Dell PowerScale OneFS v9.5

Security Target

Version 1.9

May 2024

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
0.1	November 01, 2022	Initial Draft.
0.2	9 March 2023	Addressed developer comments. Initial draft for evaluation.
1.0	3 May 2023	Addressed evaluator ORs.
1.1	14 August 2023	Updated drive list.
1.2	7 September 2023	Addressed CB ORs.
1.3	2 November 2023	Removed LDAP and Syslog claims.
1.4	9 November 2023	Added excluded functionality section.
1.5	26 January 2024	Addressed evaluator ORs.
1.6	9 April 2024	Addressed evaluator ORs.
1.7	12 April 2024	Removed drive from scope.
1.8	7 May 2024	Added iDRAC to Excluded Functionality.
1.9	22 May 2024	Address OR16, Update guidance document references

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Dell PowerScale OneFS v9.5 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The Dell PowerScale OneFS v9.5 is a storage solution for unstructured data. It provides a platform to support large data workload, simplify management and protect data at scale.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Dell PowerScale OneFS v9.5.0.8 - Build B_9_5_0_005 Patch 9.5.0.8_LTS2023_GA-RUP_PSP-4211
Security Target	Dell PowerScale OneFS v9.5 Security Target, v1.9

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) EAL2+ ALC_FLR.2

1.4 Terminology

Table 2: Terminology

Term	Definition
ACE	Access Control Entry
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
DACL	Discretionary Access Control List

Term	Definition
EAL	Evaluation Assurance Level
FEC	Forward Error Correction
FIPS	Federal Information Processing Standards
GID	Group Identifier
GUI	Graphical User Interface
HDFS	Hadoop Distributed File System
HMAC	Hash Message Authentication Code
MAC	Media Access Control
NFS	Network File System
OSP	Organizational Security Policy
POSIX	Portable Operating System Interface
PP	Protection Profile
RBAC	Role Based Access Control
SED	Self-encrypting drive
SFR	Security Functional Requirement
SID	Security Identifier
SMB	Server Message Bloc
SP	Special Publication
SSH	Secure Shell
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
WebUI	Web User Interface
WORM	Write Once, Read Many

2 TOE Description

2.1 Type

4 The TOE is a data storage device.

2.2 Usage

5 As shown in Figure 1, the TOE is a data storage solution that combines the three layers of traditional storage architectures – file system, volume manager, and data protection – into a unified software layer, creating a single distributed file system that runs on a storage cluster, and eliminates the need for volume management. The TOE is managed using a Command Line Interface (CLI), Web User Interface (WebUI) and REST API.

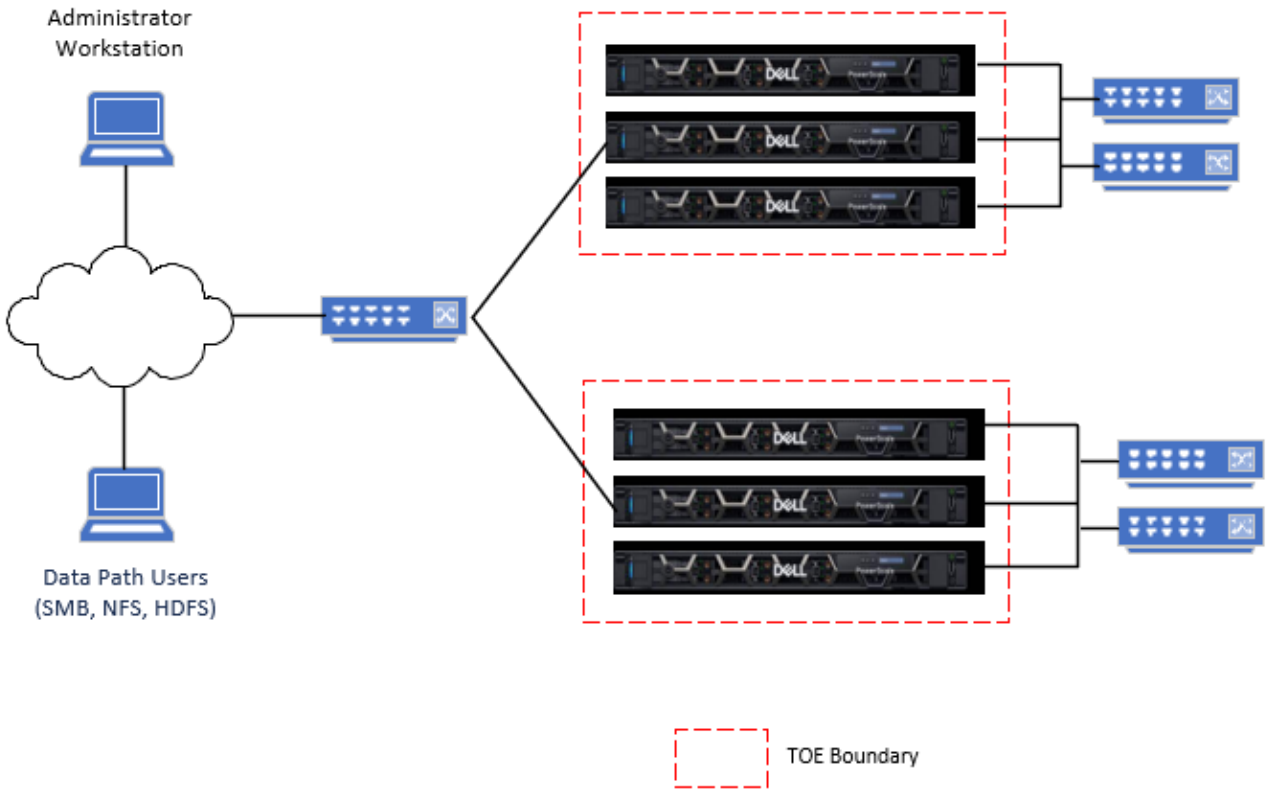


Figure 1: Example TOE Deployment

2.3 Security Functions

6 The TOE provides the following security functions:

a) **Security Audit.** Audit entries are generated for security related events. The audit logs may be reviewed and filtered by authorized administrators.

b) **Cryptographic Support.** The TOE provides for Data at Rest Encryption (D@RE) of information it has been entrusted to store.

c) **User Data Protection.** The TOE restricts access data to authorized users. Access to user data may be further restricted by creating access zones for internal groups or departments. The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE. Data is monitored for integrity errors and the data is rebuilt when errors are detected.

d) **Identification & Authentication.** Administrative users are identified and authenticated prior to being granted access to TOE functions. Only local authentication is supported in the evaluated configuration.

e) **Security Management.** The TOE provides management capabilities via a web based Graphical User Interface (GUI), a CLI and REST API. Management functions allow the administrators to manage access control, configure system settings, and view audit records.

f) **Protection of the TSF.** Data is replicated to other clusters to ensure availability. Data is automatically recovered in the case of loss in multiple scenarios. Timestamp information is provided to support auditing. Cluster-to-cluster communications are protected using TLS.

g) **TOE Access.** A banner is presented on user login to the WebUI or CLI.

h) **Trusted Path/Channels.** Communications between the TOE and remote administrators is protected using TLS (WebUI and REST API) and SSHv2 (CLI).

2.4 Physical Scope

7 The TOE includes the PowerScale OneFS v9.5 software running on the hardware models shown in Table 3. In the evaluated configuration, a TOE model may include a combination of any of the identified supported drives.

Table 3: TOE Model Mapping and Supported Drives

Model	TOE Hardware CPU	Supported KIOXIA Drives	Supported Hitachi Drives
F200	Single Socket Intel Cascade Lake 4210 (2.2GHz, 10C)	• KPM6WRUG1T92 • KPM6WRUG3T84 • KPM6WRUG7T68 • KPM6WVUG960G • P6V1T60D	• Hitachi W5QTR641 • Hitachi W5STR641
F800	Intel Broadwell-EP E5-2697A v4 (2.6GHz, 16c)		
F810			
F600	Dual Socket Intel Cascade Lake 4210 (2.2GHz, 10C)	• KCM6FRUL1T92 • KCM6FRUL3T84 • KCM6FRUL7T68 • KCM6FRUL15T3	N/A
F900	Dual Socket 2ndGeneration Intel® Xeon® Gold 6240R (2.2GHz, 24C) Cascade Lake		

2.4.1 Drive CAVP

2.4.1.1 KIOXIA Drives

8 All supported KIOXIA drives identified in Table 3 are equipped with the KIOXIA TCG Enterprise SSC Crypto Sub-Chip TC58NC1132GTC. The drive CPU (crypto sub-chip) is CAVP-validated under certificate C1925.

2.4.1.2 Hitachi Drives

9 All supported Hitachi drives identified in Table 3 are CAVP-validated under certificate AES-4309.

2.4.2 TOE Delivery

10 The TOE software is installed on the TOE hardware and delivered to the customer by a commercial courier service with a package tracking system.

11 For software updates, the software is provided to customers via secure download from the Dell support portal. Software upgrades are made available to customers who are under active support contracts, via secure web-based downloads from the Dell support site. This method enables customers who already own Dell PowerScale OneFS systems to upgrade their software to the CC-certified version.

12 Downloads are available to logged-in customers at https://www.dell.com/support.

2.4.3 Guidance Documents

13 All guidance documentation is provided in Portable Document Format (PDF) online at the Dell Documentation portal: https://www.dell.com/support/kbdoc/en-ca/000207820/onefs-9-5-0-0-documentation-info-hub.

14 The TOE includes the following guidance documentation:

a) PowerScale OneFS 9.5.0.0 Web Administration Guide, October 2023

b) PowerScale OneFS 9.5.0.0 CLI Administration Guide, October 2023

c) PowerScale OneFS 9.5.0.0 CLI Command Reference, January 2023

d) PowerScale OneFS 9.5.0.0 API Reference Guide, January 2023

e) PowerScale OneFS Event Reference Guide, January 2023

f) PowerScale OneFS 9.5.0.0 Security Configuration Guide, January 2023

15 The TOE also includes the following Common Criteria Guide, available to customers upon request to their Dell account team:

- Dell_PowerScale_EAL2_AGD_1.5.pdf

2.4.4 Non-TOE Components

16 The TOE operates with the following components in the environment:

a) **Admin Workstation**. Workstation required to access and manage the TOE.

b) **Data Path Users (Workstations)**. Support for NFS, HDFS and SMB file sharing services.

c) **Frontend Switch**. Generic network switch required for TOE cluster connection.

d) **Backend Switches**. Generic network switches required for TOE nodes in a single cluster.

2.4.5 Excluded Functionality

17 The following features are excluded from this evaluation:

a) Log offloading

b) LDAP / Active Directory Authentication

c) iDRAC

2.5 Logical Scope

18 The logical scope of the TOE comprises the security functions defined in section 2.3.

3 Security Problem Definition

3.1 Threats

Table 4: Threats

Identifier	Description
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.AVAIL	User data may become unavailable due to corruption of the data, or loss of the supporting hardware.
T.DISCLOSURE	A malicious user could expose data on the TOE due to weak encryption.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.UNDETECT	Authorized users may be able to access TOE data or modify TOE behaviour without a record of those actions in order to circumvent TOE security functionality.
T.UNAUTH	An unauthorized user may be able to gain access to user data in order to view or modify private information.

3.2 Assumptions

Table 5: Assumptions

Identifier	Description
A.AUTH	Data path users are identified and authenticated prior to gaining access to the TOE.
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE. These administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

3.3 Organizational Security Policies

Table 6: Organizational Security Policies

Identifier	Description
P.RETAIN	The TOE shall provide a means to identify a retention period before which data is not to be deleted and prevent data from being deleted prior to the expiry of the retention period.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 7: Security Objectives for the Operational Environment

Identifier	Description
OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical and logical attack.
OE.USERAUTH	Data path users must be identified and authenticated in the operational environment.

4.2 Objectives for the TOE

Table 8: Security Objectives

Identifier	Description
O. ACCESS	The TOE must restrict access to the user data held by the TOE to only authorized data path users. The TOE must be able to restrict user access based on defined access zones.
O. ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security functions provided by the TOE, and restrict these functions and facilities from unauthorized use.
O. AUDIT	The TOE must record audit events for changes to the TOE configuration, and use of the TOE data channels. Audit records must be readable by authorized administrators.

Identifier	Description
O. BANNER	The TOE must display an access warning to administrative users prior to login on the Web and CLI applications.
O. CRYPTO	The TOE must provide cryptographic functions to support encryption of data at rest.
O. IDENTAUTH	The TOE must ensure that users are identified and authenticated 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 data corruption, or disk or node failure.
O.PROTCOMMS	The TOE shall provide protected communication channels for remote administrators and cluster-to-cluster transmissions.
O. PROTECT	The TOE must provide a means of disabling access to unused TOE services.
O. RETAIN	The TOE must prevent the deletion of data prior to expiry of the assigned retention period.
O. TIME	The TOE must provide reliable timestamps.

5 Security Requirements

5.1 Conventions

19 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a number with parenthesis (e.g. “FDP_ACC.1(2)”).

5.2 Extended Components Definition

20 Table 9 identifies the extended components which are incorporated into this ST.

Table 9: Extended Components

Component	Title	Rationale
FDP_RET_EXT.1	Retention of data	The SFR addresses the requirement to retain data.
FTA_SAC_EXT.1	Service Access	The SFR addresses the requirement for controlling access to TOE services.

5.2.1 Retention of data (FDP_RET_EXT)

5.2.1.1 Family Behavior

21 This family provides requirements that address retention of user data while it is stored within containers controlled by the TOE Security Functionality (TSF), and is modelled after FDP_SDI Stored Data Integrity.

5.2.1.2 Component Leveling

5.2.1.3 Management: FDP_RET_EXT.1

22 The following actions could be considered for the management functions in FMT:

a) Setting the retention period.

5.2.1.4 Audit: FDP_RET_EXT.1

23 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Changes to the retention period.

FDP_RET_EXT.1 Retention of data

Hierarchical to: No other components.

Dependencies: FPT_STM.1

FDP_RET_EXT.1.1 The TSF shall allow a retention period to be assigned to user data.

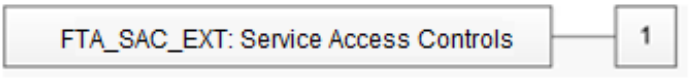
FDP_RET_EXT.1.2 The TSF shall deny requests to delete the data until the retention period has expired or has been removed.

5.2.2 Service access control (FTA_SAC_EXT)

5.2.2.1 Family Behavior

24 This family defines the requirements for controlling access to TOE services, and is modelled after FTA_TSE TOE Session Establishment.

5.2.2.2 Component Leveling



5.2.2.3 Management: FTA_SAC_EXT.1

25 The following actions could be considered for the management functions in FMT:

a) Configuration of allowed services.

5.2.2.4 Audit: FTA_SAC_EXT.1

26 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Changes to the configuration of allowed services.

FTA_SAC_EXT.1 Service and port access control

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SAC_EXT.1.1 The TSF shall restrict access to services based on system configuration.

5.3 Functional Requirements

Table 10: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FCS_COP.1	Cryptographic operation (Data at rest encryption)
FDP_ACC.1(1)	Subset access control (Data path)
FDP_ACC.1(2)	Subset access control (RBAC)
FDP_ACC.1(3)	Subset access control (Access Zones)
FDP_ACF.1(1)	Security attribute based access control (Data path)
FDP_ACF.1(2)	Security attribute based access control (RBAC)
FDP_ACF.1(3)	Security attributes based access control (Access Zones)
FDP_RET_EXT.1	Retention of data
FDP_SDI.2	Stored data integrity monitoring and action
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MSA.1(1)	Management of security attributes (Data path)
FMT_MSA.1(2)	Management of security attributes (RBAC)
FMT_MSA.1(3)	Management of security attributes (Access Zones)
FMT_MSA.3(1)	Static attribute initialisation ((Data path)
FMT_MSA.3(2)	Static attribute initialisation (RBAC)
FMT_MSA.3(3)	Static attribute initialisation (Access Zones)
FMT_SMF.1	Specification of management Functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RCV.3	Automated recovery without undue loss

Requirement	Title
FPT_STM.1	Reliable time stamps
FPT_TRC.1	Internal TSF consistency
FTA_TAB.1	Default TOE access banners
FTA_SAC_EXT.1	Service access
FTP_TRP.1	Trusted path

5.3.1 Security Audit (FAU)

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) *[user login, use of sudo, use of the REST API, logging of enabled protocols].*

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*].

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 [root and *users assigned the SystemAdmin and SecurityAdmin roles]* 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.

5.3.2 Cryptographic Operation (FCS)

FCS_COP.1 Cryptographic operation (Data at rest encryption)

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	The TSF shall perform [*symmetric encryption*] in accordance with a specified cryptographic algorithm [*AES-XTS*] and cryptographic key sizes [*256 bits*] that meet the following: [*Federal Information Processing Standard Publication 197*].

5.3.3 User Data Protection (FDP)

FDP_ACC.1(1) Subset access control (Data path)

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [*Data Access SFP*] on [*Subjects: Windows Users[1], Unix Users[2]* *Objects: Files, Directories* *Operations: read, write, delete, execute*].

FDP_ACC.1(2) Subset access control (RBAC)

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [*Role Based Access Control SFP*] on [*Subjects: Administrators* *Objects: Security Management data and functions* *Operations: view, create, delete, execute*].

[1] Windows Users are associated with the SMB protocol/file share type.

[2] Unix Users are associated with the NFS and HDS protocols/file share types.

FDP_ACC.1(3) Subset access control (Access Zones)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Access Zone SFP*] on
[*Subjects: Windows Users, Unix Users*
Objects: Files, Directories
Operations: read, write, delete, execute].

FDP_ACF.1(1) Security attribute based access control (Data path)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*Data access SFP*] to objects based on the following: [
Subjects: Windows Users, Unix Users
Subject attributes: Subject attributes defined in Table 11
Objects: Files, Directories
Object attributes: Object attributes defined in Table 11].

Table 11: Cryptographic Operation

File Share Type	Subject Attributes	Object Attributes
SMB (Windows)	UID, GID, SID	ACL
NFS (Unix)	UID, GID	POSIX mode bits
HDFS (Unix)	UID, GID	POSIX mode bits

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

- *A user may access an object if the object's ACL or POSIX mode bits indicate that the SID, UID or GID associated with the user is permitted access*
- *A user may not overwrite, modify or delete an object if the object remains subject to a retention period*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*an authorized administrator has granted explicit access through a DACL or ACE, the user is the owner of the root account*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*an authorized administrator has explicitly denied access through a DACL or ACE*].

FDP_ACF.1(2) Security attribute based access control (RBAC)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the [*Role Based Access Control SFP*] to objects based on the following: [*Subjects: Administrators* *Subject attributes: Role* *Objects: Security Management data and functions* *Object attributes: none*].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an administrator may access security management data and functions if the user is assigned to a role that permits access].*
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1(3) Security attribute based access control (Access Zones)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the [*Access Zones SFP*] to objects based on the following: [*Subjects: Windows Users, Unix Users* *Subject attributes: Groupnet, IP Address* *Objects: Files, Directories* *Object attributes: Access Zone*].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A user can access files and directories in an Access Zone if the user:* • *belongs to a Groupnet assigned to the Access Zone* • *is coming from an IP Address in the IP Address pool assigned to the Access Zone; and* • *has permission to access the object in accordance with the Data Path SFP*].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

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

FDP_RET_EXT.1 Retention of data

Hierarchical to: No other components.

Dependencies: FPT_STM.1

FDP_RET_EXT.1.1 The TSF shall allow a retention period to be assigned to user data.

FDP_RET_EXT.1.2 Where a retention period has been assigned to data, the TSF shall deny requests to delete the data until the retention period has expired, or has been removed.

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 objects, based on the following attributes: [*Forward Error Correction (FEC) codes*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*rebuild the data using Reed-Solomon encoding*].

5.3.4 Identification and Authentication (FIA)

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*viewing of node status, events, cluster details, capacity, throughput, and drive status*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1 Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow [*viewing of node status, events, cluster details, capacity, throughput, and drive status*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.3.5 Security Management (FMT)

FMT_MSA.1(1) Management of security attributes (Data path)

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	The TSF shall enforce the [*Data Access SFP*] to restrict the ability to [change_default, query, modify, delete] the security attributes [*ACL, POSIX mode bits*] to [*root, users in the SystemAdmin or SecurityAdmin role, or in a custom role with appropriate permissions*].

FMT_MSA.1(2) Management of security attributes (RBAC)

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	The TSF shall enforce the [*Role Based Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*role*] to [*root, users in the SecurityAdmin role, or in a custom role with appropriate permissions*].

FMT_MSA.1(3) Management of security attributes (Access Zones)

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	The TSF shall enforce the [*Access Zone SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Groupnet, Access Zone*] to [*root, users in the SecurityAdmin role, or in a custom role with appropriate permissions*].

FMT_MSA.3(1) Static attribute initialisation (Data path)

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [*Data Access SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [*the file owner*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(2) Static attribute initialisation (RBAC)

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [*Role Based Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [*no user*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(3) Static attribute initialisation (Access Zones)

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [*Access Zone SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*no user*] to specify alternative initial values to override the default values when an object or information is created.

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: [*view audit information, configure SmartLock retention periods, configure users and roles, configure service access, configure SyncIQ data replication, configure access banners*].

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 [*root, SecurityAdmin, SystemAdmin, AuditAdmin and custom roles*].

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

5.3.6 Protection of the TSF (FPT)

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

FPT_RCV.3 Automated recovery without undue loss

Hierarchical to: FPT_RCV.2 Automated recovery.

Dependencies: AGD_OPE.1 Operational user guidance.

FPT_RCV.3.1 When automated recovery from [*disk or node failure*] is not possible, the TSF shall ~~enter a maintenance mode~~ **maintain a constant state** where the ability to return to a secure state is provided.

FPT_RCV.3.2 For [*disk or node failure*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3	The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [*no losses*] for loss of TSF data or objects under the control of the TSF.
FPT_RCV.3.4	The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

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.

FPT_TRC.1 Internal TSF consistency

Hierarchical to:	No other components.
Dependencies:	FPT_ITT.1 Basic internal TSF data transfer protection.
FPT_TRC.1.1	The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.
FPT_TRC.1.2	When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [*changes to the cluster data*].

5.3.7 TOE Access (FTA)

FTA_TAB.1 Default TOE access banners

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TAB.1.1	Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

FTA_SAC_EXT.1 Service Access

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SAC_EXT.1.1	The TSF shall restrict access to services based on system configuration.

5.3.8 Trusted Path/ Channels (FTP)

FTP_TRP.1	**Trusted Path**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].
FTP_TRP.1.2	The TSF shall permit [remote users] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [*remote administration*]

5.4 Assurance Requirements

27 The TOE security assurance requirements are summarized in Table 12 commensurate with EAL2+ (ALC_FLR.2).

Table 12: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	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	Basic Flaw Remediation
Security Target Evaluation	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_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Security Audit

Related SFRs: FAU_GEN.1, FAU_SAR.1

28 There is a syslog auditing function on each node. These logs record events such as user login, use of sudo and start and stop of syslog services.

29 REST API logs, which must be explicitly enabled, record user activities and start up and shutdown functions. REST API auditing tracks and records all configuration events that are handled by the PowerScale REST API. The process involves auditing the CLI, web administration interface, and PowerScale APIs. System configuration auditing events are stored in the config audit topic directories.

30 Protocol auditing tracks and stores activity performed through SMB, NFS, and HDFS protocol connections. When protocol auditing is enabled for an access zone, file access events through the SMB, NFS, and HDFS protocols are recorded in the protocol audit topic directories.

31 The audit events are logged on the individual nodes where the SMB, NFS, or HDFS client initiated the activity. The events are then stored in a binary file under /ifs/.ifsvar/audit/logs. The audit logs include security relevant information including date and time of the event, type of event and the identity of the user causing the event, where applicable.

32 All audit records are presented in a manner suitable for administrators to interpret the information. Only authorized administrators assigned the SystemAdmin or the AuditAdmin role may view all audit records.

33 **Note**: Audit records may only be viewed via the CLI or Console interfaces.

6.2 Cryptographic Support

Related SFRs: FCS_COP.1

6.2.1 Data at Rest

34 Data at rest encryption is provided by self-encrypting drives within the Dell PowerScale OneFS v9.5 hardware. The TOE supports a series of KIOXIA and Hitachi drives as mapped in Table 3 above. KIOXIA drive encryption is provided by the FIPS-validated TCG Enterprise SSC Crypto Sub-Chip TC58NC1132GTC (CAVP C1925). Hitachi drives are also CAVP validated (CAVP AES-4309). 256-bit AES-XTS symmetric encryption is supported in the evaluated configuration.

6.3 User Data Protection

6.3.1 Data Path

Related SFRs: FDP_ACC.1(1), FDP_ACF.1(1)

35 PowerScale supports two types of permissions data on files and directories that control who has access: Windows-style access control lists (ACLs) and POSIX mode bits (UNIX permissions). Global policy settings can be configured to customize default ACL and UNIX permissions to best support the environment. The PowerScale file system installs with UNIX permissions as the default. An administrator can give a file or directory an ACL by using Windows Explorer or PowerScale administrative tools. Typically, files created over SMB or in a directory that has an ACL, receive an ACL. If a file receives an ACL, PowerScale stops enforcing the file's mode bits; the mode bits are provided for only protocol compatibility, not for access control.

36 In a UNIX environment, file and directory access is controlled by POSIX mode bits, which grant read, write, or execute permissions to the owning user, the owning group, and everyone else. PowerScale supports the standard UNIX tools for viewing and changing permissions: ls, chmod, and chown. All files contain 16 permission bits, which provide information about the file or directory type and the permissions. The lower 9 bits are grouped as three 3-bit sets, called triples, which contain the read, write, and execute (rwx) permissions for each class of users—owner, group, and other. Permissions flags can be set to grant permissions to each of these classes. Unless the user is root, PowerScale checks the class to determine whether to grant or deny access to the file. The classes are not cumulative: The first class matched is applied.

37 In Windows environments, file and directory permissions, referred to as access rights, are defined in access control lists (ACLs). ACLs are more complex than mode bits, and therefore can be used to express much more granular sets of access rules. PowerScale checks the ACL processing rules commonly associated with Windows ACLs. A Windows ACL contains zero or more access control entries (ACEs), each of which represents the SID of a user or a group as a trustee. In PowerScale, an ACL can contain ACEs with a UID, GID, or SID as the trustee. Each ACE contains a set of rights that allow or deny access to a file or folder. An ACE can optionally contain an inheritance flag to specify whether the ACE should be inherited by child folders and files. Instead of the standard three permissions available for mode bits, ACLs have 32 bits of fine-grained access rights. Of these, the upper 16 bits are general and apply to all object types. The lower 16 bits vary between files and directories but are defined in a way that allows most applications to apply the same bits for files and directories. Rights grant or deny access for a given trustee. User access can be blocked explicitly through a deny ACE or implicitly by ensuring that a user does not directly, or indirectly through a group, appear in an ACE that grants the right.

6.3.2 Role Based Access Control

Related SFRs: FDP_ACC.1(2), FDP_ACF.1(2)

38 Role based access control (RBAC) is used to grant the right to perform particular administrative actions to authenticated users. Roles are created by a Security Administrator, assigned privileges, and then assigned members. There are three built-in roles relevant to the security claims: SecurityAdmin, SystemAdmin, and AuditAdmin. Administrators with sufficient privileges are also able to create new roles, with a customized set of privileges. During installation, a root user account is created with the privileges of all roles.

39 Only the root user and users in administrative roles can log in to the WebUI, REST API applications or the CLI. Using roles, the root and admin users can assign others to built-in or custom roles that have login and administrative privileges to perform specific administrative tasks. Table 13 provides a general description of the privileges associated with the built-in roles.

Table 13: Roles and Privileges

Role	Privileges
SecurityAdmin	The SecurityAdmin role has the required privileges to perform security configuration on the cluster, configuration of local users and groups, and assignment of role membership.
SystemAdmin	The SystemAdmin role has the required privileges to perform all cluster configuration tasks that are not specifically handled by the SecurityAdmin role.
AuditAdmin	The AuditAdmin role has the required privileges to view all system configuration settings.

6.3.3 Access Zones

Related SFRs: FDP_ACC.1(3), FDP_ACF.1(3)

40 Using Access Zone features, administrators can partition a cluster into multiple virtual containers. The use of Access Zones allows an organization to isolate data, and control which users can access data in each zone.

41 When an Access Zone is created, it is associated with a base directory (e.g. /ifs/Department A) and assigned a Groupnet. A Groupnet is a top-level networking container that manages DNS client connection settings and contains subnets and IP address pools. Clients can connect to this zone only when coming from IP addresses in this pool.

42 A user must also have access in accordance with the Data Path SFP in order to access objects in the Access Zone.

6.3.4 Data Retention

Related SFRs: FDP_RET_EXT.1

43 Dell PowerScale OneFS v9.5 Smartlock protects files on a Dell PowerScale OneFS v9.5 cluster from being modified, overwritten, or deleted. Organizations can identify a directory in PowerScale as a Write Once, Read Many (WORM) domain. All files within the WORM domain can be committed to a WORM state, meaning that those files cannot be overwritten, modified, or deleted. After a file is removed from a WORM state, it may be deleted. However, a file that has been committed to a WORM state can never be modified or overwritten, even after it is removed from a WORM state.

44 A retention period is the length of time that a file remains in a WORM state before being released from a WORM state. An administrator can configure SmartLock directory settings that enforce default, maximum, and minimum retention periods for the directory. If a file is committed manually, the administrator can specify the date that the file is to be released from the WORM state. Files are released from the WORM state once the retention period has expired, or the release date has passed. The minimum or maximum retention period will take precedence over the manually set release date in the case of a conflict.

6.3.5 Data Integrity Monitoring and Correction

Related SFRs: FDP_SDI.2

45 Data integrity protection in PowerScale is modelled on the Reed-Solomon algorithm, which uses forward error correction (FEC). Using FEC, PowerScale allocates data in 128KB chunks. For each N data chunk, PowerScale writes M protection, or parity, chunks. Each N+M chunk, referred to as a protection group, is written on an independent disk in an independent node. This process is referred to as data striping. By striping data across the entire cluster, PowerScale is able to recover files in cases where drives or nodes fail.

6.4 Identification and Authentication

Related SFRs: FIA_UAU.1, FIA_UID.1

46 Prior to identification and authentication, administrators have no access to TOE data or functionality through the WebUI, CLI or REST API interfaces. The only access to TOE data prior to login is through the front panel, which requires physical access to the TOE hardware. From the Liquid Crystal Display (LCD) screen front panel, administrators may view node status, events, cluster details, capacity, throughput, and drive status. In the evaluated configuration, only local authentication is supported for administrative users. Dell PowerScale OneFS v9.5 ensures that administrative users are authenticated by the configured authentication provided for that user account prior to allowing access to TOE data and functions.

6.5 Security Management

Related SFRs: FMT_SMF.1, FMT_SMR.1

47 The Dell PowerScale OneFS v9.5 cluster can be managed through the WebUI, the CLI or a REST API application.

48 Table 14 shows the security management privileges associated with the built-in roles. Security management privileges can be associated with custom roles in combinations determined by a user with the SecurityAdmin role.

Table 14: Roles and Privileges

Role	Privileges
SecurityAdmin	view audit information configure users and roles
SystemAdmin	view audit information configure SmartLock retention periods configure SyncIQ data replication configure access banners
AuditAdmin	configure SmartLock retention periods (read-only) configure SyncIQ data replication (read-only)
Root	Includes the privileges of all roles.

6.5.1 Data Path

Related SFRs: FMT_MSA.1, FMT_MSA.3(1)

49 For the Data Access SFP, the subject attributes are provided by the operating system, and cannot be modified using Dell PowerScale OneFS v9.5 administrative functions. The default values for the object attributes are the ACL or POSIX mode bits on the file or directory. The root user may change the default value, query, modify, and delete all of these attributes. Administrators in the SystemAdmin role may query POSIX mode bits and change the default value, query, modify and delete ACLs on SMB shares. Administrators in the SecurityAdmin role can only query POSIX mode bits.

50 The default value of these attributes may be considered to be permissive, in that the file owner is able to determine their values. The file owner may also change the default values. Default values may be determined by the directory in which the object is created.

51 Modification of Data Access attributes by Dell PowerScale OneFS v9.5 administrators is performed using the CLI.

6.5.2 Role Based Access Control

Related SFRs: FMT_MSA.1(2), FMT_MSA.3(2)

52 For the Role Based Access Control SFP, the user role attribute may be queried, modified or deleted by the root user, a user in the SecurityAdmin role, or a custom role with sufficient permissions. The default values for ‘role’ may be considered to be restrictive in that a user does not have a role until specifically assigned by an administrator.

6.5.3 Access Zones

Related SFRs: FMT_MSA.1(3), FMT_MSA.3(3)

53 For the Access Zone SFP, the Groupnet and Access Zone may be queried, modified or deleted by the root user, a user in the SecurityAdmin role, or a custom role with sufficient privileges. The default value for ‘Groupnet’ and ‘Access Zone’ may be considered to be restrictive in that no value is present until assigned by an administrator. The IP address is determined by the network configuration, and is not modifiable under the Access Zone SFP.

6.6 Protection of the TSF

6.6.1 Automated Recovery

Related SFRs: FPT_RCV.3

54 The Dell PowerScale OneFS v9.5 cluster is designed to continuously serve data, even in the case of multiple component failure. PowerScale ensures data availability by striping or mirroring data across the cluster. If a cluster component fails, data stored on the failed component is available on another component. After a component failure, lost data is restored on healthy components.

55 PowerScale uses an Dell PowerScale OneFS v9.5 cluster's internal network to distribute data automatically across individual nodes and disks in the cluster. Before writing files to storage, PowerScale breaks files into smaller logical chunks called stripes. The size of each file chunk is referred to as the stripe unit size. Each PowerScale block is 8 KB, and a stripe unit consists of 16 blocks, for a total of 128 KB per stripe unit. During a write, PowerScale breaks data into stripes and then logically places the data into a stripe unit. As PowerScale writes data across the cluster, PowerScale fills the stripe unit and protects the data according to the number of writable nodes and the specified protection policy.

56 In the case of a component failure, a constant, secure state is maintained where the Dell PowerScale OneFS v9.5 cluster continues to respond to requests to read and write data. Under normal operating conditions, all data on the cluster is protected against one or more failures of a node or drive. However, if a node or drive fails, the cluster protection status is considered to be in a degraded state until the data is protected by PowerScale again. PowerScale reprotects data by rebuilding data in the free space of the cluster. While the protection status is in a degraded state, data is more vulnerable to data loss.

6.6.2 Timestamps

Related SFRs: FPT_STM.1

57 In the evaluated configuration, time is synchronized with the underlying hardware to ensure that all components in the TOE and its operational environment are providing a consistent time. This time is used to provide reliable timestamps to TOE functions, such as the generation of audit records.

6.6.3 Replication

Related SFRs: FPT_TRC.1

58 Data can be replicated from one Dell PowerScale OneFS v9.5 cluster to another using SyncIQ functionality. SyncIQ creates and references snapshots to replicate a consistent point-in-time image of a source directory. Metadata such as access control lists are replicated along with data. SyncIQ is used to maintain a consistent replica of the data on another Dell PowerScale OneFS v9.5 cluster and to control the frequency of data replication. SyncIQ also provides automated failover and failback capabilities to continue operations on the secondary Dell PowerScale OneFS v9.5 cluster when the primary cluster becomes unavailable.

59 Data replication is coordinated according to replication policies and replication jobs. Replication policies specify what data is replicated, where the data is replicated to, and how often the data is replicated. Replication jobs are the operations that replicate data from one Dell PowerScale OneFS v9.5 cluster to another. SyncIQ generates replication jobs according to replication policies. Data replication procedures ensure that no modifications are made to the data as it is replicated.

60 A replication policy specifies two clusters: the source and the target. The cluster on which the replication policy exists is the source cluster. The cluster that data is being replicated to is the target cluster. When a replication policy starts, SyncIQ generates a replication job for the policy. When a replication job runs, files from a directory tree on the source cluster are replicated to a directory tree on the target cluster. These directory trees are known as source and target directories. After the first replication job created by a replication policy finishes, the target directory and all files contained in the target directory are set to a read-only state, and can be modified only by other replication jobs belonging to the same replication policy.

61 Data failover and recovery are initiated manually by an administrator. When a failed node is recovered, it is synchronized with the alternate node in accordance with the replication policy. In the evaluated configuration, the replication policy must be configured to replicate immediately on reconnection.

6.7 TOE Access

6.7.1 Access Banner

Related SFRs: FTA_TAB.1

62 Administrators will see a message prior to login in either the WebUI or CLI. This message identifies the cluster, and can also be customized to display login instructions and warning messages. The information is set on the ‘Cluster Identity’ page on the WebUI.

6.7.2 Service Access

Related SFRs: FTA_SAC_EXT.1

63 All data/protocol services are disabled by default. In the evaluated configuration, administrators must manually enable the claimed data path protocols (HDFS, NFS, and SMB).

64 Only the services required for administration are open by default, which includes the HTTPS and SSH services/channels required by the WebUI, REST API, and CLI.

6.8 Trusted Path/Channel

Related SFRs: FTP_TRP.1, FPT_ITT.1

6.8.1 WebUI and REST API Communications

65 All communications with remote administrators via the WebUI and REST API are protected using TLSv1.2. The following default cipher suites are supported in the evaluated configuration:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

6.8.2 CLI Communications

66 When the CLI is used, the connection between the Dell PowerScale OneFS v9.5 node and the remote administrator is protected from modification and disclosure using SSHv2. The TOE supports both password and publickey-based authentication. The following algorithms are supported in the evaluated configuration:

Publickey Algorithms: rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256.

Encryption Algorithms: aes256-ctr, aes256gcm@openssh.com.

MAC Algorithms: hmac-sha2-256.

Key Exchange Algorithms: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, curve25519-sha256.

6.8.3 Cluster-to-Cluster Communications (SyncIQ)

67 Cluster-to-cluster communications are protected using TLSv1.2. The following cipher suites are supported in the evaluated configuration:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

7 Rationale

7.1 Security Objectives Rationale

68 Table 15 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 15: Security Objectives Mapping

	T. ACCOUNT	T.EAVES	T. AVAIL	T.DISCLOSURE	T. UNAUTH	T. UNDETECT	P. RETAIN	A. AUTH	A. LOCATE	A. MANAGE
O.ACCESS					X					
O.ADMIN	X									
O.AUDIT						X				
O.BANNER	X									
O.CRYPTO				X						
O.IDENTAUTH	X									
O.INTEGRITY			X							
O.PROTCOMMS		X								
O.PROTECT	X				X					
O.RETAIN							X			
O.TIME						X	X			
OE.ADMIN										X
OE.PHYSICAL									X	
OE.USERAUTH								X		

69 Table 16 provides the justification to show that the security objectives are suitable to address the security problem.

Table 16: Suitability of Security Objectives

Element	Justification
T.ACCOUNT	**O.ADMIN** mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized users. **O.BANNER** mitigates the threat of access by user error by allowing a clear message related to authorized access to be displayed prior to login. **O.IDENTAUTH** mitigates the threat by providing the means for users to authenticate prior to gaining access to the functions assigned to that user. **O.PROTECT** mitigates this threat by disabling access to the TOE services that should not be in use.
T.DISCLOSURE	**O.CRYPTO** mitigates the threat by protecting TOE against potential disclosure of the data it has been entrusted to store.
T.EAVES	**O.PROTCOMMS** mitigates this threat as it requires the TOE to encrypt communications with remote administrators, and cluster-to-cluster communications.
T.AVAIL	**O.INTEGRITY** mitigates this threat by protecting the integrity of user data from corruption, or hardware loss.
T.UNAUTH	**O.ACCESS** mitigates this threat by ensuring that only authorized users are permitted access to user data, and users may be further restricted based on access zones. **O.PROTECT** mitigates this threat by allowing unused services to be disabled, providing fewer paths for unauthorized users to reach the data.
T.UNDETECT	**O.AUDIT** mitigates the threat by ensuring that audit records are generated for security relevant events. **O.TIME** supports the O.AUDIT objective by providing accurate time to those audit records.
P.RETAIN	**O.RETAIN** supports this policy by preventing the accidental deletion of data, thereby ensuring that the data is retained in accordance with policy. **O.TIME** supports O.RETAIN by providing reliable time in support of this function.
A.AUTH	**OE.USERAUTH** supports this assumption by ensuring that identification and authentication of users is provided by the operational environment.

Element	Justification
A.LOCATE	**OE.PHYSICAL** supports this assumption by ensuring that the operational environment provides physical and logical protection of the TOE.
A.MANAGE	**OE.ADMIN** supports this assumption by ensuring the availability of trained, competent administrators who are trustworthy and not malicious.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

70 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 17: Security Requirements Mapping

	O. ACCESS	O. ADMIN	O. AUDIT	O. BANNER	O. CRYPTO	O. IDENTAUTH	O. INTEGRITY	O.PROTCOMMS	O. PROTECT	O. RETAIN	O. TIME
FAU_GEN.1			X								
FAU_SAR.1			X								
FCS_COP.1					X						
FDP_ACC.1(1)	X										
FDP_ACC.1(2)	X										
FDP_ACC.1(3)	X										
FDP_ACF.1(1)	X										
FDP_ACF.1(2)	X										
FDP_ACF.1(3)	X										
FDP_RET_EXT.1										X	
FDP_SDI.2							X				

	O. ACCESS	O. ADMIN	O. AUDIT	O. BANNER	O. CRYPTO	O. IDENTAUTH	O. INTEGRITY	O.PROTCOMMS	O. PROTECT	O. RETAIN	O. TIME
FIA_UAU.1						X					
FIA_UID.1						X					
FMT_MSA.1(1)		X									
FMT_MSA.1(2)		X									
FMT_MSA.1(3)		X									
FMT_MSA.3(1)		X									
FMT_MSA.3(2)		X									
FMT_MSA.3(3)		X									
FMT_SMF.1		X									
FMT_SMR.1		X									
FPT_ITT.1								X			
FPT_RCV.3							X				
FPT_STM.1											X
FPT_TRC.1							X				
FTA_TAB.1				X							
FTA_SAC_EXT.1									X		
FTP_TRP.1								X			

Table 18: Suitability of SFRs

Objectives	SFRs
O. ACCESS	**FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACC.1(3), FDP_ACF.1(1), FDP_ACF.1(2), FDP_ACF.1(3)** ensures that only authorized users are able to access data resources protected by the TOE.
O. ADMIN	**FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3)** ensure that access to the security attributes supporting access control functions is restricted to authorized Management path users. **FMT_MSA.3(1), FMT_MSA.3(2), FMT_MSA.3(3)** ensures that default values for the security attributes that make up that TSF data are permissive. **FMT_SMF.1** provides security management functionality to support storage configuration, viewing of audit records, user management, access control, enabling/disabling D@RE and retention period and policy management. **FMT_SMR.1** provides the security roles for Management path users.
O. AUDIT	**FAU_GEN.1** outlines what data must be included in audit records and what events must be audited. **FAU_SAR.1** provides the means to review audit records.
O. BANNER	**FTA_TAB.1** supports this objective by displaying an advisory warning message regarding unauthorised use of the TOE.
O. CRYPTO	**FCS_COP.1** supports this objective by providing cryptographic operations that secure data stored on the TOE.
O. IDENTAUTH	**FIA_UAU.1** meets this objective by ensuring that TOE Administrators are successfully authenticated before gaining access to TOE functions and data. **FIA_UID.1** supports this objective by ensuring that the identity of each TOE user is known before allowing access to TOE functions and data.
O. INTEGRITY	**FDP_SDI.2** monitors the stored data for integrity errors and rebuilds the data if an error is detected. **FPT_ITT.1, FPT_TRC.1** provides data replication procedures that ensure availability and integrity of the data. **FPT_RCV.3** provides automated recovery of the data in case of component failure.

Objectives	SFRs
O. PROTCOMMS	**FPT_ITT.1** requires cluster-to-cluster encrypted communications. **FTP_TRP.1** requires encrypted communications for remote administration.
O. PROTECT	**FTA_SAC_EXT.1** supports this objective by disabling unused services on the TOE.
O. RETAIN	**FDP_RET_EXT.1** ensures that data is not deleted prior to the expiry of the retention period.
O. TIME	**FPT_STM.1** satisfies this objective by providing reliable time stamps.

Table 19: Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met
FAU_SAR.1	FAU_GEN.1	Met
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Not met, as it is not required to be met by CCCS policy.
	FCS_CKM.4	
FDP_ACC.1(1)	FDP_ACF.1	Met
FDP_ACC.1(2)	FDP_ACF.1	Met
FDP_ACC.1(3)	FDP_ACF.1	Met
FDP_ACF.1(1)	FDP_ACC.1	Met
	FMT_MSA.3	Met
FDP_ACF.1(2)	FDP_ACC.1	Met
	FMT_MSA.3	Met
FDP_ACF.1(3)	FDP_ACC.1	Met
	FMT_MSA.3	Met
FDP_RET_EXT.1	FPT_STM.1	Met
FDP_SDI.2	None	-

SFR	Dependency	Rationale
FIA_UAU.1	FIA_UID.1	Met
FIA_UID.1	None	-
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1(1)
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1(2)
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.1(3)	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1(3)
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.3(1)	FMT_MSA.1	Met by FMT_MSA.1(1)
	FMT_SMR.1	Met
FMT_MSA.3(2)	FMT_MSA.1	Met by FMT_MSA.1(2)
	FMT_SMR.1	Met
FMT_MSA.3(3)	FMT_MSA.1	Met by FMT_MSA.1(3)
	FMT_SMR.1	Met
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	Met
FPT_ITT.1	None	-
FPT_RCV.3	AGD_OPE.1	Met
FPT_STM.1	None	-
FPT_TRC.1	FPT_ITT.1	Met
FTA_TAB.1	None	-
FTA_SAC_EXT.1	None	-

SFR	Dependency	Rationale
FTP_TRP.1	None	-