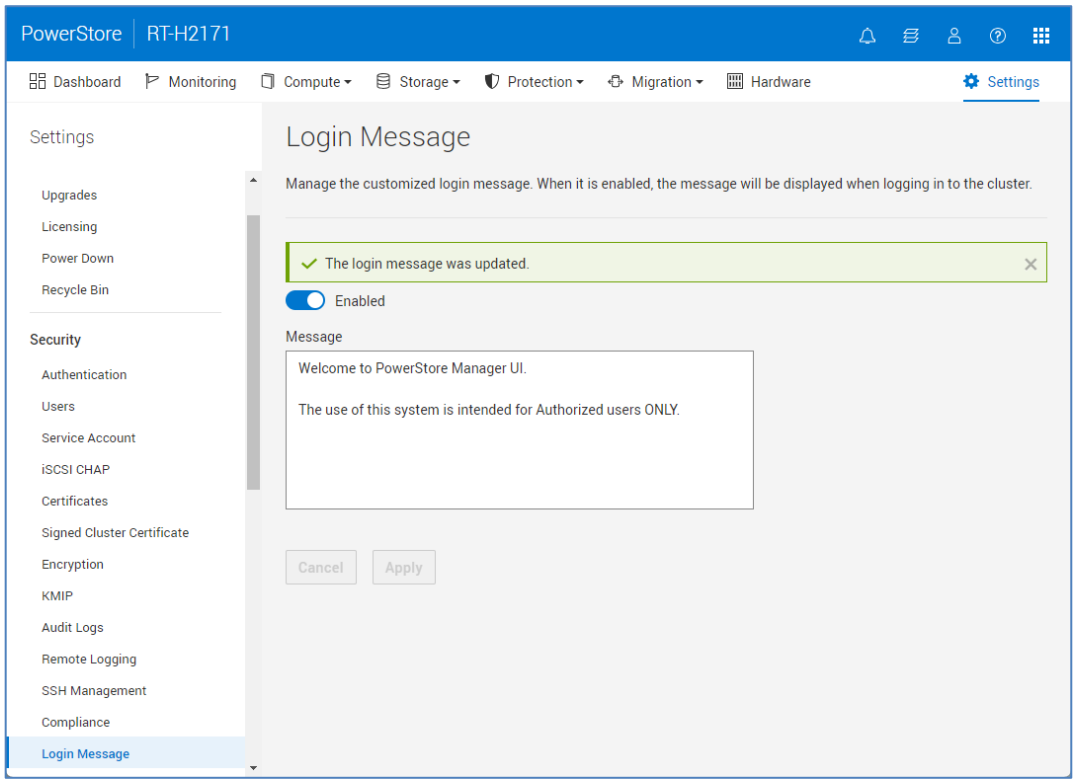

Figure 57. Settings > Security > Login Message

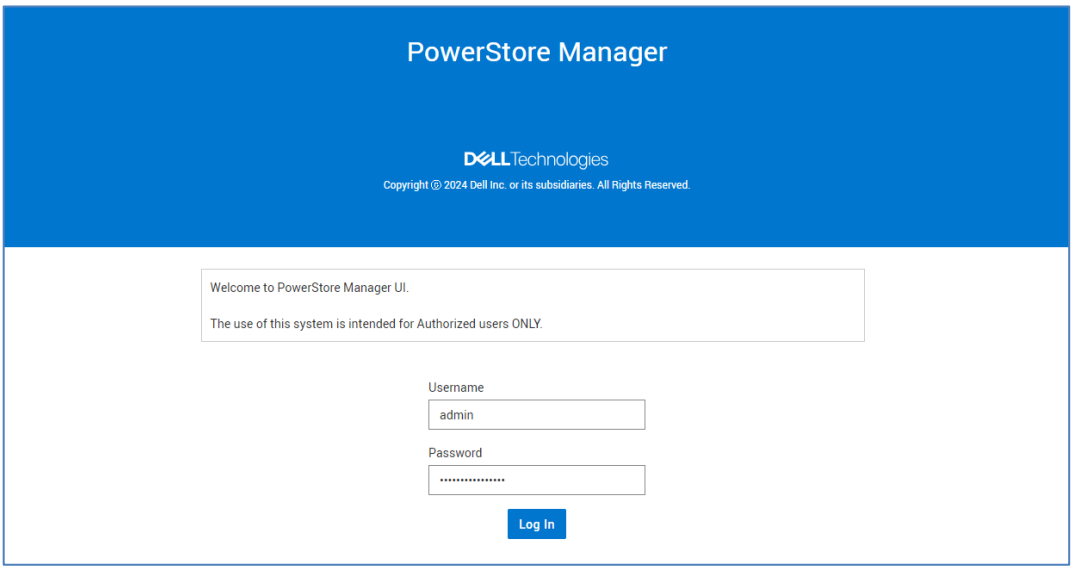

Figure 58. PowerStore Manager Login page with Login Message enabled

PowerStore CLI

Overview

For IT generalists, managing PowerStore systems through the PowerStore Manager interface is comprehensive enough to accomplish all daily administrative tasks. For advanced use cases, the PowerStore CLI (PSTCLI) interface enables users to create scripts to automate routine tasks. You can use the PSTCLI to perform the same tasks that can be performed in PowerStore Manager. These tasks include configuring and managing storage resources, protecting data, managing users, viewing performance metrics, and other similar tasks.

For more information about using the PSTCLI, see the *PowerStore Command Line Interface User Guide* and *PowerStore CLI Reference Guide* at dell.com/powerstoredocs.

PowerStore REST API

Overview

The REST API is an application programming interface that uses familiar HTTP operations like GET, PATCH, POST, and DELETE. The REST architecture includes certain constraints that ensure that different implementations of REST conform to the same guiding principles. This architecture gives developers ease of application development when working with different REST API deployments. REST APIs have become more popular and more widely used in data centers where administrators are looking to standardize their management needs across all their appliances, regardless of vendor.

The PowerStore platform includes REST API support, which provides another way to manage PowerStore appliances and automate various tasks. Generally, the PowerStore REST API has the same capabilities as PowerStore Manager. The PowerStore REST API formats all communications in JSON notation. Users can send REST API requests using their favorite scripting languages, such as Perl and PHP, to manage PowerStore systems

in their environment. This ability provides flexible management and enables more complexity with scripted operations.

After a system is up and running, users can go to the following web addresses to gain access to the REST API reference commands (**<Management_IP>** is the management IP of your PowerStore cluster):

https://<Management_IP>/swaggerui

This online REST API command reference location allows users to test REST API commands on their live system which can be incorporated into other scripts.

For more information about using REST API for PowerStore appliances, see the *REST API Developers Guide* and *PowerStore REST API Reference Guide* at dell.com/powerstoredocs.

Conclusion

Overview

PowerStore Manager realizes a core design goal of PowerStore—to simplify storage management. Using a modern HTML5 architecture and an easy-to-navigate user interface, PowerStore Manager ensures a quality experience for storage administrators while using best practices for storage-management requirements. PowerStore Manager provides an intuitive interface that does not require extensive or specialized knowledge. From simple tasks like provisioning a block volume, to using advanced features like local and remote replication, PowerStore Manager is a powerful tool that enables users to realize the potential of their PowerStore systems. For users that prefer command-line tools, PowerStore also supports a fully functional CLI and REST API which are useful for scripting use cases and enable more complex operation possibilities.

References

Dell Technologies documentation

The Dell Technologies Info Hub > Storage site provides expertise that helps to ensure customer success with Dell storage platforms.

Dell.com/powerstoredocs provides detailed documentation about how to install, configure, and manage PowerStore systems.