Dell PowerStore 3.5

Security Target

Evaluation Assurance Level (EAL): EAL 2+

Doc No: 2171-001-D102
Version: 0.31
28 February 2024

Dell EMC
176 South Street
Hopkinton, MA, USA
01748

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Dell PowerStore 3.5 Security Target
ST Version:	0.31
ST Date:	28 February 2024

1.3 TOE REFERENCE

TOE Identification:	Dell PowerStore 3.5
TOE Developer:	Dell
TOE Type:	Data Storage (Other Devices and Systems)

1.4 TOE OVERVIEW

The TOE is a midrange capacity storage system comprised of the PowerStore T bare-metal appliance running the PowerStore OS software. The PowerStore T enables the management and provision of both block and file storage. The PowerStore T models are identified in Table 2 below.

The PowerStore hardware houses the disks in the storage array which are managed by the storage processors. It provides Network Access Server (NAS) and Storage Area Network (SAN) services by interfacing with the front-end clients (application hosts) and the back-end storage disks. Each of the storage arrays is a FIPS validated Self Encrypting Drive.

Application hosts (such as database servers, file servers, etc.) can access the PowerStore storage through traditional block and file protocols. The TOE presents storage to application hosts as a standard network-based virtual file server, or in the form of logical volumes to block-based client machines.

The TOE supports the following storage protocols:

- File Storage Protocols
  - Server Message Block (SMB)
  - Network File System (NFS)
- Block Storage Protocols
  - Internet Small Computer System Interface (iSCSI)
  - Fibre Channel (FC)

Each volume is a useable storage system volume that the TOE can expose to individual hosts. Application hosts can only access volumes for which permission has been granted by an authorized administrator.

Each File-based NAS server on the TOE can be configured to interface with a Lightweight Directory Access Protocol (LDAP) or Network Information Service (NIS) server. When a request for data access is made from a File-based client machine, the TOE checks the Access Control List (ACL) of the requested file or directory, and either grants or denies access to the user.

The TOE is managed by authorized administrators through the PowerStore Command Line Interface (PSTCLI) or the PowerStore Manager Graphical User Interface (GUI). Administrators are assigned a user role that provides them with access to specific TOE features and functions. Audit records are generated for security related events.

The PSTCLI is a Command Line Interface (CLI) that provides access to common functions for monitoring and managing the TOE. The PSTCLI provides access to functions for storage provisioning, status and configuration information retrieval, and other TOE administrative functions. The PowerStore Manager GUI is an HTML5 application that runs within a web browser. To access the functions available, an authorized administrator must open a web browser and enter the Internet Protocol (IP) address or hostname of the PowerStore management port.

The TOE is a combined software and hardware TOE. The PowerStore hardware consists of a Base Enclosure that contains two Intel Nodes and houses a 25-drive slot supporting the following drive types:

- Express Non-Volatile Memory Solid State Drive (NVMe SSD)
- Express Non-Volatile Memory Storage Class Memory (NVMe SCM)

The TOE also supports a maximum of three Expansion Enclosures with twenty-four (24) 2.5” NVMe drive slots.

1.4.1 TOE Environment

The following hardware and software components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Management Workstation	Windows Server 2019 (64 bit) supporting Mozilla Firefox v75 or later and running the PSTCLI client	General Purpose Computer Hardware
LDAP Server	Windows Server 2019 supporting Active Directory	General Purpose Computer Hardware
NIS Server	SLES 12 SP5 supporting NFSv3, NFSv4, or NFSv4.1	General Purpose Computer Hardware
iSCSI Host	Windows Server 2019	General Purpose Computer Hardware
FC Host	Windows Server 2019	General Purpose Computer Hardware
SMB User Workstation	Windows Server 2019 supporting SMB 3.1.1	General Purpose Computer Hardware
NFS User Workstation	SLES 12 SP5 supporting NFSv3, NFSv4, or NFSv4.1	General Purpose Computer Hardware

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE is a stand-alone appliance consisting of the PowerStore hardware and the PowerStore OS software. Figure 1 depicts the TOE in its evaluated configuration.

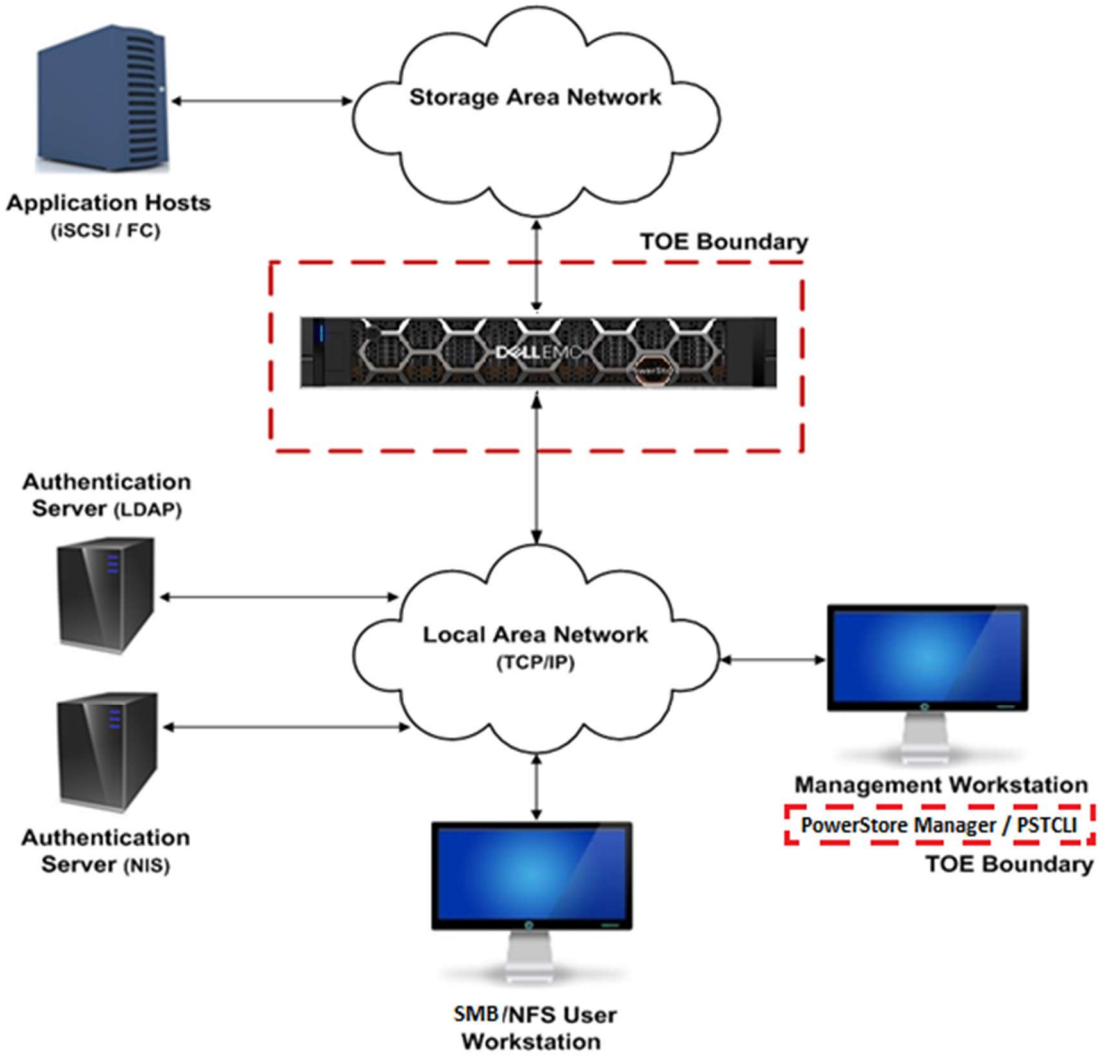

Figure 1 – TOE Deployment Diagram

1.5.2 TOE Components

The TOE is comprised of the following hardware and software.

TOE Component	Description
PowerStore Hardware	• PowerStore 500T • PowerStore 1200T • PowerStore 3200T • PowerStore 5200T • PowerStore 9200T
Software	PowerStore OS 3.5.0
	PSTCLI v3.5.0

Table 2 - TOE Hardware and Software

1.5.2.1 TOE Delivery

The PowerStore hardware is shipped directly to customers with the PowerStore OS installed. The TOE software is also available for download to registered users via the Dell Digital Locker website at:

- https://www.dell.com/support/software/us/en/4#/registration

Updating the software is described in the Dell PowerStore T Model Software Upgrade Guide. Customers must also download the PSTCLI client software from the above link. The software is presented to customers as follows:

- PowerStore T OS
  - 3.5.0.1-2083289-retail
- PSTCLI
  - pstcli-3.5.0.891-release-x64.msi

Note: The PowerStore Manager GUI is packaged as an HTML5 application deployed as part of the PowerStore OS.

1.5.2.2 TOE Guidance

All guidance documentation is provided in Portable Document Format (PDF) and is available for download to registered users at:

- https://www.dell.com/support/home/en-us. The TOE includes the following guidance documentation.

Document	Date or Revision
Dell PowerStore Planning Guide	May 2023

Document	Date or Revision
PowerStore Deployment Checklist	Rev A06
Dell PowerStore Hardware Information Guide for PowerStore 1000, 1200, 3000, 3200, 5000, 5200, 7000, 9000, and 9200	May 2023
Dell PowerStore Hardware Information Guide for PowerStore 500T Model	May 2023
Dell PowerStore Installation and Service Guide for PowerStore 1000, 1200, 3000, 3200, 5000, 5200, 7000, 9000, and 9200	May 2023
Dell PowerStore Installation and Service Guide for PowerStore 500T Model	May 2023
Dell PowerStore Networking Guide for PowerStore T Models	May 2023
Dell PowerStore T Model Software Upgrade Guide	May 2023
Dell PowerStore Security Configuration Guide	May 2023
Dell PowerStore Setting Up PowerStore Manager	May 2023
Dell PowerStore Statement of Volatility	May 2023
Dell PowerStore CLI Reference Guide	May 2023
Dell PowerStore CLI User Guide	May 2023
Dell PowerStore Configuring NFS	May 2023
Dell PowerStore Configuring SMB	May 2023
Dell PowerStore Configuring Volumes	May 2023
Dell PowerStore Monitoring Your System	May 2023
Dell PowerStore Protecting Your Data	May 2023
Dell PowerStore Release Notes for PowerStore OS Version 3.5.0.1	July 2023
Dell PowerStore Events and Alerts Reference Guide	May 2023
Dell PowerStore Power Down and Reboot Procedures Guide	May 2023
Dell PowerStore Open Source License and Copyright Information for GPLv3/LGPLv3	May 2023
Dell PowerStore Planning Guide	May 2023

Table 3 - PowerStore Documentation

The following Common Criteria Guidance Supplement is also available to customers, in PDF format, upon request:

- Dell PowerStore 3.5 Common Criteria Guidance Supplement, Version 0.7

1.5.3 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 4 summarizes the logical scope of the TOE.

Functional Class	Description
Security Audit	The TOE generates audit records for administrator login attempts and changes to the TOE configuration.
Cryptographic Support	Data stored on the TOE is encrypted and decrypted using FIPS 140-2 validated Self Encrypting Drives (SEDs). The relevant certificates are provided in section 7.2. Cryptographic keys on the PowerStore are handled by the RSA BSAFE® Crypto-C Micro Edition FIPS 140-2 validated cryptographic module (certificate #4305). The associated cryptographic algorithm validation program certificate is C2130. The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software.
User Data Protection	The TOE only allows authorized application servers access to stored user data. The integrity of stored data is protected using RAID technology.
Identification and Authentication	TOE administrators must identify and authenticate prior to gaining access to the TOE management functionality.
Security Management	The TOE provides management capabilities via a web-based GUI and a CLI. Management functions allow authorized administrators to configure system access and storage settings.
Protection of the TSF	The TOE provides reliable time stamps for auditable events.

Table 4 – Logical Scope of the TOE

1.5.4 Functionality Excluded from the Evaluated Configuration

1.5.4.1 Excluded TOE Features

The following features are excluded from this evaluation:

- Common Event Enabler (CEE)
- File-level retention
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Transfer Protocol (SNMP)
- Replication

- Network Data Management Protocol (NDMP)
- Distributed Hierarchical Storage Management (DHSM)
- Common Anti-Virus Agent (CAVA)
- Support Assist Enterprise (SAE)
- Express Non-Volatile Memory Non-Volatile Random Access Memory (NVMe NVRAM) – used for write caching
- Common Internet File System (CIFS) support
- File transfer protocol (ftp)

1.5.4.2 Excluded TOE Interfaces

The following TOE interfaces are supported but not included in this evaluation:

- Representational State Transfer (REST) Interface
    - Used by application developers to send HTTP operations for requests. It is not used in the evaluated configuration.
- vStorage APIs for Storage Awareness (VASA) Interface
    - Requires the installation of GUI plug-in and is not used in the evaluated configuration
- Ethernet Service Port connection
    - Ethernet Service port accessed only through the service account and is not used in the evaluated configuration
- Secure Shell (SSH) maintenance Interface
    - Disabled by default and not used in the evaluated configuration

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 5 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ACCESS	Access to user data could be improperly granted to application hosts which should not have access, and users with access to those hosts.
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.UNAUTH	A hostile/unauthorized person could gain access to stored data by bypassing the protection mechanisms of the TOE.
T.UNDETECT	Authorized users or unauthorized persons may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

Table 5 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 6 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.PROTECT	The TOE shall incorporate mechanisms to protect against disclosure of the data it has been entrusted to store.
P.RAID	User data must be protected from loss due to disk failure.

Table 6 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 7.

Assumption	Description
A.ATTRIBUTE	The attributes used by the TOE to make File Storage Access Control decisions are provided by the operational environment.
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NETWORK	The network on which the TOE components are operating on is sufficiently protected from attackers.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

Table 7 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the operational environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must provide a means of logging security related events.
O.CRYPTO	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.
O.PROTECT	The TOE must protect the data that it has been entrusted to store from unauthorized access.

Table 8 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.SERVER	The operational environment shall provide an Active Directory server and a NIS server for maintaining access control security attributes for file-based storage on the TOE. Files support Unix-style Access Control Lists (ACLs) or NT-style Discretionary Access Control Lists (DACLs) as appropriate.

Table 9 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ACCESS	T.ACCOUNT	T.UNAUTH	T.UNDETECT	P.PROTECT	P.RAID	A.ATTRIBUTE	A.LOCATE	A.NETWORK	A.NOEVIL
O.ADMIN	X	X	X	X						
O.AUDIT				X						
O.CRYPTO					X					
O.IDENTAUTH		X	X	X						
O.INTEGRITY						X				
O.PROTECT	X									
OE.ADMIN										X
OE.PHYSICAL								X	X	

	T.ACCESS	T.ACCOUNT	T.UNAUTH	T.UNDETECT	P.PROTECT	P.RAID	A.ATTRIBUTE	A.LOCATE	A.NETWORK	A.NOEVIL
OE.SERVER							X			

Table 10 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE.

Threat: T.ACCESS	Access to user data could be improperly granted to application hosts which should not have access, and users with access to those hosts.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.PROTECT	The TOE must protect the data that it has been entrusted to store from unauthorized access.
Rationale:	O.ADMIN mitigates this threat by only allowing authorized administrators the ability to manage TOE access functions. O.PROTECT mitigates this threat by identifying application hosts by name before allowing access to protected data.	

Threat: T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.

Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security management functions of the TOE are restricted to authorized administrators. O.IDENTAUTH mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions.

Threat: **T.UNAUTH**	A hostile/unauthorized person could gain access to stored data by bypassing the protection mechanisms of the TOE.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
Rationale:	O.ADMIN mitigates this threat by providing authorized administrators the ability to manage TOE security functions. O.IDENTAUTH mitigates this threat by ensuring that all users are identified and authenticated prior to gaining access to the TOE security management functions.	

Threat: **T.UNDETECT**	Authorized users or unauthorized persons may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.AUDIT	The TOE must provide a means of logging security related events.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.

Rationale:	O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. O.AUDIT counters this threat by ensuring that the TOE tracks all management actions taken against the TOE. O.IDENTAUTH mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions.

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE back to the OSPs applicable to the TOE.

Policy: **P.PROTECT**	The TOE shall incorporate mechanisms to protect against disclosure of the data it has been entrusted to store.	
Objectives:	O.CRYPTO	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.
Rationale:	O.CRYPTO ensures that stored data is protected from disclosure through the use of cryptographic mechanisms.	

Policy: **P.RAID**	User data must be protected from loss due to disk failure.	
Objectives:	O.INTEGRITY	The TOE must protect the user data that it has been entrusted to store from integrity errors due to disk failure.
Rationale:	O.INTEGRITY supports this policy by ensuring that the TOE provides the ability to protect data in the case of disk failure.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: A.ATTRIBUTE	The attributes used by the TOE to make File Storage Access Control decisions are provided by the operational environment.	
Objectives:	OE.SERVER	The operational environment shall provide an Active Directory server and a NIS server for maintaining access control security attributes for file-based storage on the TOE. Files support Unix-style Access Control Lists (ACLs) or NT-style Discretionary Access Control Lists (DACLs) as appropriate.
Rationale:	OE.SERVER supports this assumption by providing the attributes required by the TOE to make access control decisions for File-based storage.	

Assumption: A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: A.NETWORK	The network on which the TOE components are operating on is sufficiently protected from attackers.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting TOE components from physical attack.	

Assumption: A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated

Assumption: **A.NOEVIL**	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
		in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	OE.ADMIN supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC, summarized in Table 11.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (authentication key)
	FCS_CKM.1(2)	Cryptographic key generation (at-rest key encryption key)
	FCS_CKM.1(3)	Cryptographic key generation (in flight key encryption key)
	FCS_CKM.1(4)	Cryptographic key generation (lockbox master key)
	FCS_CKM.1(5)	Cryptographic key generation (media encryption key)

Class	Identifier	Name
	FCS_CKM.4(1)	Cryptographic key destruction (authentication key)
	FCS_CKM.4(2)	Cryptographic key destruction (at-rest key encryption key)
	FCS_CKM.4(3)	Cryptographic key destruction (in flight key encryption key)
	FCS_CKM.4(4)	Cryptographic key destruction (lockbox master key)
	FCS_CKM.4(5)	Cryptographic key destruction (media encryption key)
	FCS_COP.1(1)	Cryptographic operation (authentication key)
	FCS_COP.1(2)	Cryptographic operation (at-rest key encryption key)
	FCS_COP.1(3)	Cryptographic operation (in flight key encryption key)
	FCS_COP.1(4)	Cryptographic operation (lockbox master key)
	FCS_COP.1(5)	Cryptographic operation (media encryption key)
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (Block Storage)
	FDP_ACC.1(2)	Subset access control (File Storage)
	FDP_ACF.1(1)	Security attribute based access control (Block Storage)
	FDP_ACF.1(2)	Security attribute based access control (File Storage)
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (Block Storage)
	FMT_MSA.1(2)	Management of security attributes (File Storage)

Class	Identifier	Name
	FMT_MSA.3(1)	Static attribute initialisation (Block Storage)
	FMT_MSA.3(2)	Static attribute initialisation (File Storage)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps

Table 11 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*Administrator login attempts, the following administrator actions that result in a configuration change to the storage array:*

- *adding, modifying, or deleting volumes*
- *adding, modifying, or deleting SMB shares*
- *adding, modifying, or deleting NFS mounts*
- *changes to host access permissions*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

6.2.1.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*authorised administrators*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1(1) Cryptographic key generation (authentication key)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*HMAC DRBG*] and specified cryptographic key sizes [*256 bit*] that meet the following: [*SP800-90A*].

6.2.2.2 FCS_CKM.1(2) Cryptographic key generation (at-rest key encryption key)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*HMAC DRBG*] and specified cryptographic key sizes [*256 bit*] that meet the following: [*SP800-90A*].

6.2.2.3 FCS_CKM.1(3) Cryptographic key generation (in flight key encryption key)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*HMAC DRBG*] and specified cryptographic key sizes [*256 bit*] that meet the following: [*SP800-90A*].

6.2.2.4 FCS_CKM.1(4) Cryptographic key generation (lockbox master key)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(4) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*HMAC DRBG*] and

specified cryptographic key sizes [*256 bit*] that meet the following: [*SP800-90A*].

6.2.2.5 FCS_CKM.1(5) Cryptographic key generation (media encryption key)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(5) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*HMAC DRBG*] and specified cryptographic key sizes [*256 bit*] that meet the following: [*SP800-90A*].

6.2.2.6 FCS_CKM.4(1) Cryptographic key destruction (authentication key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1(1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwriting with 0x00)*] that meets the following: [*no standard*].

6.2.2.7 FCS_CKM.4(2) Cryptographic key destruction (at-rest key encryption key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1(2) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwriting with 0x00)*] that meets the following: [*no standard*].

6.2.2.8 FCS_CKM.4(3) Cryptographic key destruction (in flight key encryption key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1(3) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwriting with a new value*] that meets the following: [*no standard*].

6.2.2.9 FCS_CKM.4(4) Cryptographic key destruction (lockbox mater key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1(4) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwriting with 0x00)*] that meets the following: [*no standard*].

6.2.2.10 FCS_CKM.4(5) Cryptographic key destruction (media encryption key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1(5) The TSF shall destroy cryptographic keys in accordance with ~~a specified~~ **the** cryptographic key destruction method [*documented in the security policy for the validated cryptographic modules in* Table 15] that meets the following: [*no standard*].

6.2.2.11 FCS_COP.1(1) Cryptographic operation (authentication key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1) The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES-KWP*] and cryptographic key sizes [*256 bit*] that meet the following: [*FIPS 197*].

6.2.2.12 FCS_COP.1(2) Cryptographic operation (at-rest key encryption key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(2) The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES-KWP*] and cryptographic key sizes [*256 bit*] that meet the following: [*FIPS 197*].

6.2.2.13 FCS_COP.1(3) Cryptographic operation (in flight key encryption key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(3) The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES-KWP*] and cryptographic key sizes [*256 bit*] that meet the following: [*FIPS 197*].

6.2.2.14 FCS_COP.1(4) Cryptographic operation (lockbox master key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(4) The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES256-GCM-SHA256*] and cryptographic key sizes [*256 bit*] that meet the following: [*FIPS 197*].

6.2.2.15 FCS_COP.1(5) Cryptographic operation (media encryption key)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(5) The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES-XTS*] and cryptographic key sizes [*256 bit*] that meet the following: [*FIPS 197*].

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1(1) Subset access control (Block Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the [*Block Storage Access Control SFP*] on

[

Subjects: Hosts (application servers);

Objects: Storage volumes;

Operations: Read and write

].

6.2.3.2 FDP_ACC.1(2) Subset access control (File Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the [*File Storage Access Control SFP*] on

[

Subjects: Users (accessing storage from client machines);

Objects: SMB shares and NFS mounts;

Operations: Read, Write, Execute

].

6.2.3.3 FDP_ACF.1(1) Security attribute based access control (Block Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(1) The TSF shall enforce the [*Block Storage Access Control SFP*] to objects based on the following:

[

Subjects: Hosts (application servers)

Security Attributes:

1) *iSCSI Qualified Name (IQN)*
2) *World Wide Name (WWN)*

Objects: Storage volumes

Security Attributes:

1) *IQN access list*
2) *WWN access list*

].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[*A valid subject of the TOE is allowed to read and write to TOE storage if the IQN or WWN of the subject is included in the list of hosts that have access to the specified volume*].

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

6.2.3.4 FDP_ACF.1(2) Security attribute based access control (File Storage)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(2) The TSF shall enforce the [*File Storage Access Control SFP*] to objects based on the following:

[

Subjects: Users (accessing storage from client machines)

Security Attributes:

1) *Username*

2) *Authentication status (success or failure)*

3) *IP address (for NFS access)*

Objects: File Shares

Security Attributes:

1) *NFS Mount permissions: Unix-style ACLs for each file and directory*

2) *SMB Share Permissions: NT-style Discretionary Access Control Lists (DACLs) for each file and directory*

].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[*A successfully authenticated subject of the TOE is allowed to perform an operation if the content of the Access Control List (containing permissions) for the object authorizes the Subject to perform the desired operation*].

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [

1. *For SMB access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects and control over the overall share permissions for the entire domain;*
2. *For NFS access, the user must access the NFS mount from a computer running an IP address listed in the allowed hosts configuration for the TOE;*
3. *For NFS access, subjects that are authorized as superusers (root) can perform all operations on all objects;*
4. *For root users accessing an NFS mount, access will be permitted if the host that the root user is using to connect to the NFS mount is listed under the 'trusted hosts' list in the TOE configuration*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*].

6.2.3.5 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all **user data** ~~objects~~, based on the following attributes: [*parity data for RAID 5 and RAID 6*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*reconstruct the user data*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual **Administrators** ~~users~~: [*UserID, password, role*].

Application Note: UserID, password and role information are maintained for Administrators using local authentication. When LDAP authentication is used, the Administrator's username and password are maintained by the Directory server and the Administrator's role is maintained by the TOE. The term 'Administrator' is used to refer to a user in the Administrator, Operator, Security Administrator, Storage Administrator, or Storage Operator role.

6.2.4.2 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: User authentication applies to users accessing File-based storage on the TOE as well as administrators accessing management functions via the management interfaces.

6.2.4.3 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: User identification applies to users accessing File-based storage on the TOE as well as administrators accessing management functions via the management interfaces.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1(1) Management of security attributes (Block Storage)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(1) The TSF shall enforce the [*Block Storage Access control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*WWN and IQN access lists*] to [*the Administrator, Storage Administrator, and Storage Operator roles*].

Application Note: The Block Storage Access Control SFP does not actually control access to the security attributes; rather, these attributes are used in the enforcement of the Block Storage Access Control SFP and are restricted by role-based access control.

6.2.5.2 FMT_MSA.1(2) Management of security attributes (File Storage)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(2) The TSF shall enforce the [*File Storage Access control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*trusted hosts*] to [*the Administrator, Storage Administrator, and Storage Operator roles*].

Application Note: The File Storage Access Control SFP does not actually control access to the security attributes; rather, these attributes are used in the enforcement of the File Storage Access Control SFP and are restricted by role-based access control.

6.2.5.3 FMT_MSA.3(1) Static attribute initialisation (Block Storage)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(1) The TSF shall enforce the [*Block Storage Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*Administrator and Storage Administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.4 FMT_MSA.3(2) Static attribute initialisation (File Storage)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the [*File Storage Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*Administrator and Storage Administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.5 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

[

a) viewing administrative information;

b) administering the Block Storage Access Control SFP;

c) administering the File Storage Access Control SFP;

d) managing storage; and

e) managing user account information

].

6.2.5.6 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles

[

- *Administrator*
- *Operator*
- *Security Administrator*
- *Storage Administrator*
- *Storage Operator*

].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 12 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following table provides a mapping between the SFRs and Security Objectives.

	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDENTAUTH	O.INTEGRITY	O.PROTECT
FAU_GEN.1		X				
FAU_SAR.1		X				
FCS_CKM.1(1)			X			
FCS_CKM.1(2)			X			
FCS_CKM.1(3)			X			
FCS_CKM.1(4)			X			
FCS_CKM.1(5)			X			
FCS_CKM.4(1)			X			
FCS_CKM.4(2)			X			
FCS_CKM.4(3)			X			
FCS_CKM.4(4)			X			
FCS_CKM.4(5)			X			
FCS_COP.1(1)			X			
FCS_COP.1(2)			X			
FCS_COP.1(3)			X			
FCS_COP.1(4)			X			
FCS_COP.1(5)			X			
FDP_ACC.1(1)						X
FDP_ACC.1(2)						X
FDP_ACF.1(1)						X
FDP_ACF.1(2)						X
FDP_SDI.2					X	
FIA_ATD.1	X			X		
FIA_UAU.2	X			X		X
FIA_UID.2	X			X		X
FMT_MSA.1(1)	X					X

	O.ADMIN	O.AUDIT	O.CRYPTO	O.IDENTAUTH	O.INTEGRITY	O.PROTECT
FMT_MSA.1(2)	X					X
FMT_MSA.3(1)	X					X
FMT_MSA.3(2)	X					X
FMT_SMF.1	X					X
FMT_SMR.1	X					
FPT_STM.1		X				

Table 13 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ADMIN**	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MSA.1(1)	Management of security attributes (Block Storage)
	FMT_MSA.1(2)	Management of security attributes (File Storage)
	FMT_MSA.3(1)	Static attribute initialisation (Block Storage)
	FMT_MSA.3(2)	Static attribute initialisation (File Storage)
	FMT_SMF.1	Management of TSF data
	FMT_SMR.1	Security roles
Rationale:	FDP_ATD.1 supports this objective by ensuring that the TOE maintains security attributes for administrative users. FDP_UAU.2 and FDP_UID.2 support this objective by ensuring that only authorized administrators have access to TOE functions and data.	

	FMT_MSA.1(1) and FMT_MSA.3(1) support this objective by identifying the management restrictions of the Block Storage Access Control SFP. FMT_MSA.1(2) and FMT_MSA.3(1) support this objective by identifying the management restrictions of the File Storage Access Control SFP. FMT_SMF.1 meets this objective by ensuring that the management functions are utilized to securely manage the TOE. FMT_SMR.1 supports this objective by ensuring that specific roles are defined to govern management of the TOE.

Objective: **O.AUDIT**	The TOE must provide a means of logging security related events.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 supports this objective by generating records for auditable events. FAU_SAR.1 supports this objective by ensuring that the TOE provides the ability to review the audit trail. FPT_STM.1 ensures that a time stamp is provided for each auditable event.	

Objective: **O.CRYPTO**	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.	
Security Functional Requirements:	FCS_CKM.1(1)	Cryptographic key generation (authentication Key)
	FCS_CKM.1(2)	Cryptographic key generation (at-rest key encryption key)
	FCS_CKM.1(3)	Cryptographic key generation (in flight key encryption key)
	FCS_CKM.1(4)	Cryptographic key generation (lockbox master key)
	FCS_CKM.1(5)	Cryptographic key generation (media encryption key)
	FCS_CKM.4(1)	Cryptographic key destruction (authentication key)

	FCS_CKM.4(2)	Cryptographic key destruction (at-rest encryption key)
	FCS_CKM.4(3)	Cryptographic key generation (in flight key encryption key)
	FCS_CKM.4(4)	Cryptographic key generation (lockbox master key)
	FCS_CKM.4(5)	Cryptographic key generation (media encryption key)
	FCS_COP.1(1)	Cryptographic operation (authentication key)
	FCS_COP.1(2)	Cryptographic key generation (at-rest key encryption key)
	FCS_COP.1(3)	Cryptographic key generation (in flight key encryption key)
	FCS_COP.1(4)	Cryptographic key generation (lockbox master key)
	FCS_COP.1(5)	Cryptographic key generation (media encryption key)
Rationale:	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.1(4), FCS_CKM.1(5), FCS_CKM.4(1), FCS_CKM.4(2), FCS_CKM.4(3), FCS_CKM.4(4), FCS_CKM.4(5), FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), and FCS_COP.1(5) support this objective by providing the cryptographic functionality required to protect the confidentiality of data stored on the TOE.	

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.1	User identification before any action
Rationale:	FIA_ATD.1 supports this objective by ensuring that the TOE maintains security attributes for administrative users. FIA_UAU.2 meets this objective by ensuring that TOE Administrators are successfully authenticated before gaining access to TOE functions and data. FIA_UID.2 supports this objective by ensuring that the identity of each TOE Administrator is known before allowing access to TOE functions and data.	

Objective: O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.	
Security Functional Requirements:	FDP_SDI.2	Stored data integrity monitoring and action
Rationale:	FDP_SDI.2 meets this objective by providing the RAID functionality that protects against integrity errors due to a hardware failure.	

Objective: O.PROTECT	The TOE must protect the data that it has been entrusted to store from unauthorized access.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control (Block Storage)
	FDP_ACC.1(2)	Subset access control (File Storage)
	FDP_ACF.1(1)	Security attribute based access control (Block Storage)
	FDP_ACF.1(2)	Security attribute based access control (File Storage)
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_MSA.1(1)	Management of security attributes (Block Storage)
	FMT_MSA.1(2)	Management of security attributes (File Storage)
	FMT_MSA.3(1)	Static attribute initialisation (Block Storage)
	FMT_MSA.3(2)	Static attribute initialisation (File Storage)
	FMT_SMF.1	Specification of management functions
Rationale:	FDP_ACC.1(1) and FDP_ACF.1(1) support this objective by identifying the rules and attributes of the Block Storage Access Control SFP, which are used to control application host access to data stored on the TOE. FDP_ACC.1(2) and FDP_ACF.1(2) support this objective by identifying the rules and attributes of the File Storage Access Control SFP, which control user access to data stored on the TOE. FDP_UAU.2 and FIA_UID.2 support this objective by ensuring that only authorized administrators have access to TOE functions and data, and are identified and authenticated before being provided with TOE access.	

	FMT_MSA.1(1) and FMT_MSA.3(1) support this objective by restricting the management of the Block Storage Access Control SFP to authorized administrators. FMT_MSA.1(2) and FMT_MSA.3(2) support this objective by restricting the management of the File Storage Access Control SFP to authorized administrators. FMT_SMF.1 meets this objective by ensuring that the management functions are utilized to securely manage the TOE, thus protecting the integrity of stored user data.

6.4.3 Dependency Rationale

Table 14 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1(1)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(1)
FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1(2)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(2)
FCS_CKM.1(3)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1(3)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(3)
FCS_CKM.1(4)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1(4)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(4)
FCS_CKM.1(5)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1(5)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(5)
FCS_CKM.4(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(1)

SFR	Dependency	Dependency Satisfied	Rationale
FCS_CKM.4(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(2)
FCS_CKM.4(3)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(3)
FCS_CKM.4(4)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(4)
FCS_CKM.4(5)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(5)
FCS_COP.1(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(1)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(1)
FCS_COP.1(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(2)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(2)
FCS_COP.1(3)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(3)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(3)
FCS_COP.1(4)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(4)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(4)
FCS_COP.1(5)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(5)
	FCS_CKM.4	✓	Satisfied by FCS_CKM.4(5)
FDP_ACC.1(1)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(1)
FDP_ACC.1(2)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(2)
FDP_ACF.1(1)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(1)
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(1)

SFR	Dependency	Dependency Satisfied	Rationale
FDP_ACF.1(2)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(2)
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(2)
FDP_SDI.2	None	N/A	
FIA_ATD.1	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(1)
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(2)
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(1)
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2)
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_STM.1	None	N/A	

Table 14 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Reporting Procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2

augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

The TOE generates audit records for startup and shutdown of the audit function, all administrator login attempts, and all administrator actions that result in a configuration change. Audit records contain the date and time of the event, the type of event, subject identity (if applicable), and the outcome of the event (success or failure).

Authorized administrators can view the audit records from the PSTCLI or the PowerStore Manager GUI. The audit records are presented in a manner suitable for a user to interpret the information.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_SAR.1.

7.2 CRYPTOGRAPHIC SUPPORT

Data at Rest Encryption (D@RE) in PowerStore utilizes FIPS 140-2 validated Self-Encrypting Drives (SEDs) for primary storage (NVMe SSD, NVMe SCM and SAS SSD).

The D@RE feature on the PowerStore appliance is set at the factory, and when enabled, encryption cannot be disabled. The PowerStore appliance must contain all SEDs. If you try to add a non-self-encrypting drive to an appliance, the appliance raises an error. When the TOE detects a new drive, it will automatically follow the steps as required in the FIPS security policy for that specific drive to enable encryption, set up locking features and authentication key for protection. The following table identifies each supported SED and the relevant Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP) certificate numbers:

SED, Part Number, CMVP Cert #	Function	Algorithm	CAVP Cert #
Intel Optane D4800X SSD PN 005053029 CMVP # 3511	Key Generation	DRBG	C214
	Encryption/Decryption	AES	C1431
Intel DC SSD D7-D4512 005052919 - 005052925 CMVP # 3662	Key Generation	DRBG	C817
	Encryption/Decryption	AES	C586
	Encryption/Decryption	AES	C587
	Encryption/Decryption	AES	C793

SED, Part Number, CMVP Cert #	Function	Algorithm	CAVP Cert #
Kioxia CM6 005053981 - 005053982 CMVP # 3983	Key Generation	DRBG	C2002
	Encryption/Decryption	AES	C1925
Samsung PM1723b 005053076 - 005053083 CMVP # 3525	Key Generation	DRBG	C1845
	Encryption/Decryption	AES	C5007
Samsung PM1733 005053702 - 005053709 CMVP # 3755	Key Generation	DRBG	C1292
	Encryption/Decryption	AES	C1271

Table 15 - Cryptographic Algorithms

Encryption is performed within each drive before the data is written to the media. This protects the data on the drive against theft or loss and attempts to read the drive directly by physically de-constructing the drive. Reading encrypted data requires the authentication key for the SED to unlock the drive. Only authenticated SEDs will be unlocked and accessible. Once the drive is unlocked, the SED decrypts the encrypted data back to its original form.

An embedded Key Manager Service (KMS) runs on the active node of each PowerStore appliance. The KMS uses the RSA BSAFE® Crypto-C Micro Edition FIPS 140-2 validated cryptographic module (certificate #4305). The KMS automatically generates a random authentication key for SEDs during the initialization of the appliance. Each drive has a unique authentication key that is used in the SED lock and unlock processes that are controlled by the KMS. The KMS also manages the local keystore file lockbox storage to support automatic encryption key backup to system and boot drives. The lockbox is encrypted with the lockbox master key using AES256-GCM, and the authentication key is also wrapped with the at-rest KEK before being secured by the lockbox.

The PowerStore has two KEKs. One KEK is for wrapping cryptographic keys while stored in keystore (at-rest KEK). The other KEK is used for in flight processing within the appliance (in flight KEK). Both are generated following FCS_CKM.1. After a cryptographic key for drive authentication is generated, it is wrapped with an at-rest KEK and persisted in the keystore. When the authentication key is required by the processing module for drive operations it is wrapped with the in-flight KEK. The processing module receives this doubly wrapped authentication key and upwraps it for use by the SED. The AES-KWP key wrap algorithm is used for wrapping/unwrapping.

When encryption is enabled, all the authentication keys are stored within the appliance and are wrapped with an in flight KEK or at-rest KEK. Media Encryption Keys (MEKs) are generated internally within the SEDs and are stored

on the dedicated hardware of the SEDs. The MEKs cannot be accessed but can be erased to allow for decommissioning of a SED.

Keys within the PowerStore OS software are erased either by overwriting with 0x00 values or by overwriting with a new value. The MEKs are erased according to each SSD's security policy.

TOE Security Functional Requirements addressed: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.1(3), FCS_CKM.1(4), FCS_CKM.1(5), FCS_CKM.4(1), FCS_CKM.4(2), FCS_CKM.4(3), FCS_CKM.4(4), FCS_CKM.4(5), FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5).

7.3 USER DATA PROTECTION

The TOE supports user data protected by the File Storage Access Control SFP and the Block Storage Access Control SFP. File Users are any users accessing data or storage on the TOE via one of the file protocols (SMB or NFS). Block Users are any application servers (hosts) accessing data or storage on the TOE via one of the block protocols (iSCSI or FC).

7.3.1 File Storage Access Control SFP

All access to storage is performed via a SMB or NFS client on behalf of the user. These clients are basic pieces of software (such as the client within Windows Explorer) used to map and access file-based storage. The TOE enforces the File Storage Access Control SFP on users connecting to the storage on the TOE for NFS and SMB.

- After successful authentication for NFS users, the TOE checks user permissions for each file or directory's ACL on each user's access request to determine if the user has appropriate permissions to access the files or directories.
- After successful authentication for SMB users, the TOE checks user permissions for each file or directory's DACL on each user's access request to determine if the user has appropriate permissions to access the files or directories.

The ability to connect to an NFS mount, and SMB share, is granted to users by Administrators or Storage Administrators. Users are associated with SMB shares via an access list, while a list of IP addresses is associated with NFS mounts as an access list.

Individual file and directory access control management is granted to SMB users with File Owner or Change Permissions set in the DACL for the user. NFS users with the root role can modify permissions for all files and directories, or users with the File Owner or Change Permissions for any given file or directory can manage access controls for those particular files and directories.

A Linux/Unix host can mount to the PowerStore-hosted NFS Shared Folder Server if the host has been explicitly authorized. Similarly, a Windows user can map to the PowerStore-hosted SMB NAS Servers if the user has been explicitly authorized.

The export of a SMB Shared Folder Server is determined in part by the Server Configuration LDAP setting. The PowerStore-hosted SMB Shared Folder Server must be in a Windows domain with an LDAPv3-compatible server set up. A Windows client machine can map to the share only if it is a member of the defined domain. For SMB access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects.

Client machine access to the PowerStore-hosted NFS Shared Folder Server can be configured based on IP address or network host name, IP subnet range, or a Netgroup. For the NFS access protocol, users connecting to TOE storage who are *superusers* can perform all operations on all objects. Clients must be recognized as "trusted" by the system in order to submit a root request, otherwise it will be mapped to the "nobody" role.

Each file and directory has an ACL associated with it. Each ACL has a set of permissions that are granted or explicitly denied to that user. Whenever a user requests an access to a file or directory, the TOE utilizes its File Storage Access Control SFP (stored with each file and directory) to decide whether or not that access is permitted.

TOE Security Functional Requirements addressed: FDP_ACC.1(2), FDP_ACF.1(2).

7.3.2 Block Storage Access Control SFP

The TOE enforces the Block Storage Access Control Security Function Policy (SFP) which is used to manage access from block-based application servers to configured Logical Units on the TOE. Access must specifically be granted for a host to access storage.

When a host is configured, the administrator provides:

- The name of the host
- The IP address of the host
- For iSCSI access, the iSCSI address (iSCSI Qualified Name (IQN)) of the host. Within the Storage Area Network (SAN), this is the address of the iSCSI initiator
- For FC access, the WWN of the host. This is the unique address of the Host Bus Adapter (HBA) that initiates the connection to the storage resources
- Access settings. The options are:
    - No access
    - Volume access
    - Snapshot access
    - Volume and Snapshot access

When a storage volume is configured, the administrator identifies:

- Name and description of the storage resource
- The size associated with the volume
- The hosts that have access to this resource. Hosts are identified by address:
    - For iSCSI, this is the IQN
    - For FC access, this is the WWN of the host

When a user attempts to access storage resources, PowerStore verifies the IQN or WWN of the host initiator and verifies that the host has access to the requested volume before allowing access.

Storage may be accessed as a volume or a snapshot. A snapshot is a point-in-time copy of the stored data. It provides a record of the content in the targeted storage resource at a particular date and time, and may be used to support data protection and recovery. The presentation of stored data as a snapshot is beyond the scope of the evaluation; however, the Block Storage Access Control SFP applies equally to both access types.

Both Windows and Linux hosts may access storage via iSCSI and FC as follows.

- iSCSI Access
    - For a Windows host, the host must be able to access the iSCSI interface. The Microsoft iSCSI initiator service must be started.
    - For a Linux host, hosts connect to storage resources by using Linux iSCSI software available on the host. Those responsible for the host will have to mount the directory for the file system associated with the storage.
- FC Access
    - On the Windows host, the server connection must be added using Microsoft Storage Manager for SANs. Storage Manager for SANs is a Microsoft Management Console (MMC) snap-in used to create and manage storage volumes on Fibre Channel.
    - Hosts connect to storage resources by using Linux FC software available on the host. Those responsible for the host will have to mount the directory for the file system associated with the storage.

TOE Security Functional Requirements addressed: FDP_ACC.1(1), FDP_ACF.1(1)

7.3.3 Stored Data Integrity

The TOE implements a parity protection mechanism known as “Mapped RAID” to protect the user data from integrity errors. Mapped RAID consumes the physical disk space on the drives and implements stripe protection of the physical devices using Redundant Array of Independent Disks (RAID). Mapped RAID includes a proprietary algorithm that provides single drive failure redundancy

within a RAID Resiliency Set (RRS) and enforces distributed parity and automatic rebuilds of the user-data.

When an integrity error is detected, an alert is placed in a log file. Administrators may view alerts via the Alerts page of the PowerStore Manager GUI or from the PSTCLI.

TOE Security Functional Requirements addressed: FDP_SDI.2.

7.4 IDENTIFICATION AND AUTHENTICATION

7.4.1 Administrative Identification and Authentication

The TOE supports the use of both local and LDAP authentication. The TOE maintains the UserID, password and role for Administrators subject to local authentication, and only the role information for users authenticating via an LDAP directory. The TOE verifies the UserID and password on login and assigns a role.

Administrators can access the TOE through a web browser or through a command line interface. Identification and authentication must be completed before Administrators are provided with access to the TOE.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_UAU.2, FIA_UID.2.

7.4.2 File-Based Identification and Authentication

NFS users are authenticated against a NIS server in the operational environment. The server from which the request is coming is identified and authenticated based on the username and password. If the UserID is `root` then the host must also be assigned as a trusted host within the TOE configuration.

SMB users are authenticated locally or with LDAP. The server from which the request is coming is identified and authenticated based on the username and password.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_UAU.2, FIA_UID.2.

7.5 SECURITY MANAGEMENT

The TOE is shipped with a factory default Management account (`admin`) and password (`Password123#`) for initial access and configuration. With this default account, administrators can reset default passwords, configure the system settings, create user accounts, and allocate storage. Changing the default password for the admin account is a requirement during the initial configuration process.

Once the TOE has been configured, authorized administrators can access the TOE management functions via the PSTCLI or the PowerStore Manager GUI.

Each administrator is assigned a role which determines TOE access capabilities. Table 16 identifies the administrative roles and describes the available TOE functions:

Management Task	**Operator**	**Storage Administrator**	**Administrator**	**Security Administrator**	**Storage Operator**
Change own local login password	X	X	X	X	X
Add, delete, or modify hosts		X	X		X
Create storage		X	X		X
Delete storage		X	X		X
Add storage objects, such as volumes, shares, and storage groups to a storage resource		X	X		X
View storage configuration and status	X	X	X	X	X
View user accounts			X	X	
Add, delete or modify user accounts			X	X	
View current software status	X	X	X	X	X
Perform software upgrade		X	X		
Perform initial configuration			X		
Modify NAS server configuration		X	X		
Modify system settings		X	X		X
Modify network settings			X		
View Alerts, Events, and Jobs	X	X	X	X	X
View Audit Log		X	X	X	

Table 16 - TOE Administrative Roles and Privileges

Default attributes for the Block Storage Access Control SFP are restrictive because an application host will not have access to storage resources until its WWN or IQN is specifically listed in the volume's host access list. The TOE provides mechanisms to govern which hosts can access which volumes. Default attributes for the File Storage Access Control SFP are restrictive because trusted host does not exist until entered by an Administrator. The Security Management functions allow Administrators assigned the appropriate role to configure this functionality.

Client machines accessing the TOE via SMB, or NFS protocols do not have access until the user is authenticated. Once authenticated, the user is granted access according to the Access Control List associated with each file and directory. SMB, and NFS file and directory attributes that can be modified include read, write, and execute permissions. There are no set default permissions.

TOE Security Functional Requirements addressed: FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1.

7.6 PROTECTION OF THE TSF

The TOE provides reliable time stamps for auditable events. Timestamp information is provided by the TOE hardware.

TOE Security Functional Requirements addressed: FPT_STM.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Administrator	The generic term 'Administrator' is used to refer to a user in the Administrator, Operator, Security Administrator, Storage Administrator or Storage Operator role.
Application Host	An Application Host is a term used to generically define systems and/or applications accessing storage on the TOE.
In Flight	This term is used when referring to the passing of encryption keys between software components within the appliance.

Table 17 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
CAVA	Common Anti-Virus Agent
CAVP	Cryptographic Algorithm Validation Program
CIFS	Common Internet File System
CMVP	Cryptographic Module Validation Program
CC	Common Criteria
CEE	Common Event Enabler
CLI	Command Line Interface
DACL	Discretionary Access Control List
DAE	Disk Array Enclosure
DHSM	Distributed Hierarchical Storage Management
DPE	Disk Processor Enclosure
DRBG	Deterministic Random Bit Generator

Acronym	Definition
D@RE	Data at Rest Encryption
EAL	Evaluation Assurance Level
FC	Fibre Channel
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTML5	Hypertext Markup Language 5
IP	Internet Protocol
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
IT	Information Technology
KEK	Key Encryption Key
KMS	Key Manager Service
LDAP	Lightweight Directory Access Protocol
MEK	Media Encryption Key
MMC	Microsoft Management Console
NAS	Network Attached Storage
NVMe	Express Non-Volatile Memory
NDMP	Network Data Management Protocol
NFS	Network File System
NIS	Network Information Service
NVRAM	Non-Volatile Random Access Memory
OE	Operating Environment
OSP	Organizational Security Policy
PDF	Portable Document Format
PP	Protection Profile
PSTCLI	PowerStore Command Line Interface
RAID	Redundant Array of Independent Disks

Acronym	Definition
REST	Representational State Transfer
RRS	RAID Resiliency Set
SAN	Storage Area Network
SAS	Serial Attached SCSI
SCM	Storage Class Memory
SED	Self-Encrypting Drive
SFP	Security Function Policy
SFR	Security Functional Requirement
SMB	Server Message Block
SMI-S	Storage Management Initiative Specification
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Transfer Protocol
SSD	Solid State Drive
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
UEMCLI	Unified Element Manager Command Line Interface
VASA	vStorage APIs for Storage Awareness
WWN	World Wide Name

Table 18 – Acronyms