NetApp Element Software 12.2

on SolidFire Appliances

Security Target

Evaluation Assurance Level (EAL): EAL 2+

Document Version 1.0
March 2022

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	8 Mar 2022	G Nickel	Release for Certification

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the NetApp Element Software 12.2 on SolidFire Appliances Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 NetApp Element Software 12.2 is an Operating System (OS) for nodes within a SolidFire Storage System – a scale-out, all-flash, highly-available clustered storage system. A cluster (see Figure 1) is made up of a collection of nodes that provide data storage and management. Each cluster of the storage system is scalable from 4-40 independent nodes providing 80 TB to over 3 PB of capacity.

Figure 1: Typical SolidFire Cluster

3 Each self-contained storage node is built on standard hardware, houses multiple SSDs, runs the Element Software 12.2, and is connected to other nodes in the cluster through a 10/25 GbE network. To iSCSI clients, a cluster appears on a storage network as a single logical group, represented by a virtual IP (VIP) address that can be accessed as block storage (volume).

4 Each volume within a cluster can be allocated with an exact amount of capacity and performance, which can be separately controlled. In this way performance can be managed independently of capacity. Nodes can be added or removed non-disruptively with automatic load balancing of data across the cluster, and high availability is provided with Elements Helix™ RAID-less data protection. These features allow for linear, predictable performance gains as the system grows, despite failure conditions.

5 Other features incorporated into the Storage System include data reduction techniques like de-duplication, compression, and thin provisioning to increase efficiency and enhance performance.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	NetApp Element Software 12.2 on SolidFire Appliances Build: 12.2.0.777
Security Target	NetApp Element Software 12.2 on SolidFire Appliances Security Target, v1.0
Evaluation Assurance Level	EAL2+

1.3 Conformance Claims

6 This ST supports the following conformance claims:

a) CC version 3.1 release 5

b) CC Part 2 conformant

c) CC Part 3 conformant

d) EAL2 augmented (ALC_FLR.2)

1.4 Terminology

Table 2: Terminology

Term	Definition
API	Application Programming Interface
CC	Common Criteria
CHAP	Challenge-Handshake Authentication Protocol
EAL	Evaluation Assurance Level
GB	Gigabyte
GbE	Gigabit Ethernet
GHz	Gigahertz
Group Snapshot	TOE users can create a group snapshot of a related set of volumes to preserve a point-in-time copy of the metadata for each volume. TOE users can use the group snapshot in the future as a backup or rollback to restore the state of the group of volumes to a desired point in time.
Helix™	NetApp's Helix data protection is a distributed replication algorithm that spreads redundant copies of data for single disk throughout all the other disks in the cluster.
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface - an IP-based storage networking standard for linking data storage facilities. It provides block-level access to storage devices by carrying SCSI commands over a TCP/IP network.
iSCSI Client / Initiator	A consumer of storage that sends SCSI commands over an IP network (available with most popular operating systems).
IQN	iSCSI Qualified Name – a unique identifier for iSCSI devices.

Term	Definition
JSON-RPC	JavaScript Object Notation – Remote Procedure Call (API protocol used by the TOE)
LDAP	Lightweight Directory Access Protocol
MIP	Management IP
MVIP	Management Virtual IP
NetApp Hybrid Cloud Control	The new SolidFire UI. References to “Node UI” in this document are used to represent NetApp Hybrid Cloud Control.
NTP	Network Time Protocol
OS	Operating System
PB	Petabyte
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SFP	Security Function Policy
SIP	Storage IP (related to SVIP)
Snapshot / Volume Snapshot	A volume snapshot is a point-in-time copy of a volume. TOE users can use snapshots to roll a volume back to the state it was in at the time the snapshot was created.
SSD	Solid State Drive
SVIP	Storage Virtual IP - single point of access for all initial iSCSI connections. The SVIP is logically located on a node identified as a “cluster master”. The node holding the cluster master role can change as a cluster operates. Upon this initial iSCSI connection to the SVIP, the cluster master sends an iSCSI redirect back to the client indicating a specific node’s SIP that the client will use going forward for storage traffic to that specific volume.
TB	Terabyte
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality

Term	Definition
TUI	Text User Interface
VIP	Virtual IP
Volume	The TOE provisions storage using volumes. Volumes are block devices accessed over the network by iSCSI clients.
Volume AG	Volume Access Group - provide access control between a list of clients and an associated group of volumes.

2 TOE Description

2.1 Type

7 The TOE is a data storage system.

2.2 Usage

8 The TOE functions in a standalone SolidFire cluster of storage nodes (each an instance of the TOE) that are used as shown in Figure 2.

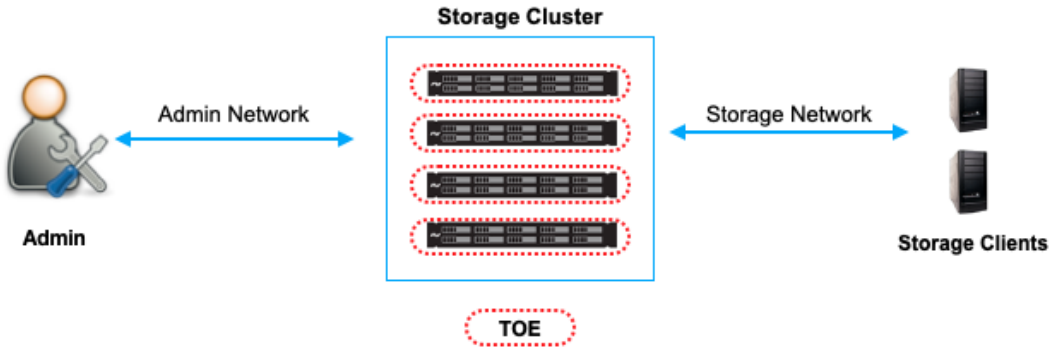

Figure 2: TOE Usage Scenario

9 The core components of a NetApp SolidFire Storage System are as follows:

a) **Cluster.** A minimum of four storage nodes in a cluster is required to create a functional NetApp SolidFire Storage System. A cluster appears on the network as a single logical group and can then be accessed as block storage by iSCSI clients.

b) **Storage node.** A storage node is a hardware appliance that contains a collection of drives that communicate with each other. Drives in the node contain block and metadata space for data storage and data management.

2.2.1 TOE Administration

10 Within a cluster, a master node is assigned for cluster-level management via WebUI or Element API (JSON-RPC) over HTTPS. The cluster master is assigned a management VIP (MVIP). Each node also has a limited UI (called the Node UI) and a node-level API that listens on a separate

port accessible by the individual node's management IP address (MIP). An attempt to access the cluster-level Web UI or API on an individual node's MIP will redirect the browser to the cluster's MVIP.

11 A Text User Interface (TUI) is accessible via console cable directly connected to the TOE to initially configure nodes and prepare them for establishing a cluster (i.e. initial system deployment). Further use of the TUI in the evaluated configuration is limited to scenarios where the Node UI is inaccessible. More information on the TUI can be found in the NetApp Element Software 12.2 on SolidFire Appliances Common Criteria Guide (see section 2.4.1).

2.3 Security Functions

12 The TOE provides the following security functions:

a) **Volume Access Control.** The TOE enforces an administrator defined access control policy governing client access to Storage System volumes.

b) **Volume Rollback.** The TOE provides volume snapshot capabilities, allowing for the rollback of a volume to the point-in-time a chosen snapshot was created.

c) **Data Protection.** The TOE detects and automatically recovers when multiple drive failures occur on the same node or a node failure occurs. The TOE automatically re-replicates data across all other nodes and drives in the cluster should a node or drive go offline for more than 5½ minutes.

d) **Secure Administration.** The TOE enforces authentication of administrators, enables management of its security functions and protects remote administrator communications.

e) **Security Audit.** The TOE keeps audit records of security relevant events.

f) **Self-tests.** The TOE provides a suite of self-tests to ensure correct operation of the security functions.

2.4 Physical Scope

13 The physical boundary of the TOE is the Element Software 12.2 executing on the SolidFire Appliances identified in section 2.4.2. The TOE is delivered via commercial courier.

2.4.1 Guidance Documents

14 The TOE includes the following guidance documents (available in PDF format):

a) NetApp Element Software 12.2 on SolidFire Appliances Common Criteria Guide, v1.0

b) NetApp Element 12.2 Setup Guide, 215-15135_2020-12_en-us
https://docs.netapp.com/sfe-122/topic/com.netapp.doc.sfe-sg/home.html

c) NetApp Element 12.2 User Guide, 215-15136_2021-06_en-us
https://docs.netapp.com/sfe-122/topic/com.netapp.doc.sfe-ug/home.html

d) NetApp Element 12.2 API Reference Guide, 215-15139_2020-11_en-us
https://docs.netapp.com/sfe-122/topic/com.netapp.doc.sfe-api/home.html

e) NetApp Element 12.2 Release Notes
https://docs.netapp.com/sfe-122/topic/com.netapp.doc.sfe-rn/GUID-D85AC3C1-460C-4E12-9689-FA5A284038EC.html

f) NetApp H-Series Hardware – Installing and Setting up the H-series Storage Nodes, 215-14250_2020-06_en-us, June 2020
https://docs.netapp.com/sfe-122/topic/com.netapp.doc.sfe-isg/home.html

g) NetApp SF-Series Hardware – Installing and Setting up the SF-Series Hardware https://docs.netapp.com/sfe-122/index.jsp?topic=%2Fcom.netapp.ndc.hsf%2FGUID-39CA8195-1048-469F-BB80-7F9F5FCC2247.html

2.4.2 TOE Hardware Devices

15 The TOE includes the nodes shown in Table 3. All of nodes run the same software with differences being the CPU, memory, and drive sizes.

Table 3: TOE Hardware Devices (Nodes)

Model	Manufacturer	Processor
SF4805	Dell	Intel Xeon E5-2620 v4, 2.10 GHz (Broadwell)
SF9605	Dell	Intel Xeon E5-2650 v4, 2.20 GHz (Broadwell)
SF19210	Dell	Intel Xeon E5-2697 v3, 2.60 GHz (Haswell)
SF38410	Dell	Intel Xeon E5-2697 v3, 2.60 GHz (Haswell)
H410S-0 H410S-1 H410S-2	NetApp	Intel Xeon E5-2695 v4, 2.10 GHz (Broadwell)
H610S-1 H610S-2 H610S-2F H610S-4	NetApp	Intel Xeon Gold 5120, 2.20 GHz (Skylake)

2.5 TOE Environment

16 The deployed configuration of the TOE is shown in Figure 3 (does not show routers, switches, firewalls or other infrastructure that are present in an enterprise network environment). A cluster can incorporate any of the TOE nodes shown in Table 3.

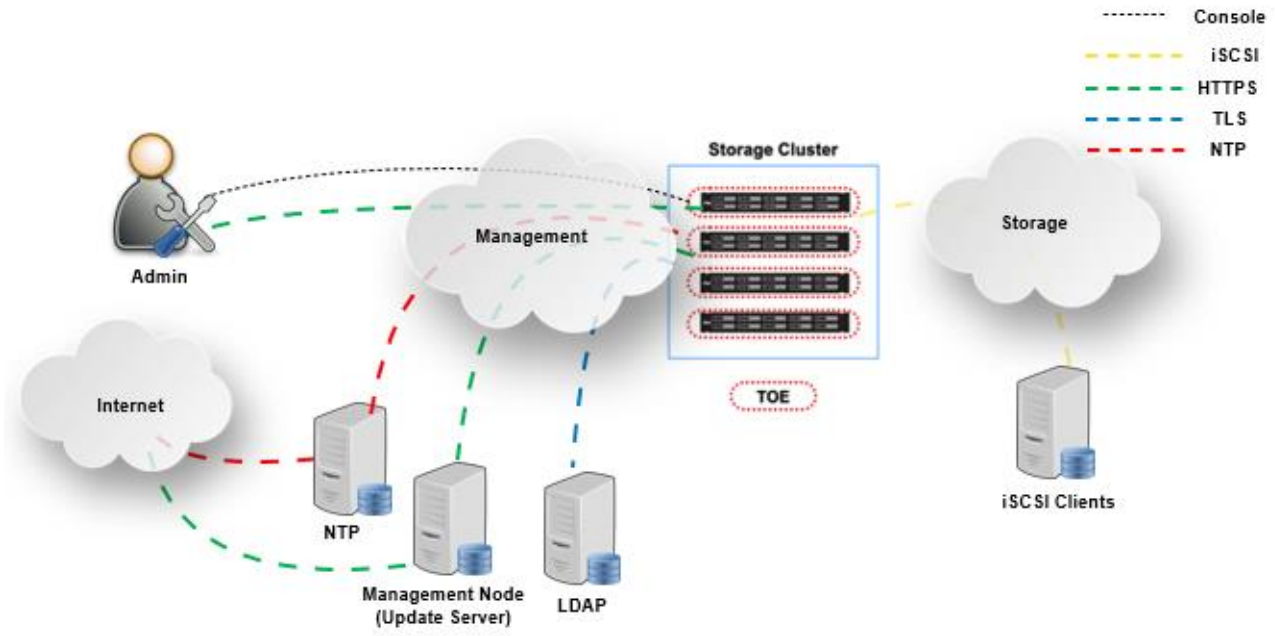

Figure 3: TOE & Environment

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

a) **Element Software Management Node.** Virtual node that is used to perform software updates on cluster nodes.

b) **LDAP Server.** Provides LDAP services for authentication.

c) **NTP Server**. For cluster time synchronization.

d) **iSCSI clients.** Used to connect to the cluster.

2.6 Logical Scope

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

2.6.1 Excluded Functions

19 Element Software 12.2 on SolidFire Appliances provides other security features that are out of the scope of the TOE. The following features are not included in the TOE and will not be evaluated:

a) Encryption At Rest – Encryption is used to encrypt data on SSDs (not enabled by default).

b) Integrated Backup and Restore – volumes are backed up to and restored from external object stores.

c) Remote Replication – an asynchronous process is used to connect two clusters for continuous data protection.

d) Remote Syslog – audit data is forwarded to a remote syslog server.

e) Deduplication – multiple copies of data are replaced with references to a shared copy in order to save storage space and/or bandwidth.

f) Quality of Service (QoS) – guaranteed performance is provided by setting minimum, maximum, and burst parameters for volumes.

g) SSH – the SSH protocol used for remote support of a customer's system.

h) SNMP– the SNMP protocol is used to generate SNMP traps, or notifications, associated with audit events (not enabled by default).

i) Multiple VLANs - multi-tenant environment connection to a cluster.

2.7 TOE Delivery

20 TOE software may be delivered in any of the following ways:

a) Pre-installed on TOE hardware

b) Downloaded from the NetApp support portal

21 TOE hardware is shipped to the customer using a commercial carrier.

22 TOE guidance documents may be downloaded from the NetApp support portal.

3 Security Problem Definition

3.1 Threats

23 Threat agents are divided into three categories:

a) **Attackers who are not TOE users.** Attackers have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.

b) **TOE administrator users.** Users in charge of administration of the TOE that have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE (TOE administrators are, however, assumed not to be willfully hostile to the TOE).

c) **iSCSI clients.** Users of the TOE functionality that have access to the TOE and could attempt to bypass its protection mechanisms for access to another user's data.

24 All threat agents are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE.

Table 4: Threats

Identifier	Description
T.DATA_CORRUPTION	Data could become corrupted or security functionality compromised due to hardware failure or incorrect system access by iSCSI clients or attackers.
T.UNAUTH	An administrator with Reporting privileges may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy, resulting in a compromise of TSF or User data.

Identifier	Description
T.UNINTENDED_ACCESS	An attacker and user of the TOE functionality (iSCSI client) could access storage volumes they are not authorized to access, resulting in a compromise of TSF or User data.
T.MGMT_NET	An attacker intercepts remote administrator traffic compromising the integrity and/or confidentiality of TSF data in transit.

3.2 Assumptions

Table 5: Assumptions

Identifier	Description
A.TIME	The IT environment provides the TOE with the necessary reliable time.
A.LOCATE	The TOE, the storage nodes, storage clients, switches, storage and management networks, and NTP and LDAP servers are located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The administrator users with Administrator privileges who manage the TOE are non-hostile, appropriately trained, and follow all guidance. Administrators will never accept unknown/untrusted certificates for the web communication with the TOE.
A.ADMIN_PROTECT	No malicious software is installed or running on the administrator workstation.
A.CLUSTER_NET	The cluster network is protected from unauthorized access.

3.3 Organizational Security Policies

25 There are no Organizational Security Policies (OSPs) imposed upon the TOE or its operational environment.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 6: Security Objectives for the Operational Environment

Identifier	Description
OE.TIME	The TOE environment must provide reliable time to the TOE via an NTP server.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.ADMIN_PROTECT	The administrator workstation must be protected from any external interference or tampering.
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.
OE.CLUSTER_PROTECT	The TOE environment must protect the cluster network from unauthorized access.

4.2 Objectives for the TOE

Table 7: Security Objectives

Identifier	Description
O.AUDIT	The TOE must record security relevant events and associate each API event with the identity of the administrator that caused the event. The TOE must prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide authorized administrators with the ability to review the audit trail.
O.ACCESS	The TOE must implement rules to govern iSCSI client access to stored user data.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.
O.AUTHENTICATE	The TOE must be able to identify and authenticate administrators through multiple authentication mechanisms prior to allowing any access to TOE administrative functions and TSF data. An administrator's security attributes must be associated with every API and Web UI management action.
O.USER_DATA_PROTECT	The TOE must ensure the integrity of stored user data by monitoring for errors and providing the means for an authorized administrator to restore a volume (of user data) to a desired point- in-time.

Identifier	Description
O.TSF_PROTECT	The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when drive or node failures occur. It also must provide for the ability to check that its nodes are operating correctly.
O.MGMT_PROTECT	The TOE must protect the confidentiality and integrity of communications with remote administrators.

5 Security Requirements

5.1 Conventions

26 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) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

27 No extended components are defined.

5.3 Functional Requirements

Table 8: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ROL.1	Basic rollback

Requirement	Title
FDP_SDI.2	Stored data integrity monitoring and action
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
FIA_USB.1	User subject binding
FMT_MOF.1	Management of security function behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FPT_STM.1	Reliable time stamps
FRU_FLT.1	Degraded fault tolerance
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[1];

[1] *ST Author Note:* Start-up and shutdown of the audit service is intrinsically tied to the start-up and shutdown of the system itself and its core services.

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

c) *[APIEvent, ServiceEvent, PlatformHardwareEvent, DriveEvent].*

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, [*Event ID, Message, Service ID, Node ID, Drive ID].*

FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note: ServiceEvent, PlatformHardwareEvent, and DriveEvent are not intended to be a success/fail operation; they are generated when system events occur. Therefore, there will not be a success or failure indication for these events.

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 [*Administrator and Reporting users*] with the capability to read [*all audit information for the APIEvent, ServiceEvent, PlatformHardwareEvent, DriveEvent, and start-up and shutdown events*] 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.

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

5.3.2 Cryptographic Support (FCS)

FCS_COP.1 Cryptographic operation

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 [*operations in Table 9*] in accordance with a specified cryptographic algorithm [*shown in Table 9*] and cryptographic key sizes [*shown in Table 9*] that meet the following: [*standards shown in Table 9*].

Table 9: Cryptographic Operations

Operation	Algorithm	Key Size	Standard	CAVP Cert.
Encryption / Decryption	AES CBC	128, 256	ISO 18033-3, ISO 10116	A950 C2114
	AES GCM	256	ISO 18033-3, ISO 19772	
Signature Generation	RSA	2048	FIPS PUB 186-4	
Hash	SHA-1, 256, 384	-	ISO/IEC 10118-3:2004	
Keyed Hash	HMAC-SHA-1, 256, 384	160, 256, 384	ISO/IEC 9797-2:2011, Section 7	
Key Agreement	ECDH	P-256	NIST SP 800-56A	
	DH	2048	NIST SP 800-56A	n/a

5.3.3 User Data Protection (FDP)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

- *Subjects: iSCSI clients*
- *Objects: Volumes*
- *Operations: Read and Write*].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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

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

a) iSCSI client SFP-relevant security attributes:

- *IQN*
- *Username for CHAP authentication (i.e., account name defined on volume)*
- *Initiator Secret for CHAP authentication*
- *Access control record (for CHAP target authentication)*

b) Volume SFP-relevant security attributes:

- *Target Secret for CHAP authentication*
- *Volume AG*
- *Volume ID*
- *Account Name (i.e., iSCSI client username)*
- *Access control record (for CHAP initiator authentication)].*

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 iSCSI client can access a volume to perform read/write operations if 1) CHAP authentication is successful or 2) its IQN is in the Volume AG defined for the volume*].

FDP_ACF.1.3 The TSF shall explicitly authorize 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 [*no other rules*].

FDP_ROL.1 Basic rollback Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ROL.1.1 The TSF shall enforce [*Storage Access Control SFP*] to permit the rollback of the [*modifications*] on the [*data located in storage volumes*].

FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [*period of time since a chosen snapshot was created*].

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: [*checksum associated with the data*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*stop the block service on which the data is located, repair the data from a known good copy, re-replicate the data by distributing it across the remaining drives and nodes within the cluster, and send an alert viewable via the Alert tab of the Web UI*].

5.3.4 Identification and Authentication (FIA)

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 users: [*username, role, and password for local authentication; LDAP users and groups and associated roles for LDAP authentication*].

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.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide [*local and LDAP authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*username and password provided by user matches that in distributed database (for local authentication) or LDAP (for LDAP authentication)*].

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.

FIA_USB.1 User-subject binding

Hierarchical to: No other components

Dependencies: FIA_ATD.1 User Attribute Definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*credentials provided with API calls, role*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*every API call will be associated with the provided credentials*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*the user's credentials will remain unchanged for the duration of the API call*].

5.3.5 Security Management (FMT)

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to [**perform the actions listed in Table 10 below**] the functions [*listed in Table 10 below*] to [*the roles listed in Table 10 below*].

Table 10: Management of Security Functions

Function	Action	Role
User identification and authentication	Determine the behavior of Modify the behavior of	Administrator
Rollback	Determine the behavior of	Administrator Reporting
	Modify the behavior of	Administrator

Function	Action	Role
Access Controls	Determine the behavior of	Administrator Reporting
	Modify the behavior of	Administrator
Self-tests	Determine the behavior of	Administrator
Auditing	Determine the behavior of	Administrator Reporting

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*Storage Access Control SFP*] to restrict the ability to [query, modify, delete, [*add*]] the security attributes [*CHAP credentials, Volume AG, volume account name (modify only)*] to [*Administrator and Reporting (query only*)].

FMT_MSA.3 Static attribute initialization

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 [*Storage 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 [*Administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to [[*perform the operations listed in Table 11*]] **on** the [*TSF data listed in Table 11*] to [*the roles listed in Table 11*].

Table 11: Management of TSF Data

Operation	TSF Data	Role
Create, Modify, Delete	Volumes, accounts	Administrator
View	Volumes, accounts	Administrator, Reporting
Add, Remove	Drives, nodes	Administrator
View	Drives, nodes	Administrator, Reporting
View	Element Software version	Administrator, Reporting
Modify	Node settings	Administrator
Add, Remove	Volumes and initiators from Volume AG	Administrator
Delete	Volume AG	Administrator
Create, delete	Snapshots, Group snapshots	Administrator
Assign, View, Modify	NTP settings	Administrator
Add, View, Delete	Cluster Admin accounts	Administrator
View	Host Connections (iSCSI sessions)	Administrator, Reporting

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: [*configuring clusters, volumes, and nodes; configuring NTP; viewing the Event logs; configuring user authentication; performing snapshots and rollbacks; setting access controls; running self-tests*].

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 [*Reporting and Administrator*].

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

Application Note: The Administrator role (or access) provides full privileges and is obtained by selecting all access settings when a Cluster Admin account is created: Reporting,

Nodes, Drives, Volumes, Accounts and Cluster-level. The Reporting role is read-only and is obtained by selecting the Reporting access when a Cluster Admin account is created.

5.3.6 Protection of the TSF (FPT)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*1 or more drive failures on the TOE node or a TOE node failure*].

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [during initial start-up, periodically during normal operation, at the request of the authorized user] to demonstrate the correct operation of [*network connectivity, cluster consistency, distributed database*].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [*TSF data stored in the distributed database*].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [*no other parts of the TSF*].

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.

5.3.7 Resource Utilization (FRU)

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1 **The TSF shall ensure the operation of [*availability of user data*] when the following failures occur: [*1 or more drive failures on the TOE node or a TOE node failure*].**

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 **be capable of using HTTPS to** provide a communication path between itself and **authorized** [remote] **administrators ~~users~~** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure, [*and provides detection of modification of the channel data*]].

FTP_TRP.1.2 The TSF shall permit [remote **administrators ~~users~~**] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*initial administrator authentication and all remote administration actions*]].

5.4 Assurance Requirements

28 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	Flaw Reporting Procedures
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction

Assurance Class	Components	Description
	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 Volume Access Control

Related SFRs: FDP_ACC.1, FDP_ACF.1

29 The TOE enforces the Storage Access Control SFP to control iSCSI client access to Storage System volumes. An authorized administrator configures this access by setting security attributes (e.g., CHAP credentials, IQNs, Volume AGs) via the Web UI or API. If these security attributes are not configured, clients have no access to volumes on the Storage System. The TOE enforces access control to hosted volumes using accounts (CHAP authentication) and Volume AGs.

30 For account-based access control, every volume is assigned an account name (i.e., the username of the iSCSI client to whom authorized access will be granted) and associated CHAP credentials. Through an IP connection to the node holding the SVIP, an iSCSI client can access a volume to perform read/write operations if CHAP authentication is successful. For authentication to succeed, the iSCSI client username and password (initiator secret) must match that assigned to the volume. If bidirectional CHAP is configured, then the target (volume) must also authenticate with the initiator (iSCSI client). In this case, the iSCSI client must have a record of the username and password (target secret) for the volume(s) being accessed.

31 Volume AGs provide access control between a list of iSCSI initiator IQNs and an associated group of volumes. Volume AGs may contain volumes from more than one account. Each iSCSI initiator IQN that is added to a Volume AG can securely access each volume in the group without requiring CHAP authentication.

6.2 Volume Rollback

Related SFRs: FDP_ROL.1

32 The TOE provides volume and volume group snapshot capabilities, allowing for the rollback of a volume or volume group to a point-in-time a chosen snapshot was created.

33 Creating a volume snapshot takes only a small amount of system resources and space; this makes snapshot creation faster than cloning. Because snapshots are simply replicas of volume metadata, you cannot mount or write to them.

34 TOE users can create a snapshot of the active volume to preserve the volume image at any point in time. Users can create up to 32 snapshots for a single volume. Rolling back to a previous snapshot reverts any changes made to the volume since the snapshot was created.

35 TOE users can create a group snapshot of a related set of volumes to preserve a point-in-time copy of the metadata for each volume. A single group snapshot can snapshot up to 32 volumes at one time.

6.3 Data Protection

Related SFRs: FDP_SDI.2, FPT_FLS.1, FRU_FLT.1

36 Data storage integrity is provided with Helix data protection, which provides built-in integrity checking and self- healing capabilities. To implement Helix, the TOE operates a block service on every drive to track the location of 4K blocks as they are written to the drive and keep checksums of the data. A 32-bit checksum is pre-pended to data by the block service on a per-block basis using the CRC32 algorithm. This checksum is performed after compression and follows the data through the rest of the system. Before the block service writes data to disk, a 4-byte checksum is added to each compressed data block using the CRC32 algorithm. This checksum is verified whenever the data block is read. The TOE monitors these checksums to check for data integrity errors. If an error is encountered, the TOE will stop the block service on which the data is located, repair the data from a known good copy, re-replicate the data by distributing it across the remaining drives and nodes within the cluster, and send an alert viewable via the Alert tab of the Web UI.

37 The TOE is able to preserve a secure state when one or more drives on the TOE node fail, or the TOE node as a whole fails. The TOE collaborates with other nodes in a cluster (each an instance of the TOE) - TSF data is replicated across the cluster such that drive or node failures do not result in the failure to enforce any SFRs in any given instance of the TOE.

38 In the much the same way the TOE ensures the availability of user data – software algorithms within the TOE (i.e. Helix) prevent two copies of the same data from being stored on the same node and ensures two copies of unique data are always kept on a cluster. Drive and node failures are reported in the Event Log.

6.4 Secure Administration

Related SFRs: FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FCS_COP.1, FIA_UID.2, FIA_USB.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT MTD.1, FMT_SMF.1, FMT_SMR.1, FTP_TRP.1

39 User (administrator) authentication can be performed in multiple ways on the TOE. The TOE supports both local and LDAP authentication.

40 With local authentication, administrators are authenticated using a local password-based mechanism, which authenticates and authorizes them based on their username, password, and role attributes, which are stored in the distributed database. All Web UI, Node UI, and API actions require a valid username and password combination upon invocation. Passwords are passed to the cluster on each API call. No functionality is available to an administrator prior to authentication.

41 For LDAP authentication, the TOE uses an LDAP server in the TOE environment to authenticate administrators. Note that LDAP authentication is only supported at the Web UI and API. The Node UI only supports local authentication.

42 The TOE is managed by authorized administrators in either the Administrator or Reporting role. The same role capabilities apply to both the Web and Node UI and API. The TOE provides Administrator users with the ability to manage security attributes, and TSF data. For example, Administrator users can configure user authentication, run self-tests, and perform rollbacks. They can manage all of the security attributes required to enforce the Storage access control SFP. They are also able to manage TSF data, like creating, modifying, or deleting volumes and accounts or adding and removing volumes and initiators from a Volume Access Group (AG). Default values for the Storage access control SFP are restrictive – no access to a volume is granted unless explicitly defined by an Administrator.

43 The Reporting user has read only access and is able to determine the behavior of security functions and view TSF data. However, Reporting users are explicitly denied access to the Node UI. They are also denied access to the Web UI Cluster Admin tab and parts of the Web UI Cluster Settings tab.

44 The TOE is capable of performing the following management functions: configuring clusters, volumes, and nodes; configuring NTP; viewing the Event logs; configuring user authentication; performing snapshots and rollbacks; setting access controls; and running self-tests.

45 The TOE uses HTTPS to protect communication with remote administrators accessing the Web UI, Node UI and API. The TOE implements TLS v1.2 with support for cipher suites using FIPS approved algorithms.

46 The TOE also provides a Text User Interface (TUI) for initial configuration of nodes to prepare them for joining a cluster. The TUI is only accessible via directly connected console cable and therefore requires physical access to the TOE. Once a node has been joined to a cluster, all node management is performed via the Node UI. Should a node become unresponsive or the Node UI is otherwise unavailable, the TUI can be used to access the node and perform reboot or network configuration functions.

47 Cryptographic functionality is provided by the NetApp Cryptographic Security Module (NCSM).

6.5 Security Audit

Related SFRs: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.4, FPT_STM.1

48 The TOE generates audit records for events initiated by an authorized administrator through the API, Web UI, or Node UI that modify settings, as well as system level events. Authorized administrators can view the audit records in the Event Log through the Web UI or by extracting them with the API; however, they are prevented from deleting the audit records. The audit records for all API events show the identity of the authorized administrator that caused the event.

49 The TOE maintains approximately 4,000 of the most recent log entries, meaning that the oldest records will be discarded once this threshold is reached.

50 The TOE generates audit records for the following event types:

a) APIEvent – Events initiated by an authorized administrator through the API, Web UI, or Node UI that modify settings, authentication failures, and stopping services

b) ServiceEvent – service monitoring events, for example, starting services

c) PlatformHardwareEvent – Events related to issues detected on hardware devices

d) DriveEvent – Events related to drive operations

51 The start-up and shutdown of the audit service is intrinsically tied to the start-up and shutdown of the TOE nodes and their core services. Once a node has fully booted, the appearance of audit messages in the TOE administrative interfaces is implicit of the audit service functionality.

52 The TOE audit records contain the information identified in Table 13.

Table 13: Audit Record Contents

Field	Content
Event ID	Unique ID associated with each event
Event Types	The type of event being logged, for example, API events or Service events
Message	Message associated with the event
Service ID	The service that reported the event (if applicable)
Node ID	The node that reported the event (if applicable)
Drive ID	The drive that reported the event (if applicable)
Details	Information that helps identify why the event occurred
Event Time	The time the event occurred

53 Through a networked connection to an external NTP server, the TOE periodically synchronizes time to an external time source. Once the TOE obtains the time from the NTP server, it maintains this time internally and uses it to provide reliable time stamps for auditing.

6.6 Self-tests

Related SFRs: FPT_TST.1

54 The TOE provides a suite of self-tests that that are run during initial start-up, periodically during normal operation, and at the request of an Administrator user to demonstrate the correct operation of the TOE. The consistency of the cluster and the integrity of the distributed database are checked periodically to ensure that no corruption has occurred.

55 To ensure a node is stable and can be brought online without issues, many tests can be executed by an Administrator user from the System Tests tab of the Node UI. These tests check for proper network connectivity between nodes and to the MVIP and SVIP of the cluster, the consistency of the cluster, and the integrity of the distributed database.

56 During initial startup, network connectivity tests are conducted to ensure cluster consistency and that required nodes are online and communicating correctly.

57 During normal operation, periodic tests (every 30 seconds) are conducted by the management subsystem which send RPC heartbeats to the Slice Services on each node. If a Slice Service does not respond to the heartbeat within 10 attempts (after 5.5 minutes), it will be reported as failed and an alert will be generated in the ZooKeeper database.

58 In addition to the tests described above, when the FIPS feature is enabled, each node will run two self-tests during startup:

a) Expected Failure Verification. This test attempts an MD5 operation that should fail. If it passes (unexpected behavior) a cluster fault and panic condition are raised.

b) Expected Success Verification. This test attempts a SHA1 operation that should pass. If it fails (unexpected behavior) a cluster fault and panic condition are raised.

7 Rationale

7.1 Security Objectives Rationale

59 Table 14 provides a mapping between security objectives, threats, OSPs and assumptions.

Table 14: Security Objectives Mapping

	T.DATA_CORRUPTION	T.UNAUTH	T.UNINTENDED_ACCESS	T.MGMT_NET	A.CLUSTER_NET	A.TIME	A.LOCATE	A.PROTECT	A.MANAGE	A.NOEVIL	A.ADMIN_PROTECT
O.AUDIT	X		X								
O.ACCESS			X								
O.ADMIN		X									
O.AUTHENTICATE		X									
O.USER_DATA_PROTECT	X										
O.TSF_PROTECT	X	X	X								
O.MGMT_PROTECT				X							
OE.TIME						X					
OE.PROTECT	X							X			
OE.ADMIN_PROTECT											X
OE.MANAGE									X	X	
OE.PHYSICAL							X				
OE.CLUSTER_PROTECT					X						

60 Table 15 provides the justification to show that the security objectives are suitable to address the security problem.

Table 15: Suitability of Security Objectives

Element	Justification
T.DATA_CORRUPTION	O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded. O.USER_DATA_PROTECT mitigates this threat by monitoring user data for errors and allowing rollbacks to a point-in-time. O.TSF_PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification. OE.PROTECT ensures that the TOE is protected from external interference or tampering.
T.UNAUTH	O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE. O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining any access to TOE security data. O.TSF_PROTECT mitigates this threat by ensuring continued operation of TOE in a secure state in the event of hardware failures.
T.UNINTENDED_ACCESS	O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded. O.ACCESS ensures only authorized iSCSI clients obtain access to TOE storage. O.TSF_PROTECT mitigates this threat by ensuring continued operation of TOE in a secure state in the event of hardware failures.
T.MGMT_NET	O.MGMT_PROTECT counters this threat by requiring protection of communications with remote administrators.
A.CLUSTER_NET	OE.CLUSTER_PROTECT upholds this assumption by requiring the cluster network to be protected from unauthorized access.
A.TIME	OE.TIME upholds this assumption by requiring an NTP server.
A.LOCATE	OE.PHYSICAL upholds this assumption by requiring the TOE environment to provide appropriate physical protection to the network resources.
A.PROTECT	OE.PROTECT satisfies this assumption by requiring the TOE environment to provide protection from external interference or tampering.
A.MANAGE	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.

Element	Justification
A.ADMIN_PROTECT	OE.ADMIN_PROTECT satisfies the assumption by ensuring that the Administrator Workstations is protected from external interference or tampering.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

61 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 16: Security Requirements Mapping

	O.AUDIT	O.ACCESS	O.ADMIN	O.AUTHENTICATE	O.USER_DATA_PROTECT	O.TSF_PROTECT	O.MGMT_PROTECT
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_STG.1	X						
FAU_STG.4	X						
FCS_COP.1							X
FDP_ACC.1		X					
FDP_ACF.1		X					
FDP_ROL.1					X		
FDP_SDI.2					X		
FIA_ATD.1				X			

	O.AUDIT	O.ACCESS	O.ADMIN	O.AUTHENTICATE	O.USER_DATA_PROTECT	O.TSF_PROTECT	O.MGMT_PROTECT
FIA_UAU.2				X			
FIA_UAU.5				X			
FIA_UID.2				X			
FIA_USB.1				X			
FMT_MOF.1			X				
FMT_MSA.1			X				
FMT_MSA.3			X				
FMT_MTD.1			X				
FMT_SMF.1			X				
FMT_SMR.1			X				
FPT_FLS.1						X	
FPT_TST.1						X	
FPT_STM.1	X						
FRU_FLT.1						X	
FTP_TRP.1							X

Table 17: Suitability of SFRs

Objectives	SFRs
O.AUDIT	FAU_GEN.1 meets the objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.

Objectives	SFRs
	FAU_GEN.2 meets the objective by ensuring all API calls, including the Web UI and Node UI actions, are associated with the administrator that invoked the event. FAU_SAR.1 meets the objective by ensuring that the TOE provides authorized administrators the ability to review logs. FAU_STG.1 meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion. FAU_STG.4 If the audit facilities become full, the TOE ensures that only the oldest records are overwritten. This requirement meets this objective by mitigating the risk of loss of audit trail data. FPT_STM.1 meets the objective by providing reliable time stamps for audit records.
O.ACCESS	FDP_ACC.1 meets the objective by ensuring that the Storage Access Control SFP is applied to all storage connection attempts by iSCSI clients. FDP_ACF.1 meets the objective by ensuring that the TOE enforces the Storage Access Control SFP on all storage connection attempts by iSCSI clients.
O.ADMIN	FMT_MOF.1 meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges. FMT_MSA.1 meets the objective by ensuring that the TOE restricts management of security attributes to only those users with the appropriate privileges. FMT_MSA.3 meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges. FMT_MTD.1 meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role. FMT_SMF.1 meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF. FMT_SMR.1 meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions, security attributes, and TSF data.
O.AUTHENTICATE	FIA_ATD.1 meets the objective by storing administrators' security attributes that are used for identification and authentication. FIA_UAU.2 meets the objective by ensuring each user is successfully authenticated before being allowed access to any TSF functionality. FIA_UAU.5 meets the objective by providing both local and LDAP authentication mechanisms. FIA_UID.2 meets the objective by ensuring that each user is identified before being allowed access to any TSF functionality.

Objectives	SFRs
	FIA_USB.1 meets the objective by ensuring that every API call is associated with the user that invoked the call through the user's security attributes.
O.USER_DATA_PROTECT	FDP_ROL.1 meets the objective by permitting rollbacks of volumes to defined points-in-time (snapshots). FDP_SDI.2 meets the objective by ensuring user data is monitored for integrity errors.
O.TSF_PROTECT	FPT_FLS.1 meets the objective by ensuring the TOE preserves a secure state upon defined drive or node hardware failures. FPT_TST.1 meets the objective by ensuring the TOE performs self-tests on TSF functions and data to detect failures. FRU_FLT.1 meets the objective by ensuring the operation of all the TOE's capabilities when defined hardware failures occur.
O.MGMT_PROTECT	FCS_COP.1 & FTP_TRP.1 meet this objective together by ensuring the protection of remote administrator traffic.

7.2.3 SFR Dependency Rationale

62 Table 18 below presents the SFR dependency rationale.

Table 18: SFR Dependency Rationale

Requirement	Dependencies	Met / Rationale if not met
FAU_GEN.1	FPT_STM.1	Met
FAU_GEN.2	FAU_GEN.1	Met
	FIA_UID.1	Met
FAU_SAR.1	FAU_GEN.1	Met
FAU_STG.1	FAU_GEN.1	Met
FAU_STG.4	FAU_STG.1	Met
FCS_COP.1	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	Not met. FCS_CKM.1 excluded per scheme guidance (CSE Instruction #4)
	FCS_CKM.4	Not met. Excluded per scheme guidance (CSE Instruction #4).
FDP_ACC.1	FDP_ACF.1	Met
FDP_ACF.1	FDP_ACC.1	Met

Requirement	Dependencies	Met / Rationale if not met
	FMT_MSA.3	Met
FDP_ROL.1	FDP_ACC.1	Met
FDP_SDI.2	No dependencies	Met
FIA_ATD.1	No dependencies	Met
FIA_UAU.2	FIA_UID.1	Met (FIA_UID.2)
FIA_UAU.5	No dependencies	Met
FIA_UID.2	No dependencies	Met
FIA_USB.1	FIA_ATD.1	Met
FMT_MOF.1	FMT_SMF.1	Met
	FMT_SMR.1	Met
FMT_MSA.1	FDP_ACC.1	Met
	FMT_SMF.1	Met
	FMT_SMR.1	Met
FMT_MSA.3	FMT_MSA.1	Met
	FMT_SMR.1	Met
FMT_MTD.1	FMT_SMF.1	Met
	FMT_SMR.1	Met
FMT_SMF.1	No dependencies	Met
FMT_SMR.1	FIA_UID.1	Met (FIA_UID.2)
FPT_FLS.1	No dependencies	Met
FPT_STM.1	No dependencies	Met
FRU_FLT.1	FPT_FLS.1	Met
FPT_TST.1	No dependencies	Met
FTP_TRP.1	No dependencies	Met

7.3 TOE Summary Specification Rationale

63 Table 19 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 19: Map of SFRs to TSS Security Functions

	Volume Access Control	Volume Rollback	Data Protection (Helix™)	Secure Administration	Security Audit	Self-tests
FAU_GEN.1					X	
FAU_GEN.2					X	
FAU_SAR.1					X	
FAU_STG.1					X	
FAU_STG.4					X	
FCS_COP.1				X		
FDP_ACC.1	X					
FDP_ACF.1	X					
FDP_ROL.1		X				
FDP_SDI.2			X			
FIA_ATD.1				X		
FIA_UAU.2				X		
FIA_UAU.5				X		
FIA_UID.2				X		
FIA_USB.1				X		
FMT_MOF.1				X		
FMT_MSA.1				X		

	Volume Access Control	Volume Rollback	Data Protection (Helix™)	Secure Administration	Security Audit	Self-tests
FMT_MSA.3				X		
FMT_MTD.1				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_FLS.1			X			
FPT_TST.1						X
FPT_STM.1					X	
FRU_FLT.1			X			
FTP_TRP.1				X		