

Dell PowerStore: Cybersecurity

May 2024

H19084.4

White Paper

Abstract

This document provides an overview of cybersecurity-related features and solutions for Dell PowerStore.

Copyright

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2022– 2024 Dell Inc. or its subsidiaries. All Rights Reserved. Published in the USA May 2024 H19084.4.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Executive summary.....4

Cyber essentials by Dell Technologies6

Authentication and access6

Data security.....11

Communications security.....14

Auditing17

Federal compliance.....17

CloudIQ Error! Bookmark not defined.

References.....21

Executive summary

Overview

Cybersecurity is a growing priority for organizations. With growing concerns, demands, and regulations, the need to address the evolving security requirements is vital. Attackers continue to find new creative techniques to infiltrate IT infrastructures to penetrate existing security measures. In addition to external threats, there is also the potential of internal threats from disgruntled or compromised employees or contractors. These threats to organizations have negative economic consequences:

- A ransomware attack occurred every 11 seconds in 2021.¹
- 84% of IT leaders report that data loss prevention is more challenging with a remote workforce.²
- More than 60% of companies have experienced a data compromise due to an exploited vulnerability.³
- The average cost of a cybercrime for an organization is \$13 million USD.⁴
- The total global impact of cybercrime is 8 trillion USD.⁵

In addition to immediate economic consequences, loss of organizational reputation may be even more damaging because its impact can extend over many years. The cost of a data breach can have immediate and lasting effects for organizations of all sizes and across all industries. Dell takes a comprehensive approach to cyber resiliency with a framework that helps organizations achieve their security objectives and requirements. The Dell cybersecurity framework aligns with the National Institute of Standards and Technologies (NIST) Cybersecurity framework and consists of the following functions:

- Identify
- Protect
- Detect
- Respond
- Recover

¹ Estimated for 2021, Cybersecurity Ventures: <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>.

² Tessian, [The State of DLP - Why DLP Has Failed and What the Future Looks Like](#), May 2020.

³ Forrester Consulting Thought Leadership Paper Commissioned by Dell, [BIOS Security – The Next Frontier for Endpoint Protection](#), June 2019.

⁴ Accenture Insights, Ninth Annual Cost of Cybercrime Study March 2019 <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>.

⁵ USAID, [Cybersecurity Briefer: Economic Growth and Trade](#), October 2023.

This paper discusses data services and solutions that are related to Dell PowerStore that safeguard sensitive and mission-critical data. It is divided into the following five sections: Authentication and Access, Data Security, Communications Security, Auditing, and APEX AIOps Infrastructure Observability .

Revisions

Date	Part number/ revision	Description
February 2022	H19084	Initial release
July 2022	H19084.1	Updated for PowerStoreOS 3.0 features
August 2022	H19084.2	Updated with CEPA support, FLR, and HWRoT
May 2023	H19084.3	Updated for PowerStoreOS 3.5 features: <ul style="list-style-type: none"> • Multi-Factor Authentication through RSA SecurID • Secure snapshot feature • Third-party certificate support for VASA • STIG mode support for federal compliance
May 2024	H19084.4	Updated for PowerStoreOS 4.0 features: <ul style="list-style-type: none"> • VMware vCenter Certificate • APEX AIOps Infrastructure Observability Health Score in PowerStore Manager • Approved Product List (APL) certification

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: Derek Barboza, Andrew Sirpis, Subomi Gbotosho

Note: For links to other documentation on this topic, see the [PowerStore Info Hub](#).

Cyber essentials by Dell Technologies

Overview

Dell Technologies follows a shift-left approach to security that ensures that security is baked into every process in the development life cycle. The Dell Secure Development Lifecycle (SDL) defines security controls that are based on industry standards that Dell product teams adopt while developing new features and functionality. The Dell SDL includes both analysis activities and prescriptive proactive controls around key risk areas.

Dell Technologies strives to help customers minimize the risk associated with security vulnerabilities in our products. Our goal is to provide customers with timely information, guidance, and mitigation options to address vulnerabilities. The Dell Product Security Incident Response Team (Dell PSIRT) is chartered and responsible for coordinating the response and disclosure for all product vulnerabilities that are reported to Dell Technologies. We employ a rigorous process to continually evaluate and improve our vulnerability response practices and regularly benchmark these responses against the rest of the industry. Dell Technologies has an ingrained culture of security.

Dell Technologies solutions for PowerStore are providing modern data protection around cyber data protection and resiliency.

For more information about each topic, see [References](#).

Authentication and access

HWRoT

The PowerStore 500, 1200, 3200, 5200, and 9200 models are based on the new Intel CPU chipsets that provide Hardware Root of Trust (HWRoT). HWRoT provides an immutable, silicon-based Root of Trust to cryptographically attest to the integrity of the BIOS and firmware, and it ensures that there have been no malicious modifications throughout the supply chain or after installation. These PowerStore models provide the following security features for firmware images and the operating system through the Secure Boot and x86 Secure Boot technologies that are provided through the enclosure management software on the system:

- Authentication and root of trust, which provide the capability to authenticate boot loader and firmware
- Verified and measured boot
- Authentication of firmware images and operating system boot loader at boot time
- Digitally signed firmware upgrades to ensure that root of trust authenticates all signed upgrade firmware images

RBAC

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 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 Dell PowerStore Security Configuration Guide at: dell.com/powerstoredocs.

Lightweight Directory Access Protocol (LDAP)

Authentication to PowerStore Manager can be performed either locally or using LDAP. Configuring authentication using LDAP allows for central management of authentication to PowerStore Manager, REST API, or CLI. The PowerStore Manager roles can be assigned to LDAP users or groups to manage the level of authorization that a user or group will have in administering the storage system. For more information, see the [Dell PowerStore Manager Overview white paper](#) and the [Dell PowerStore Security Configuration Guide](https://dell.com/powerstoredocs) at: dell.com/powerstoredocs.

Multi-Factor Authentication through RSA SecurID

PowerStoreOS 3.5 and later allows users to implement Multi-Factor Authentication (MFA) through RSA SecurID. MFA, which is also known as advanced or two-factor authentication, provides an additional layer of security when logging in or performing transactions on the PowerStore system. MFA provides many advantages including: increasing the security of accounts and data against hackers, mitigating the risk of poor password practices, and helping users stay compliant with regulations. It can be used with both local and LDAP user accounts for PowerStore.

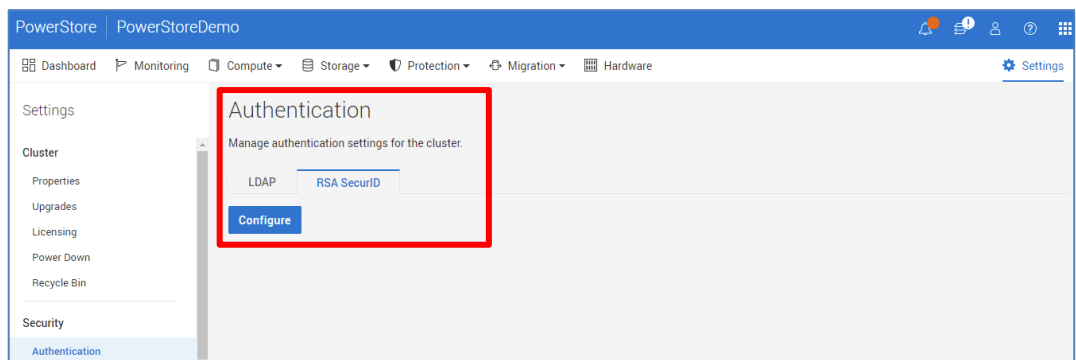


Figure 1. SecurID configuration

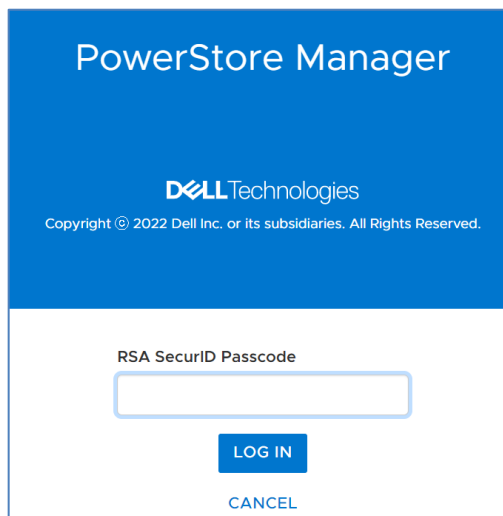


Figure 2. RSA SecurID passcode prompt

SSH

Each appliance can optionally enable external SSH access to the SSH port of the appliance IP address, which takes the user to the service feature on the primary node of an appliance. The appliance IP address floats between the two nodes of the appliance as the primary designation changes. If external SSH is disabled, SSH access is disallowed. When an appliance first comes up and is not configured, SSH is enabled by default so that the appliance can be serviced if issues are encountered before it is added to a cluster. When a new cluster is created or for a join cluster operation, all appliances have SSH initially set to a disabled status.

Network File System (NFS)

PowerStore supports NFSv3 through NFSv4.1. Secure NFS uses Kerberos to secure data transmissions through user authentication and data signing through encryption. Kerberos provides integrity (signing) and privacy (encryption). Integrity and privacy are not required to be enabled: they are NFS mount options.

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

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

With NFS secure, encryption is supported using the Advanced Encryption Standard (AES). Both AES128 and AES256 encryption in Kerberos is supported. Along with secure NFS, this also impacts Server Message Block (SMB) and LDAP. These encryptions are now supported by default by Windows and Linux. Although these new encryption methods are more secure, it is up to the client whether they are used. From that User Principal Name (UPN), the server builds the credential of that user by querying the active UNIX Directory Service (UDS). Since Networked Information Service (NIS) is not secure, it is not recommended to use it with secure NFS. We recommend using Kerberos with LDAP or LDAP over SSL (LDAPS).

Secure NFS can be configured through PowerStore Manager. For more information, see the [Dell PowerStore: File Capabilities white paper](#).

File Level Retention

File Level Retention (FLR), also known as Write-Once, Read-Many (WORM), is available starting with PowerStoreOS 3.0. FLR prevents modification or deletion of locked files until a specific retention date. PowerStore supports both FLR Enterprise (FLR-E) and FLR Compliance (FLR-C) modes, which enable different degrees of file locking controls. FLR-C is designed for companies that need to comply with federal regulations and meets the requirements of SEC Rule 17a-4(f). For more information, see the [Dell PowerStore: File Capabilities white paper](#).

CHAP

Challenge Handshake Authentication Protocol (CHAP) is a method of authenticating iSCSI initiators (hosts) and targets (volumes and snapshots). CHAP exposes iSCSI storage and ensures a secure standard storage protocol. Authentication depends on a

secret, similar to a password, that is known to both the authenticator and the peer. There are two variants of CHAP protocol:

- Single CHAP authentication allows for the iSCSI target to authenticate the initiator. When an initiator tries to connect to a target (Normal mode or through Discovery mode), it provides a username and password to the target.
- Mutual CHAP allows for the iSCSI target and the initiator to authenticate each other. The iSCSI initiator authenticates each iSCSI target that the group presents. When an initiator tries to connect to a target, the target provides a username and password to the initiator. The initiator compares the supplied username and password to information that it holds. If they match, the initiator can connect to the target.

CHAP is disabled by default. The user can enable it on the CHAP settings page in PowerStore Manager or through the REST API.

Banner

Starting in PowerStoreOS 2.1, storage administrators can create a customizable login banner. The message appears when users access the PowerStore Manager login page. It can be used to set a security warning for users.

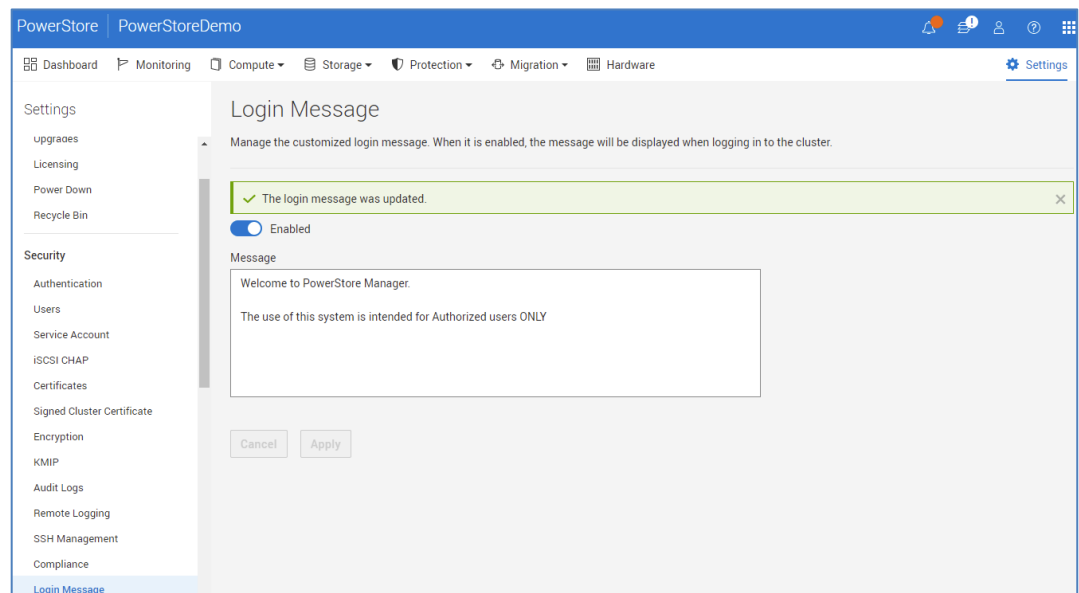


Figure 3. Login banner configuration

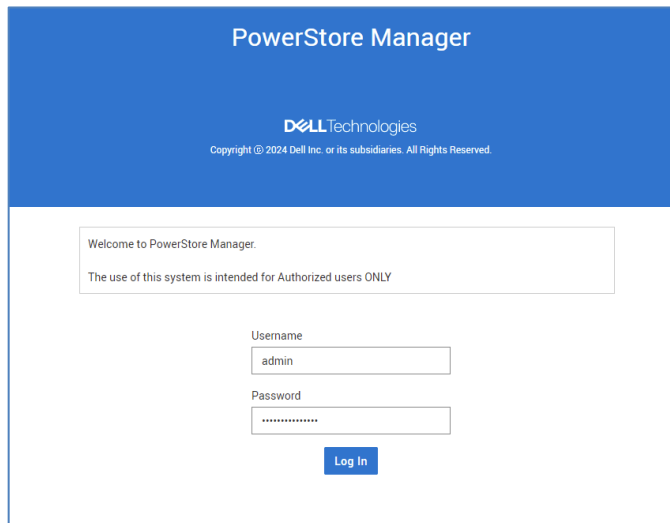


Figure 4. Example of login banner

HTTP Redirect

With PowerStoreOS 3.0, users can be automatically redirected from http to https when browsing to PowerStore Manager. Users can turn this feature on or off from PowerStore Manager and from the Initial Configuration Wizard (ICW). For more information, see the [Dell PowerStore Manager Overview white paper](#).

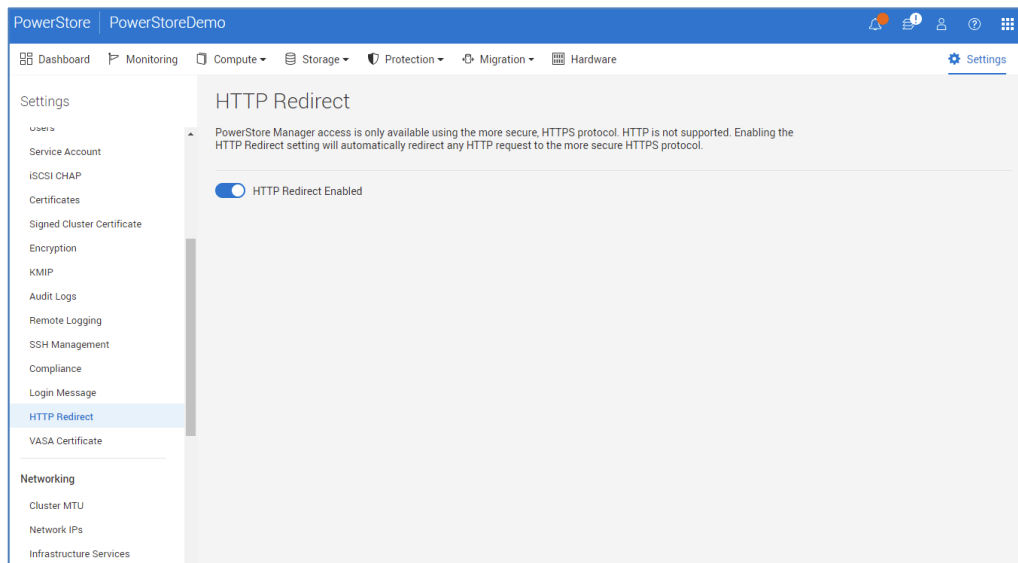


Figure 5. HTTP Redirect

CEPA

The Common Event Publishing Agent (CEPA) is supported starting with PowerStoreOS 3.0. CEPA delivers SMB and NFS file and directory event notifications to a server, allowing third-party applications to take event-driven actions on PowerStore. These actions can be used to detect ransomware, manage user access, configure quotas, and provide storage analytics. Event data monitoring also helps customers recover quickly from ransomware attacks by identifying how far back to restore their storage. CEPA provides integration points for leading monitoring vendors such as Varonis, Stealthbits, DefendX, and ProLion. For more information, see the [Dell PowerStore: File Capabilities](#)

[white paper](#) and the [Dell PowerStore Security Configuration Guide](#). For information about configuring CEPA, see *Configuring SMB* and *Configuring NFS* on [Dell.com/powerstoredocs](https://dell.com/powerstoredocs).

Data security

D@RE

Data at Rest Encryption (D@RE) in PowerStore uses FIPS 140-2 validated Self-Encrypting Drives (SEDs) by respective drive vendors for primary storage (NVMe SSD, NVMe SCM, and SAS SSD). Starting with PowerStoreOS 2.1, the PowerStore 500 model is fully FIPS 140-2 compliant. Starting with PowerStoreOS 3.0, all newly shipped models above PowerStore 500 are also FIPS 140-2 compliant. For existing systems that are upgraded to PowerStoreOS 3.0, a procedure to upgrade the system to be FIPS 140-2 compliant is available.

Encryption is performed within each drive before the data is written to the media. This protects the data on the drive against theft or loss and attempts to read the drive directly by physically deconstructing the drive. The encryption also provides a means to erase information quickly and securely on a drive to ensure that the information is not recoverable.

Reading encrypted data requires the authentication key for the SED to unlock the drive. Only authenticated SEDs are unlocked and accessible. Once the drive is unlocked, the SED decrypts the encrypted data back to its original form. The lockbox keeps the keys to each drive in the appliance, which are each encrypted to keep sensitive data safe. We recommend that you download the generated keystore archive file to an external, secure location. The PowerStore appliance must contain all SEDs.

PowerStoreOS 3.0 supports the usage of external key management applications using the Key Management Interoperability Protocol (KMIP). External key managers for storage arrays provide extra protection in the event the array is stolen. If the external key server is not present to provide the relevant Key Encryption Key (KEK), the storage system cannot be powered on.

For more information, see the [Dell PowerStore Security Configuration Guide](#).

Snapshots

Snapshots provide a simple and effective method for protecting local data. Snapshots provide immutable point in time copies of data and the ability to instantly recover if there is data corruption or deletion. Because PowerStore snapshots are 100% read-only and cannot be modified or manipulated, they are ideal for recovering instantly from ransomware attacks.

Snapshot rules can be created as part of a protection policy to define a schedule for snapshot creation, access, and retention. Only users with an Administrator or Storage Administrator role can administer snapshot policies. When used with Dell AppSync, application-consistent snapshots can automatically be created and scheduled.

PowerStore

Dashboard

Protection

Protection Policies

Snapshot Rules

Replication Rule

Remote Backup

Create Protection Policy

Policy Properties

Name

Platinum Policy

Description - optional

Snapshot Rules

+ Create

2 Snapshot Rules

<input type="checkbox"/>	Name	Days	Frequency/Start Time	Retention	Policies	File Snapshot Access Type
<input type="checkbox"/>	SnapshotRule1	Monday, Tuesday, Wed...	3 hours	36 hours	1	Protocol (Read-Only)
<input type="checkbox"/>	SnapshotRule2	Monday, Tuesday, Wed...	24 hours	8 days	2	Protocol (Read-Only)

Cancel

Create

Figure 6. Create a protection policy in PowerStore Manager

For more information, see the following white papers: [Dell PowerStore: Snapshots and Thin Clones](#) and [Dell PowerStore: AppSync](#).

Secure snapshots

Starting in PowerStoreOS 3.5, an optional secure snapshot setting provides additional protection for snapshots, volumes, and volume groups. When the secure snapshot setting is enabled, the snapshot and its parent resource are protected from deletion until the retention period expires on all secure snapshots. This provides a cost-effective line of defense against ransom attacks and accidental deletion of snapshots, volumes, or volume groups.

Create Snapshot of Volume

Storage Resource

Snapshot Properties

Name

2023-03-02 10:32:14 AM UTC -05:00

Description (Optional)

Local Retention Policy

☐ No Automatic Deletion
☒ Retain until

2023-03-09 10:32 AM

☐ Secure Snapshot

Secure snapshots are snapshots that prevent accidental or intentional deletion of snapshots. Secure snapshots cannot be manually deleted while the retention period is in effect. [Learn more](#)

CANCEL

CREATE SNAPSHOT

Create Snapshot of Volume Group

Sales-VG

Snapshot Properties

Name

2023-03-02 10:34:21 AM UTC -05:00

Description (Optional)

Local Retention Policy

☐ No Automatic Deletion
☒ Retain until

2023-03-09 10:34 AM

☐ Secure Snapshot

Secure snapshots are snapshots that prevent accidental or intentional deletion of snapshots. Secure snapshots cannot be manually deleted while the retention period is in effect. [Learn more](#)

CANCEL

CREATE SNAPSHOT

Figure 7. Create Snapshot windows—volume and volume group examples

Cyber Recovery

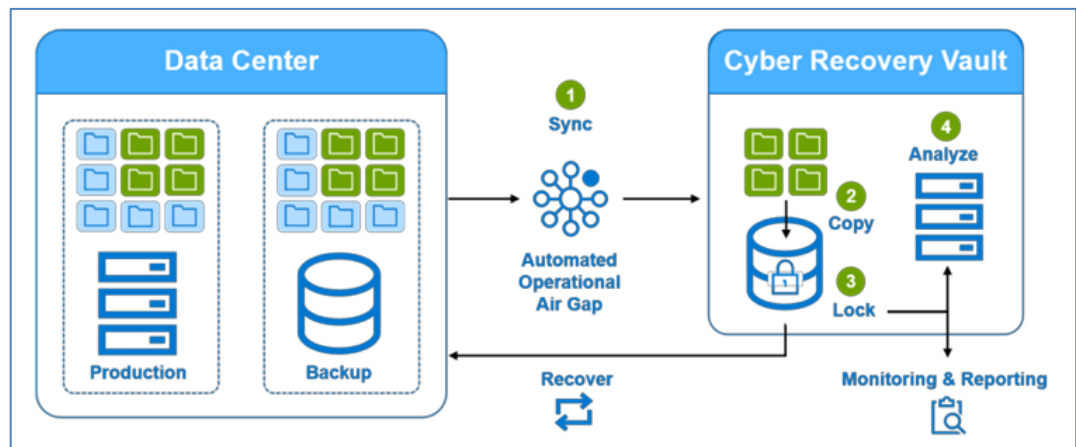


Figure 8. PowerProtect Cyber Recovery solution

Dell PowerProtect Cyber Recovery with CyberSense analytics offers a data protection solution that isolates business-critical data away from attack surfaces, using an automated operational air gap. Critical data is stored immutably in a hardened vault enabling recovery with assured data availability, integrity, and confidentiality. Fully integrated with CyberSense, the solution uses machine learning to identify suspicious activity and allows users to recover known good data and resume normal business operations with confidence. For more information, see the [Dell PowerProtect Cyber Recovery Solution Brief](#).

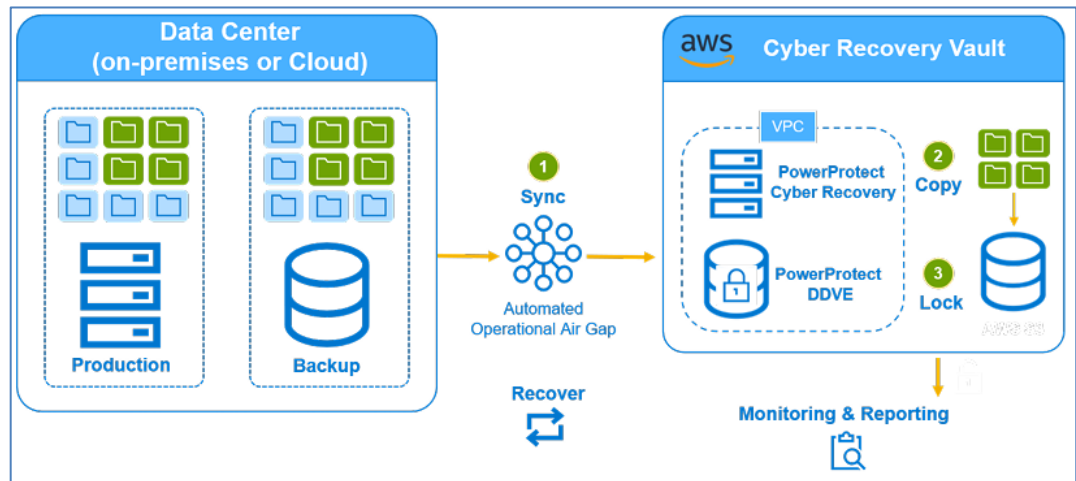


Figure 9. PowerProtect Cyber Recovery solution for AWS

The Dell PowerProtect Cyber Recovery solution supports integration with an AWS vaulting solution for protecting critical data to the cloud. The air-gapped cyber-recovery vault securely isolates data within AWS, improving cyber resiliency and reducing the impact of cyberattacks. For more information, see the [Dell PowerProtect Cyber Recovery for AWS Solution Brief](#).

Communications security

TLS

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

Cluster communications

Communications between PowerStore appliances in a cluster are secure. During cluster creation, the primary node of the cluster primary appliance creates a certificate authority (CA) certificate, also known as the cluster CA. The primary appliance passes the cluster CA certificate to the appliances joining the cluster. Each PowerStore appliance in a cluster generates its own unique Internet Protocol Security (IPsec) certificate that is signed by the cluster CA certificate. The sensitive data that PowerStore appliances transmit over their cluster network is protected by IPsec and TLS so that the security and integrity of the data is preserved.

Replication and data import

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

- Retrieving and validating a server certificate during TLS handshake
- Adding the trusted CA certificate from the remote system to the credential store

- Adding the trusted server/client certificate to the credential store
- Helping to establish secure connections when the trust is established

PowerStore supports the following certificate management functionality:

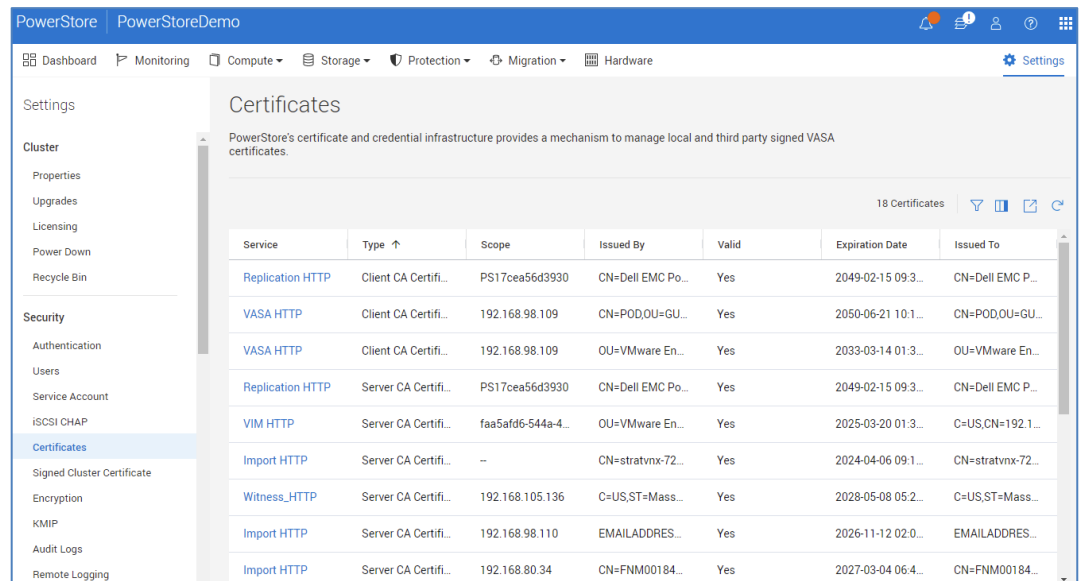
- For replication, a certificate exchange between two PowerStore clusters to establish trusted management communication. To facilitate replication between PowerStore clusters, bi-directional trust must be established between the clusters to allow for mutual TLS authentication when issuing replication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

Third-party certificate support

Beginning with PowerStoreOS 2.1, customers can import a custom third-party certificate chain to PowerStore for connections to PowerStore Manager. The imported certificate replaces the onboard self-signed certificate for management.

With PowerStoreOS 3.5 and later, customers can import a custom third-party certificate chain to PowerStore for the VASA Provider. The imported certificate replaces the onboard self-signed certificate for VASA.

The certificates are visible from the **Settings > Security > Certificates** in PowerStore Manager.



Service	Type ↑	Scope	Issued By	Valid	Expiration Date	Issued To
Replication HTTP	Client CA Certifi...	PS17cea56d3930	CN=Dell EMC Po...	Yes	2049-02-15 09:3...	CN=Dell EMC P...
VASA HTTP	Client CA Certifi...	192.168.98.109	CN=POD,OU=GU...	Yes	2050-06-21 10:1...	CN=POD,OU=GU...
VASA HTTP	Client CA Certifi...	192.168.98.109	OU=VMware En...	Yes	2033-03-14 01:3...	OU=VMware En...
Replication HTTP	Server CA Certifi...	PS17cea56d3930	CN=Dell EMC Po...	Yes	2049-02-15 09:3...	CN=Dell EMC P...
VIM HTTP	Server CA Certifi...	faa5afd6-544a-4...	OU=VMware En...	Yes	2025-03-20 01:3...	C=US,CN=192.1...
Import HTTP	Server CA Certifi...	--	CN=stratvnx-72...	Yes	2024-04-06 09:1...	CN=stratvnx-72...
Witness_HTTP	Server CA Certifi...	192.168.105.136	C=US,ST=Mass...	Yes	2028-05-08 05:2...	C=US,ST=Mass...
Import HTTP	Server CA Certifi...	192.168.98.110	EMAILADDRES...	Yes	2026-11-12 02:0...	EMAILADDRES...
Import HTTP	Server CA Certifi...	192.168.80.34	CN=FNMO0184...	Yes	2027-03-04 06:4...	CN=FNMO0184...

Figure 10. Certificates in PowerStore Manager

VMware vCenter Certificate

Administrators can gain visibility into VMware virtual machines directly in PowerStore Manager by establishing a connection to a vCenter server.

In the IT industry, cybersecurity vulnerabilities such as man-in-the-middle attacks, data breaches, denial of service, and identity theft are prevalent, especially concerning data. PowerStoreOS 4.0 and later allows administrators to enable certificate verification before the system communicates with vCenter to strengthen its cybersecurity. This provides the administrator the ability to confirm that PowerStore is interacting with the intended

vCenter. When registering a new vCenter on PowerStoreOS 4.0, the newly added "Verify SSL server certificate" checkbox is checked by default and highly recommended

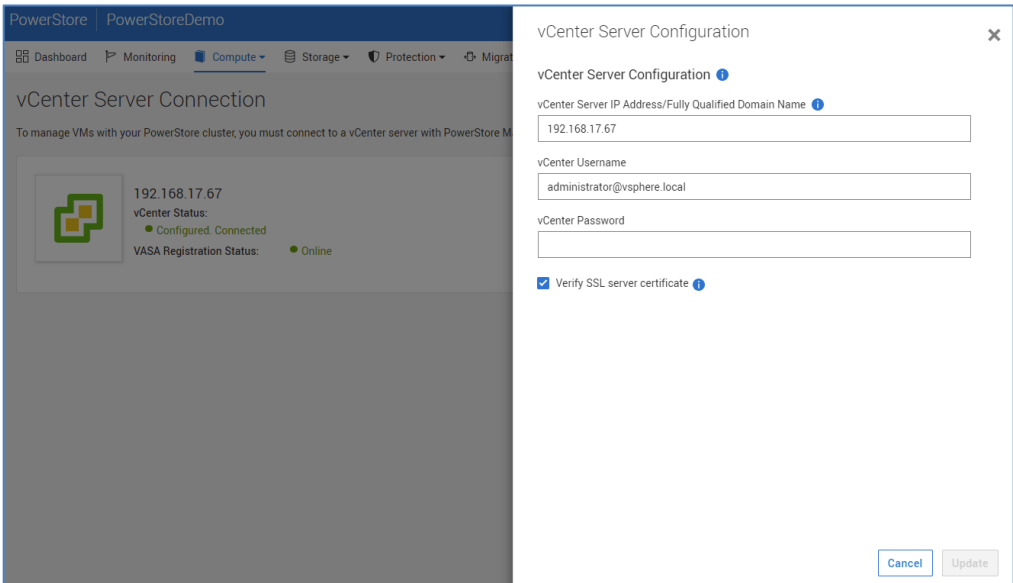


Figure 11. vCenter Verify SSL Certificate

When this is enabled, the system checks the validity of the certificate by comparing the Fully Qualified Domain Name (FQDN) or IP address, confirms the certificate's start date has passed, and ensures the certificate has not expired and will not expire soon. If all checks pass, the certificate details are displayed to the administrator. The administrator can then compare these details to the certificate in vCenter directly. If the administrator confirms that everything matches, PowerStore then saves a copy of the certificate, and authorizes communication between vCenter and PowerStore. If the certificate does not match, the system immediately designates it as untrusted, blocking communication with vCenter.

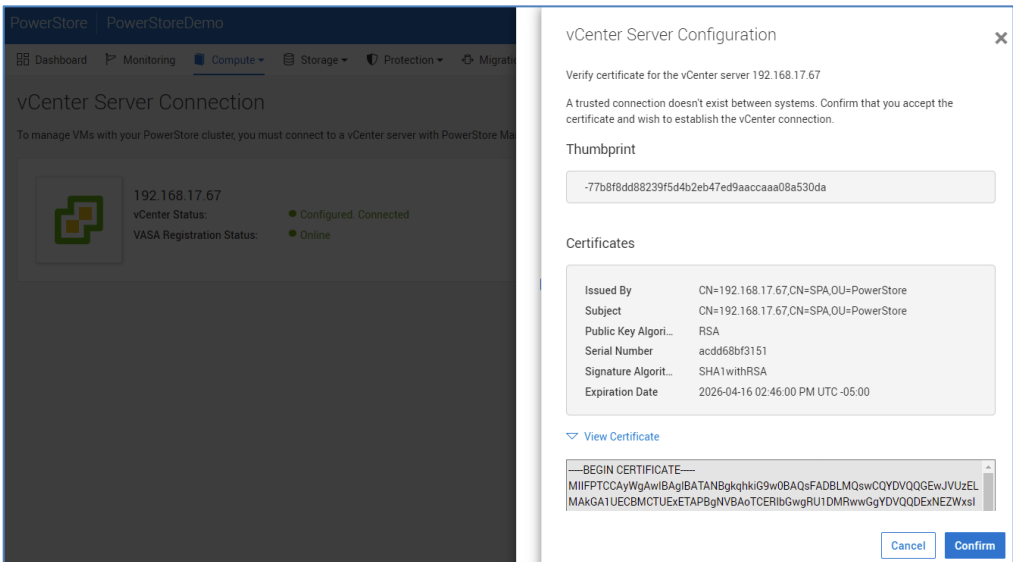


Figure 12. vCenter Certificate

If an administrator disables this feature, the registration process proceeds without vCenter certificate verification, similar to pre-4.0 releases. If the vCenter connection is removed in PowerStore Manager, the vCenter certificate is also removed, making the certificate untrusted and all communication with the disconnected vCenter ceases. However, the vCenter can be re-added again later using the same process.

If certificate verification is enabled and the administrator re-validates the certificate, it's marked as trusted, and communication is allowed. If certificate verification is disabled, the vCenter registration process proceeds without validating the certificate's details, and it is not displayed to the administrator.

Auditing

Auditing overview

Auditing provides a historical view of user activity on the system. A user with the role of Administrator, Security Administrator, or Storage Administrator can search and view configuration change events using the PowerStore Manager UI, PowerStore CLI, or REST API. The events that are audited are not just security-related: all create, modify, and delete operations are recorded to the audit log.

Remote logging

The storage system supports sending audit log messages to a maximum of two hosts. The hosts must be accessible from the storage system. Audit log message transfers can use a one-way authentication (Server CA Certificates) or an optional two-way authentication (Mutual Authentication Certificate). An imported certificate applies to each remote syslog server that is configured to use TLS Encryption. For more information about remote logging, see the [Dell PowerStore Security Configuration Guide](#).

Federal compliance

STIG

PowerStoreOS 3.5 and later offers Security Technical Implementation Guide (STIG) mode. STIG mode on PowerStore applies configuration changes to the core of the product so that the underlying containers meet STIG requirements related to the operating system, embedded web server, internal database use, and various networking functions.

PowerStore in STIG mode meets the stringent requirements of U.S. Federal sites. PowerStore is certified as a Data Storage Controller (DSC) on the Department of Defense Information Networks' (DoDIN) Approved Product List (APL).

For more information about STIG, see the [Dell PowerStore Security Configuration Guide](#).

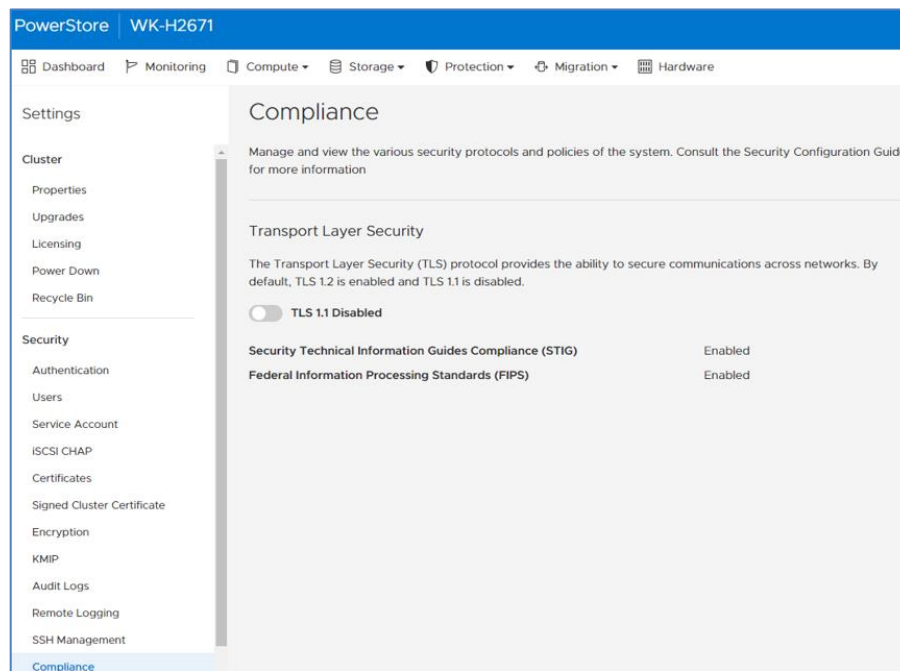


Figure 13. STIG mode

APEX AIOps Infrastructure Observability

APEX AIOps Infrastructure Observability overview

APEX AIOps Infrastructure Observability is a cloud-based AIOps proactive monitoring and predictive analytics application for Dell systems. Each customer is provided an independent, secure portal in which users can register and monitor their systems from a single portal. The secure portal ensures that each customer will only be able to see systems in their environment. Infrastructure Observability is included at no additional cost for systems under a ProSupport or higher contract.

Infrastructure Observability uses machine learning and predictive analytics to identify potential issues, anomalies, and security risks, and proactively notifies users, allowing them to take quick action to remediate identified issues.

- Performance metrics are compared with historical values to determine any deviation outside of normal ranges.
- Performance impacts are also analyzed to identify any increases in latency against other metrics such as IOPS and bandwidth. The analysis determines if workload characteristics or other competing resources cause an increase of latency and identifies where the impact is coming from.
- Capacity anomaly detection uses hourly analysis of usage to identify any surges of capacity utilization to identify resources at imminent risk of running out of space.

The Cybersecurity feature in Infrastructure Observability constantly compares the configuration of the PowerStore system to a set of user-selected security-related evaluation tests. Upon identifying a deviation between the actual and wanted configuration setting, Infrastructure Observability proactively notifies users of the violation and provides remediation steps to correct the issue. Based on NIST 800-53 R5 standards and Dell best practices, Cybersecurity in Infrastructure Observability quickly and

automatically ensures that the storage infrastructure is secure per the industry's best practices.

The Security Advisories section of the Cybersecurity feature in Infrastructure Observability notifies users of relevant Dell and VMware Security Advisories. Users quickly see a summary of vulnerabilities specific to their systems and code levels along with links to remediation details.

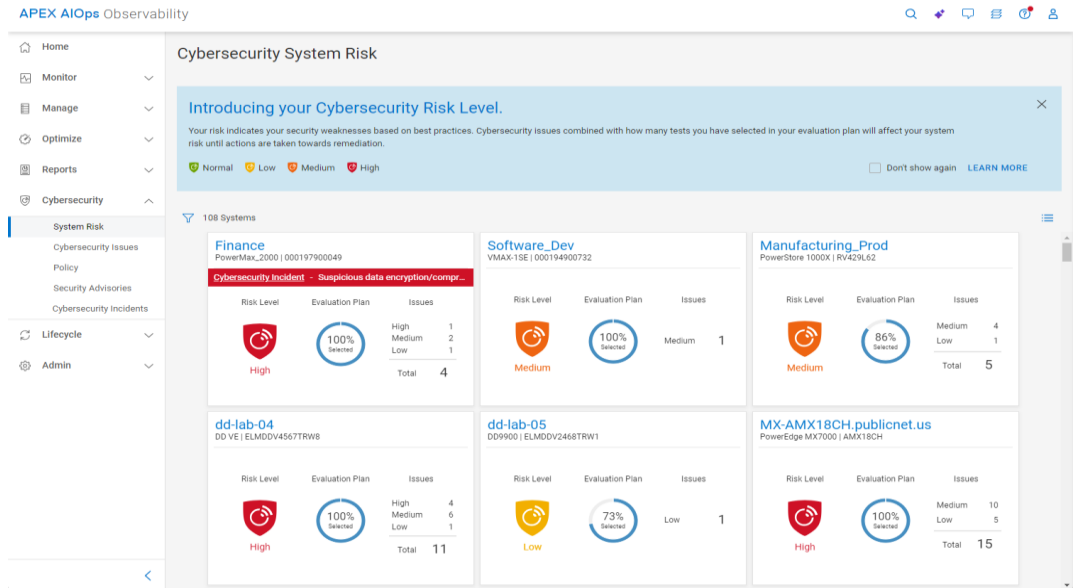


Figure 14. Cybersecurity system risk in Apex AIops Infrastructure Observability

With PowerStoreOS 4.0 and later, the Infrastructure Observability health score is now available on the PowerStore Manager Dashboard page if Support Connectivity and the **Connect to CloudIQ** options are enabled. This provides customers with a high-level overview of their cluster's health and provides the same look and feel as Infrastructure Observability .

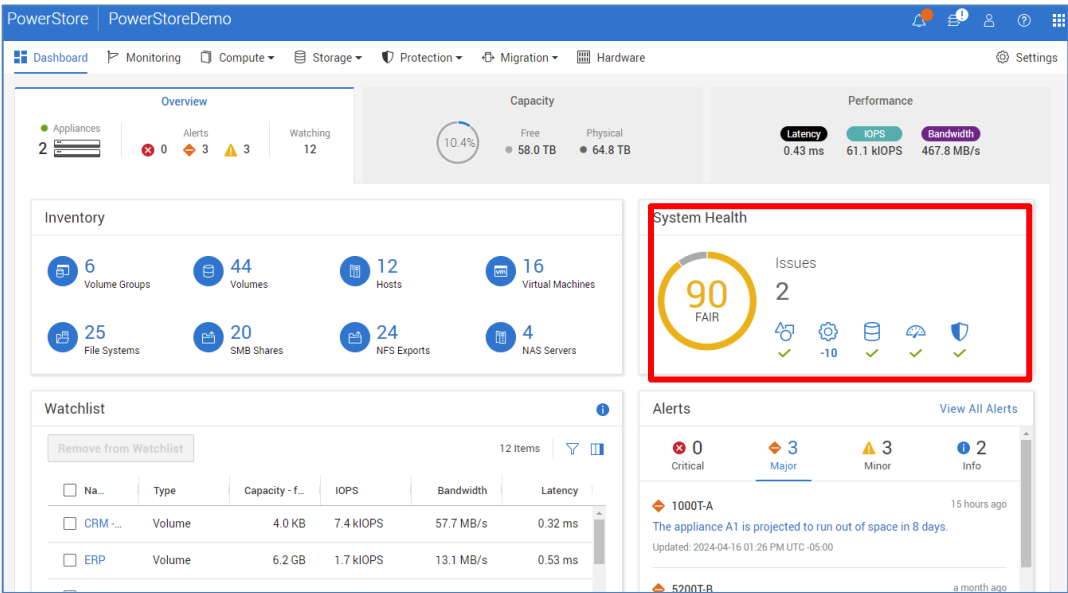


Figure 15. APEX AIOps Infrastructure Observability Health Score in PowerStore Manager

For more information about CloudIQ, see the [*Dell CloudIQ: A Detailed Review white paper*](#).

References

Dell Technologies documentation

The following Dell Technologies resources provide other information that is related to this document. Access to the documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- [PowerStore Info Hub](#)
- [Dell PowerStore product documentation and videos](#)
- [Dell PowerStore: Security Configuration Guide](#)
- [Dell PowerStore: PowerStore Manager Overview](#)
- [Dell PowerStore: Snapshots and Thin Clones](#)
- [PowerStore: File Capabilities](#)
- [Dell PowerStore: AppSync](#)
- [Dell PowerProtect Cyber Recovery](#)
- [Dell PowerProtect Cyber Recovery for AWS](#)
- [Dell CloudIQ: A Detailed Review](#)