NetApp StorageGRID 11.5

Security Target

Evaluation Assurance Level (EAL): EAL 2+

Version 1.1

July 2022

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	24 Jun 2022	G Nickel	Release for Certification
1.1	19 Jul 2022	G Nickel	Amended release for Certification

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the NetApp StorageGRID 11.5 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The NetApp StorageGRID 11.5 provides a flexible software-defined object-based storage solution for various use cases involving unstructured data including large archives, media repositories, and web data stores.

3 NetApp StorageGRID seamlessly and intelligently transfers data between on-premises and public cloud storage for increased availability, protection, and performance.

4 StorageGRID also supports industry-standard object APIs such as Amazon Simple Storage Service (S3) and the Open Stack Swift API.

Figure 1: Typical StorageGRID Appliance

1.2 Identification

Table 1: Evaluation identifiers

TOE Name	NetApp StorageGRID 11.5
TOE Version	11.5.0.5, Build 20211207.0815.1972031
Security Target	NetApp StorageGRID 11.5 Security Target, v1.1
Evaluation Assurance Level	EAL2+

1.3 Conformance Claims

5 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.1)

1.4 Terminology

Table 2: Terminology

Term	Definition
API	Application Programming Interface
ARN	Amazon Resource Name
CC	Common Criteria
EAL	Evaluation Assurance Level
HTTPS	Hypertext Transfer Protocol Secure
ILM	Information Lifecycle Management
NTP	Network Time Protocol
PP	Protection Profile
S3	Amazon Simple Storage Service
SFP	Security Function Policies
SSH	Secure Shell
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface

2 TOE Description

2.1 Type

6 The TOE is a data storage system.

2.2 Usage

7 The TOE consists of several grid nodes running in a cluster that complete the StorageGRID system as shown in Figure 1. At minimum, each site must have one Primary Admin node and three Storage nodes as depicted in Figure 2.

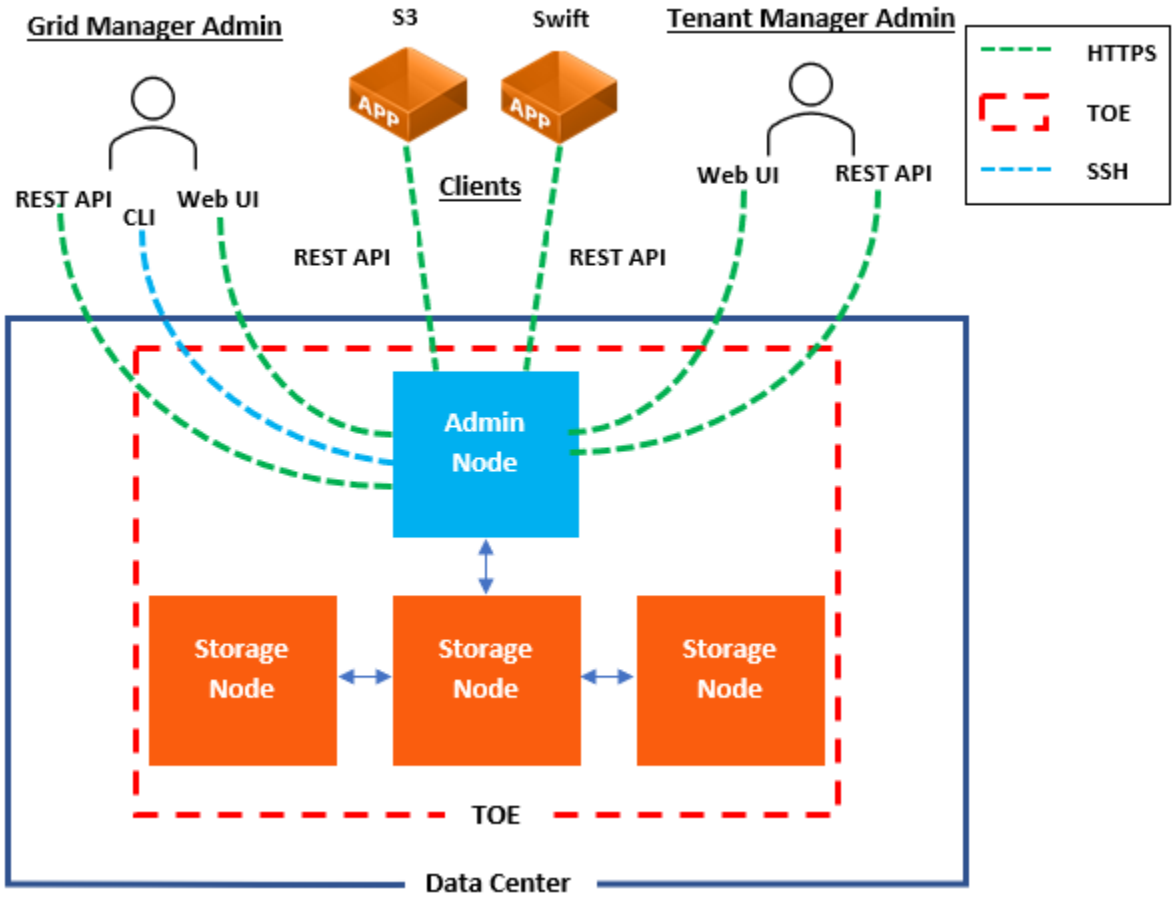

Figure 2: Example TOE deployment

8 The core components of the StorageGRID system are as follows:

a) **Admin Node.** Admin nodes provide management services such as system configuration, monitoring, logging, and management of storage accounts. The Admin node is what is connected to when signing into the Grid Manager and Tenant Manager (described in Section 2.2.1 TOE Administration). Each grid must contain one Primary Admin node for performing maintenance and any number of non-primary admin nodes for redundancy.

b) **Storage Node.** Storage nodes manage and store object data and metadata. Each grid must contain at least three storage nodes. If multiple sites are used, each site must also contain three storage nodes.

9 Each node runs the same core OS, but in addition contain services which are software modules that provide unique capabilities to the grid node.

10 At minimum, each site must contain one Admin Node and three Storage Nodes to create a functional grid network.

2.2.1 TOE Administration

11 Configuration, management, and monitoring functions for the StorageGRID system are accessed via:

a) **Grid Manager**. The Grid Manager UI provides the management environment for the TOE, Grid services, infrastructure topology, and creation of tenant accounts. Grid Manager also handles the data management policies and storage quotas for tenant accounts. The Grid Manager UI is hosted on an Admin Node. Each StorageGRID system must include one primary Admin Node and any number of non-primary Admin Nodes, however you can log in to any Admin Node to see similar views of the StorageGRID system. Bulk administration tasks can be performed via the associated Grid Manager REST API.

b) **Tenant Manager.** The Tenant Manager UI provides the management environment for tenant accounts, and the users and data it contains. Tenant Manager also retains the S3 access keys for S3 users and any bucket policies specified. The Tenant Manager UI is also hosted on an Admin Node. The Tenant Manager provides an interface for tenant users to configure, manage, and monitor their storage accounts. Bulk administration tasks can be performed via the associated Tenant Manager REST API.

c) **CLI (SSH).** Initial configuration, disaster recovery, and audit log access functions are performed via the CLI interface, but most administrative functionality is conducted through the browser-based Grid and Tenant Manager interfaces.

2.2.2 Client Communication

12 Client applications can store or retrieve objects by connecting to the Load Balancer service on Admin Nodes or directly to the Storage Nodes without a load balancer via the S3 REST API or Swift REST API. A corresponding S3 or Swift Tenant account must exist before API clients can store or retrieve objects. Each Tenant account has its own account ID, users and groups, and containers and objects. Tenant users can create and manage S3 buckets with the Tenant Manager, but they must have S3 access keys to use the S3 REST API to ingest, manage and access objects.

13 Information Lifecycle Management (ILM) rules are created by the Grid Administrator to manage object data ingested into the StorageGRID system via S3 REST API client applications. Once the specific rules are added to the ILM policy, StorageGRID can determine where and how object data is stored over time.

2.3 Security Functions / Logical Scope

14 The TOE provides the following security functions:

a) **Object Access Control.** The TOE enforces an administrator defined access control policy governing S3 and Swift client access to StorageGRID objects and buckets.

b) **Data Protection.** The TOE creates multiple replicas or Erasure Coded copies of objects according to an administrator-defined policy. This policy supports geographic rules to guard against site loss. Object data corruption is detected and repaired automatically when an object is accessed, or an administrator can trigger repairs after loss of physical storage. Three copies of object metadata are automatically created in each logical site.

c) **Security Management.** The TOE provides administrators with the ability to manage its security features and functions.

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

e) **Secure Communications.** The TOE provides secure communications for remote administrators and external applications.

2.3.1 Unevaluated Security Functions

15 The evaluation is limited to those security functions identified in section 2.3

16 Use of data-at-rest encryption in the SG5600 and SG5700 series appliances require the following:

a) Secure-capable drives, either FDE or FIPS drives

b) Security key to be used by the controller and drives for read/write access

c) Enable Drive Security for pools and volume groups

This functionality is not addressed by the security claims.

2.4 Physical Scope

17 The physical boundary of the TOE is the StorageGRID v11.5.0 software executing on the hardware identified in section 2.4.2. The TOE hardware is delivered via commercial courier and TOE software can be downloaded from the NetApp customer support portal.
Note: A NetApp customer support account is required to access software downloads.

2.4.1 Guidance Documents

18 The TOE includes the following guidance documents (PDF):

a) NetApp StorageGRID 11.5 Administrator Guide, 215-15094_2021-05_en-us | May 2021

b) NetApp StorageGRID 11.5 Tenant User's Guide, 215-15097_2021-05_en-us | May 2021

c) NetApp StorageGRID 11.5 Common Criteria Guidance Supplement, v1.1 | July 2022

19 Additional documentation can be found in the NetApp StorageGRID 11.5 Documentation Center: https://docs.netapp.com/sgws-115/index.jsp

2.4.2 TOE Hardware Components

20 The TOE includes the nodes listed in Table 3. All nodes run the same software and only have differences in CPU, memory, and drive capacity.

Table 3: TOE Hardware Devices (Nodes)

Model	Manufacturer	Processor
SG1000 Services Appliance (Admin Node)	NetApp	Intel Xeon(R) Gold 6230 CPU (Cascade Lake)
SG100 Services Appliance (Admin Node)	NetApp	Intel Xeon(R) Silver 4210R CPU (Cascade Lake)
SG5612 Storage Appliance (Storage Node)	NetApp	Intel Xeon(R) CPU E5-1428L v2 (Ivy Bridge)
SG5660 Storage Appliance (Storage Node)	NetApp	Intel Xeon(R) CPU E5-1428L v2 (Ivy Bridge)
SG5712 Storage Appliance (Storage Node)	NetApp	Intel Xeon(R) CPU D-1548 (Broadwell)
SG5760 Storage Appliance (Storage Node)	NetApp	Intel Xeon(R) CPU D-1548 (Broadwell)

2.4.3 Unevaluated Hardware

21 The NetApp StorageGRID 11.5 software is also supported on the following hardware appliances, but was not tested as part of this evaluation:

a) NetApp SG6000 Series Storage Appliances

b) NetApp SGF6000 Series Storage Appliances

2.4.4 Non-TOE Components

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

a) **NTP.** The TOE synchronizes with a minimum of four and a maximum of six external time servers via Network Time Protocol (NTP) to provide reliable timestamps.

3 Security Problem Definition

3.1 Threats

23 Threat agents are categorized by two separate sources:

a) **TOE End Users/Clients.** Consumers of the TOE who have user level access to TOE services or functions and could attempt to access data in which they are not privileged or intended to have access to.

b) **Non-TOE User Attackers.** External entities that have access to publicly available information on the functional operation or feature sets of the TOE and may attempt to access information or alter parameters in which they are not privileged to for a malicious purpose.

Table 4: Threats

Identifier	Description
T.DATA_CORRUPTION	Data could become corrupt or otherwise inaccessible due to hardware failure or invalid system access by TOE users or attackers.
T.UNAUTHORIZED_ ADMIN_ACCESS	A TOE end user, or attacker could gain access to StorageGRID data in which they are not authorized to access, resulting in compromise of the TSF or user data.
T.INTERCEPT	An attacker could intercept administrative communications or traffic thereby impacting the confidentiality and integrity of TSF data.
T.MALFUNCTION	The TOE, or TOE environment (including the network) could experience a malfunction or failure rendering the TOE inaccessible or non-functional.

3.2 Assumptions

Table 5: Assumptions

Identifier	Description
A.PHYSICAL_ACCESS_ CONTROL	The TOE is located within a secure facility with controlled physical access.
A.NO_EVIL	Administrators act in good faith during the course of their duties and follow all guidance, best practices, and policies.
A.CLUSTER_NETWORK	The TOE is deployed on a local network that is protected from unauthorized access.

3.3 Organizational Security Policies

24 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.PHYSICAL	The TOE shall be located within a secure facility with controlled access.
OE.TRUSTED	Administrators shall be trusted to act in good faith and follow guidance, and best practices in a trusted manner.
OE.CLUSTER_NETWORK	The TOE shall be deployed on a local network that is protected from unauthorized access (i.e. all nodes for a given instance of the TOE are deployed on the same local network).

4.2 Objectives for the TOE

Table 7: Security Objectives

Identifier	Description
O.AUDIT	The TOE must record security relevant events and associate each 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.

Identifier	Description
O.ACCESS	The TOE must implement rules to govern client access to objects and 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 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 and metadata 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.

5 Security Requirements

5.1 Conventions

25 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 string starting with “/” (e.g. “FCS_COP.1/Hash”).

5.2 Extended Components Definition

26 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
FDP_ACC.1	Subset access control

Requirement	Title
FDP_ACF.1	Security attribute based access control
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
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_STM.1	Reliable time stamps
FRU_FLT.1	Degraded fault tolerance
FTA_SSL.3	TSF-Initiated Termination
FTA_SSL.4	User-Initiated Termination
FTP_ITC.1	Inter-TSF Trusted Channel
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) [*Authentication events, Object events, Node events, Data Corruption events*]

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, [*Module ID, Node ID, Trace ID, Timestamp, Event Type, Version, Result/Message*].

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.

5.3.2 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 [*Tenant Storage Access Control SFP*] on [

- *Subjects: Principals (Users & Groups)*
- *Objects: Resources (Buckets and objects)*
- *Operations: Get, List, Create, Put, Delete*]

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 [*Tenant Storage Access Control SFP*] to objects based on the following: [

a) Principal (user or group) security attributes:

- *Account username*
- *Local permission group*
- *S3 Access Key*

b) Resource (bucket or object) security attributes:

- *S3 resource ARN*
- *Policy variables inside the object key*]

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 Bucket policy attached to a bucket and configured to allow access to buckets/objects by users in the bucket owner tenant account (or other accounts to the bucket and the objects in it), or a Group policy configured in the Tenant Manager that is attached to a group and configured to allow access to objects/resources by users in a specific group*].

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 following additional rules: [*No S3 Access (Default option, as configured in the Tenant Manager)*].

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 [*corrupt data fragments*] 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 [*remove the corrupt copy from its location and quarantine it elsewhere on the node. A new uncorrupted copy is generated and placed to satisfy the active ILM policy*].

5.3.3 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, permission groups, password for local authentication, S3 access key].*

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 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 the user and matching a local database*].

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.

5.3.4 Security Management (FMT)

FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [**perform the actions listed in Table 9 below**] the functions [*listed in Table 9 below*] to [*the roles listed in Table 9 below*].

Table 9: Management of Security Functions

Function	Action	Role/Permission
Sign in to the Grid Manager	Enable	Grid Administrator (with at least one permission)
Sign in to the Tenant Manager	Enable	Tenant Administrator (with at least one permission)
Change own Password (local user)	Modify the behaviour of	Grid Administrator*, Tenant Administrator* * - with at least one permission
Access to all Grid administration features	Modify the behaviour of	Grid Administrator (Root Access Permission)

Function	Action	Role/Permission
Managing alerts (silences, notifications, rules)	Modify the behaviour of	Grid Administrator (Manage Alerts Permission)
Acknowledge and respond to alarms	Modify the behaviour of	Grid Administrator (Acknowledge Alarms Permission)
Access to Grid configuration pages and menu options	Modify the behaviour of	Grid Administrator (Grid Topology Page Configuration Permission)
Create Tenant accounts and manage Tenant group policies	Modify the behaviour of	Grid Administrator (Tenant Accounts Permission)
Tenant account root password	Modify the behaviour of	Grid Administrator (Tenant Accounts Permission & Change Tenant Root Password Permission)
Access to maintenance and recovery tasks, DNS and NTP network configuration, software updates, and licensing.	Modify the behaviour of	Grid Administrator (Maintenance Permission)
Access to system metrics page, perform metrics queries.	Determine the behaviour of	Grid Administrator (Metrics Query Permission)
Access to ILM rules, policies, erasure coding, and regions menu options	Modify the behaviour of	Grid Administrator (ILM Permission)
Full access to the Tenant Manager and Tenant Management API	Modify the behaviour of	Tenant Administrator (Root Access Permission)
Full access to Swift containers and objects for tenant account	Modify the behaviour of	Tenant Administrator (Administrator Permission)
Create and remove own S3 access keys	Modify the behaviour of	Tenant Administrator (Manage Own S3 Credentials*) * - S3 Tenants only
Create and delete S3 buckets, manage settings for all S3 buckets in tenant account	Modify the behaviour of	Tenant Administrator (Manage All Containers Permission)

Function	Action	Role/Permission
Create or edit endpoints to be used as destinations for platform services	Modify the behaviour of	Tenant Administrator (Manage Endpoints Permission)

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_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*Tenant Storage Access Control SFP*] to restrict the ability to [query, modify, delete, *[add]*] the security attributes [*permission groups*] to [*Tenant Administrators*].

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 [*Tenant 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 [*Tenant 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_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*perform the operations listed in Table 10*] to [*Grid Administrators with the defined permission*].

Table 10: Management of TSF Data

Management Permission	Operation Description
Root Access	Provides access to all grid administration features.
Manage Alerts	Provides access to options for managing alerts. Users must have this permission to manage silences, alert notifications, and alert rules.

Management Permission	Operation Description
Acknowledge Alarms (legacy systems)	Provides access to acknowledge and respond to alarms (legacy systems). All signed-in users can view current and historical alarms. This permission allows a user to monitor grid topology and acknowledge alarms only.
Grid Topology Page Configuration	Provides access to the following menu options: • Configuration tabs in the Grid Topology page • Reset event counts in the Events tab

Other Grid Configuration	Provides access to additional grid configuration options
	Note: to access these additional options, users must also have the ***Grid Topology Page Configuration*** permission.
	• Alarms (legacy system)
	  ○ Global Alarms
	  ○ Email Setup
	• ILM
	  ○ Storage Pools
	  ○ Storage Grades
	• System Settings
	  ○ Grid Options
	  ○ Link Cost
	  ○ Storage Options
	  ○ Display Options
	• Monitoring
	  ○ Events
	• Support
	  ○ Auto Support

Tenant Accounts	Provides access to the Tenant Accounts page.
Change Tenant Root Password	Provides access to the Change Root Password button on the Tenant Accounts page. This allows control over who can change the password for the tenant's local root user. Note: you must assign the Tenant Accounts permission to an admin group before this permission can be assigned.

Management Permission	Operation Description

Maintenance	Provides access to the following menu options:
	• Configuration > System Settings
	  ○ Domain Names*
	  ○ Server Certificates*
	• Configuration > Monitoring
	  ○ Audit*
	• Maintenance > Maintenance Tasks
	  ○ Expansion
	  ○ Decommission
	  ○ Recovery
	• Maintenance > Network
	  ○ Grid Network*
	  ○ DNS Servers*
	  ○ NTP Servers*
	• Maintenance > System
	  ○ Software Update
	  ○ License*
	  ○ Recovery Package
	• Support
	  ○ Logs
	*Users who do not have the Maintenance permission can view, but not edit, the pages marked with an asterisk.

Metrics Query	Provides access to the Support > Metrics page. Also provides access to custom metrics queries using the Metrics section of the Grid Management API.

ILM	Provides access to the following menu options:
	• ILM
	  ○ Rules
	  ○ Policies
	  ○ Erasure Coding
	  ○ Regions

Object Metadata Lookup	Provides access to the ILM > Object Metadata Lookup menu option.
Storage Appliance Administrator	Provides access to E-Series SANtricity System Manager.

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: [*Manage alerts, acknowledge alarms, configure grid topology, configure tenant accounts, conduct Grid maintenance actions, view metrics and event logs, restore and repair data objects, control access to data objects (Tenant Administrator only)*].

FMT_SMR.1 Security Roles

Hierarchical to:	No other dependencies
Dependencies:	FIA_UID.1 Timing of Identification
FMT_SMR.1.1	The TSF shall maintain the roles [*Grid Administrator, Tenant Administrator*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

5.3.5 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: [*one or more drive failures on a TOE node, a TOE node failure, or a TOE site failure*].

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.

5.3.6 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 a TOE node, a TOE node failure, or a TOE site failure*].

5.3.7 TOE Access (FTA)

FTA_SSL.3 TSF-initiated Termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*Administrator-configurable time interval of session inactivity or expiration*].

Application Note: Applicable to both the Grid Manager and Tenant Manager administrative interfaces which includes the associated REST API's.

FTA_SSL.4 User-initiated Termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.4.1 The TSF shall allow user-initiated termination of user's own interactive session.

5.3.8 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [another trusted It product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*no other functions*].

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~~ **administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure].

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

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

5.4 Assurance Requirements

27 The TOE security assurance requirements are summarized in Table 11 commensurate with EAL2+ (ALC_FLR.1).

Table 11: Assurance Requirements

Assurance Class	Components	Description
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: 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.1	Basic Flaw Remediation
ASE: 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

Assurance Class	Components	Description
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Object Access Control

28 The TOE enforces an administrator defined access control policy governing S3 and Swift client access to StorageGRID objects and buckets.

Table 12: Security Function SFRs

SFR	Fulfilment
FDP_ACC.1	The TOE enforces the Tenant Storage Access Control SFP to control subject/principal access to StorageGRID objects and resources. Principals are defined by users and groups that are the subjects to an object or resource. Resources are defined by buckets and the objects contained within the bucket. StorageGRID implements a subset of the S3 REST API policy language that uses JSON format for writing policies. Bucket policies are configured using the GET, PUT, and DELETE Bucket policy S3 API operations. Bucket policies are attached to buckets and are configured to control access by users in the bucket owner account or other accounts to the bucket and the objects in it. Bucket policies apply to one bucket and potentially many groups.
FDP_ACF.1	Access to objects is configured by a Tenant administrator defining the security attributes of the subjects/principals (users & groups) including identity ARN, and account username. Group policies are configured using the Tenant Manager or Tenant Management API. Group policies are attached to a group in the account and are configured to allow a specific group access to specific resources owned by that account. Group policies apply to one group and possibly many buckets. StorageGRID supports S3 IAM policies enabling the specification of granular access controls by tenant, bucket, or object prefix. Support for IAM policy conditions and variables is also provided by StorageGRID for more dynamic policies. This allows for administrators to specify access by user groups for the whole tenant as well as individual user buckets and objects. Each user of an S3 tenant account must have an access key to store and retrieve objects on the StorageGRID system. Access keys consist of an access key ID and a secret access key. Users that are granted the *Manage Your Own S3 Credentials* permission can create or remove their own S3 access keys. Users who have the *Root Access* permission can manage the access keys for the S3 root account, and all other users.

6.2 Data Protection

29 The TOE creates multiple replicas or Erasure Coded copies of objects according to an administrator-defined policy. This policy supports geographic rules to guard against site loss. Object data corruption is detected and repaired automatically, although an administrator can trigger repairs after loss of physical storage.

30 The TOE also automatically creates three copies of object metadata in each logical site. These copies are stored in a Cassandra database and are evenly distributed across storage nodes. An administrator can trigger repairs after loss of physical storage.

Table 13: Security Function SFRs

SFR	Fulfilment
FPT_FLS.1	The TOE is designed to preserve a secure state when a failure of a drive or node occurs. The TOE creates physically and logically redundant environments. Each site must contain a minimum of three storage nodes to achieve fault tolerance. Exact copies of data that are then created and replicated to other Storage Nodes or Archive Nodes. In the event of a failure, the replicated copies of the data can be retrieved from another node.
FRU_FLT.1	The TOE ensures the availability of user data should a failure of a drive or node occur. Erasure coding is implemented to fragment data and distributed it across nodes for redundancy. Each object is divided into fragments. Parity fragments are then created from the object data and distributed across different nodes. Should a data or parity fragment become corrupt, the erasure coding algorithm can rebuild the corrupt fragment using the remaining data and parity fragments.
FDP_SDI.2	The TOE actively monitors stored user data for corrupt fragments. After every 64KB of data, a CRC32 checksum is added which is checked by integrity verification processes as well as on reads and replication events. Two object integrity verification processes are implemented by the TOE: Background Verification and Foreground Verification. Background verification automatically runs in the background to continuously check Storage nodes for the correctness of object data. Foreground verification is manually triggered by a user to verify the existence of objects. Background verification will identify any corrupt copies of object data and attempt to repair issues automatically. Background verification checks the integrity of both replicated objects and erasure-coded objects. Corrupt objects are not deleted from the system, they are instead quarantined in order that they may still be accessed. Object metadata is also protected with a CRC32 checksum that is checked automatically on read events. Object metadata is stored in a Cassandra database which is called a metadata store. Three copies of object metadata are retained and distributed across storage nodes to prevent metadata loss.

6.3 Security Management

31 The TOE provides administrators with the ability to manage its security features and functions.

SFR	Fulfilment
FIA_ATD.1	The TOE maintains a record of security attributes for each user in a local database. These attributes include: username, password, and assigned permissions groups.
FIA_UAU.2	The TOE does not offer any functionality to an administrator prior to authentication. Administrators must be part of a group that is assigned at least one permission in order to sign in to the grid manager or tenant manager.

SFR	Fulfilment
FIA_UAU.5	The TOE authenticates users with a local authentication mechanism. Users must provide a username and password credential that matches a local database entry.
FIA_UID.2	The TOE does not offer any functionality or actions to be taken on behalf of a user before they are successfully identified and authenticated. Administrators must be a member of a group that is assigned at least one permission in order to claim an identity and successfully authenticate against that identity.
FMT_MOF.1	The TSF requires at least one management permission to be assigned to an admin group, otherwise users belonging to that group will not be able to sign-in to the Grid Manager or Tenant Manager. By default, any Grid Manager user who belongs to a group that has at least one management permission assigned to it can perform the following tasks: - Sign-in to the Grid Manager - View the Dashboard - View the Nodes pages - Monitor the Grid topology - View current and historical alerts and alarms - Change their own password - View limited information on the Configuration and Maintenance pages For more granular control over the management of security functions in the Grid Manager, users must be a member of a group that is assigned one or more of the following permissions: - Root Access – Provides access to all grid administration features. - Manage Alerts – Provides access to options for managing alerts, silences, notifications, and rules. - Acknowledge Alarms – Provides access to acknowledge and respond to alarms. - Grid Topology Page Configuration – Provides access to the Grid Topology configuration menu tabs and event count reset link in the events page. - Other Grid Configuration – Provides access to additional grid configuration options including global alarms, ILM storage pools, display options, and support. - Tenant Accounts – Provides access to the Tenant Accounts page. - Change Tenant Root Password – Provides access to the Change Root Password button on the Tenant Accounts page. - Maintenance – Provides access to system settings for domain names and server certificates, expansion, decommission, and

SFR	Fulfilment
	recovery tasks, DNS and NTP network settings, and software updates including license and recovery options. - Metrics Query – Provides access to the Metrics page, and metrics queries. - ILM – Provides access to ILM rules, policies, erasure coding settings, and region configuration. - Object Metadata Lookup – Provides access to the Object Metadata Lookup feature. - Storage Appliance Administrator – Provides access to E-Series SANtricity System Manager. By default, any Tenant Manager user who belongs to a group that has at least one management permission assigned to it can perform the following tasks: - Sign-in to the Tenant Manager - View the Dashboard - Change their own password (local users) For more granular control over the management of security functions in the Tenant Manager, users must be a member of a group that is assigned one or more of the following permissions: - Root Access – Provides full access to the Tenant Manager and the Tenant Management API. - Administrator – Swift tenants only. Provides access to the Swift containers and objects for the specific tenant account. Swift users must have this permission to perform any operations with the Swift REST API. - Manage Your Own S3 Credentials – S3 tenants only. Allows users to create and remove their own S3 access keys. - Manage All Buckets – Allows users to change settings of all S3 buckets (or Swift containers) in the account. - Manage Endpoints – S3 tenants only. Allows users to configure endpoints to be used as destinations for StorageGRID platform services.
FMT_MSA.1	The TSF restricts the ability to query, modify, delete, or add security attributes to administrators that are either assigned the required permissions directly, or has membership to an admin group that is assigned the required permission to execute actions on security attributes.
FMT_MSA.3	The TOE only allows administrators within function-specific groups to override default values or configurations for a given security function. This behaviour is replicated for newly created objects or information. By default, access is denied to objects unless explicitly granted by an administrator.
FMT_MTD.1	The TSF defines several management permissions that allow specific actions or operations to be taken allowing for administrative separation of duties and least privilege principle.

SFR	Fulfilment
	Grid Administrators assigned to groups with appropriate permissions are permitted to manage and modify the configuration of the Grid topology, network parameters, alert and alarms, and recovery functions. Tenant Administrators are denied access to Grid Management features and functionality, but with appropriate permissions are permitted to manage access to data contained within the tenant account and the users that may access it.
FMT_SMF.1	The TOE is capable of performing the following management functions: Providing alerting and alarm functions, node and topology configuration, creating storage pools, controlling access to storage objects, managing Tenant accounts, maintenance of the Grid topology, and recovery functions.
FMT_SMR.1	All local users created on the TOE are of administrative function. By default, newly created accounts will not have any access or be able to log into the TOE unless the account becomes a member of a group with at least one administrative permission.
FTA_SSL.3	The TOE implements a session timeout feature that allows an administrator to control whether Grid Manager and Tenant Manager users are automatically signed out if they are inactive for more than a configurable period of time. By default, the GUI inactivity timeout occurs at 900 seconds (15 minutes) and can be increased or decreased. If a user's browser session times out, the system behaves as if the user clicked 'Sign Out' manually, and therefore the user must re-enter their credentials to regain access. The Management API supports the Bearer Token Authentication Scheme and issues a security token if the user is successfully authenticated. These security tokens have a default expiration time of 16 hours but is configurable by an administrator.
FTA_SSL.4	The TOE provides a Sign Out feature to allow administrators to terminate their own session by manually signing out of an interactive session.

6.4 Security Audit

32 The TOE keeps audit records of security relevant events.

SFR	Fulfilment
FAU_GEN.1	The TOE generates audit records for the following events: start-up and shut-down events, authentication events, object events including requests to retrieve, create, or modify an object, node events, data verification and corruption events. For each event logged, the TOE collects and logs the following information: Module ID, Node ID, Trace ID, Timestamp, Event type, Version of the audit message (for new versions of services), and Result (the outcome of the event). Only administrators with the 'Maintenance' permission are able to delete the audit log.
FAU_GEN.2	The TOE generates audit records of events that include the identity (where applicable) of the user that triggered or caused the event.

SFR	Fulfilment
FPT_STM.1	The TOE provides reliable time stamps by synchronizing with an external NTP server. In each site, a minimum of two nodes in the StorageGRID system must be assigned the Primary NTP role for redundancy. These nodes must then synchronize to a minimum of four and maximum of six external time sources. The primary NTP nodes will then provide reliable time source to the other nodes within the grid.

6.5 Secure Communications

33 The TOE provides secure communications for remote administrators and external applications.

SFR	Fulfilment
FTP_ITC.1	The TOE uses HTTPS to protect communications between itself and the S3 and Swift API clients. The TOE implements TLS 1.2 and 1.3 only and supports the following ciphersuites for the client access interface: TLS v1.2 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS v1.3 • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 The ciphersuites listed above are not configurable.
FTP_TRP.1	The TOE protects all communications between remote administrators and the Grid Manager, Tenant Manager, and API via HTTPS. The TOE implements TLS 1.2 and 1.3 only and supports the following ciphersuites for the web management interface. TLS v1.2 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

SFR	Fulfilment
	• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS v1.3 • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 The TOE also provides a CLI interface for initial configuration and maintenance activities that is accessible to an administrator via SSHv2 with the following characteristics (in the evaluated configuration): • Password based and public key based authentication is supported with the following types: ▪ ecdsa-sha2-nistp256 ▪ ecdsa-sha2-nistp384 ▪ ecdsa-sha2-nistp521 ▪ rsa-sha2-512 ▪ rsa-sha2-256 ▪ ssh-rsa ▪ ssh-ed25519 • Encryption with support for the following ciphers: ▪ aes128-ctr ▪ aes192-ctr ▪ aes256-ctr ▪ aes128-gcm@openssh.com ▪ aes256-gcm@openssh.com • Data integrity for SSH connections with support for the following MAC algorithms: ▪ hmac-sha1 ▪ hmac-sha1-etm@openssh.com ▪ hmac-sha2-256 ▪ hmac-sha2-256-etm@openssh.com ▪ hmac-sha2-512 ▪ hmac-sha2-512-etm@openssh.com • Secure key exchange with support for the following algorithms: ▪ ecdh-sha2-nistp256 ▪ ecdh-sha2-nistp384

SFR	Fulfilment
	▪ ecdh-sha2-nistp521 ▪ diffie-hellman-group16-sha512 ▪ diffie-hellman-group18-sha512 ▪ diffie-hellman-group14-sha256 ▪ diffie-hellman-group-exchange-sha256 ▪ curve25519-sha256 ▪ curve25519-sha256@libssh.org

7 Rationale

7.1 Security Objectives Rationale

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

Table 14: Security Objectives Mapping

	T.DATA_CORRUPTION	T.UNAUTHORIZED_ADMIN_ACCESS	T.INTERCEPT	T.MALFUNCTION	A.PHYSICAL_ACCESS_CONTROL	A.NO_EVIL	A.CLUSTER_NETWORK
O.AUDIT	X	X					
O.ACCESS		X					
O.ADMIN		X					
O.AUTHENTICATE		X					
O.USER_DATA_PROTECT	X			X			
OE.PHYSICAL		X			X		X
OE.TRUSTED						X	
OE.CLUSTER_NETWORK			X				X

35 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** requires that security relevant events including unauthorized access or modification attempts to the TOE are recorded. **O.USER_DATA_PROTECT** ensures that all data and metadata is monitored for errors or corruption and if detected, can be restored to a known good state or point in time.

Element	Justification
T.UNAUTHORIZED_ADMIN_ ACCESS	**O.AUDIT** requires that security relevant events including unauthorized access or modification attempts to the TOE are recorded. **O.ACCESS** enforces rules to control both client access to stored data objects and administrative access to the TOE for authorized users only. **O.ADMIN** ensures that all functionality that facilitates the secure management of TOE functions, attributes, and data are accessible only to authorized administrators with appropriate permissions. **O.AUTHENTICATE** protects the TOE from unauthorized access by enforcing complete identification and authentication processes prior to allowing access to the TOE and its TSF data. **OE.PHYSICAL** satisfies the assumption by requiring the TOE environment to provide appropriate physical protection for the TOE and network resources.
T.INTERCEPT	**OE.CLUSTER_NETWORK** ensures that all Administrative workstations are secured from external interference or tampering and integrity of communications are protected.
T.MALFUNCTION	**O.USER_DATA_PROTECT** ensures that all data and metadata is monitored for errors or corruption and if detected, can be restored to a known good state or point in time.
A.PHYSICAL_ACCESS_ CONTROL	**OE.PHYSICAL** satisfies the assumption by requiring the TOE environment to provide appropriate physical protection for the TOE and network resources.
A.NO_EVIL	**OE.TRUSTED** satisfies the assumption by trusting administrators to act in good faith by following all guidance, best practices and policies for the secure administration of the TOE.
A.CLUSTER_NETWORK	**OE.PHYSICAL** satisfies the assumption by requiring the TOE environment to provide appropriate physical protection for the TOE and network resources. **OE.CLUSTER_NETWORK.** ensures that all Administrative workstations are secured from external interference or tampering and integrity of communications are protected.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

36 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.1 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
FAU_GEN.1	X				
FAU_GEN.2	X				
FDP_ACC.1		X			
FDP_ACF.1		X			
FDP_SDI.2					X
FIA_ATD.1				X	
FIA_UAU.2				X	
FIA_UAU.5				X	
FIA_UID.2				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_STM.1	X				
FRU_FLT.1					X

	O.AUDIT	O.ACCESS	O.ADMIN	O.AUTHENTICATE	O.USER_DATA_PROTECT
FTA_SSL.3			X		
FTA_SSL.4			X		
FTP_ITC.1		X			
FTP_TRP.1			X		

Table 17: Suitability of SFRs

Objectives	SFRs
O.AUDIT	**FAU_GEN.1** satisfies the objective by ensuring the TOE maintains records of security related events that include relevant details. **FAU_GEN.2** satisfies the objective by ensuring all API calls, WebUI, and CLI actions are associated with the specific administrator that caused the event. **FPT_STM.1** meets the objective by providing reliable timestamps for use in audit records and other functions.
O.ACCESS	**FDP_ACC.1** meets the objective by enforcing the Tenant Storage Access Control SFP on all subjects, objects, and operations by ensuring it is applied to all storage connection attempts by clients. **FDP_ACF.1** meets the objective by ensuring that the TOE enforces the Tenant Storage Access Control SFP on all storage connection attempts by clients and ensuring the correct security attributes for each client are present for authorized access. **FTP_ITC.1** meets the objective by providing a trusted communication channel that is protected from disclosure of data in transit by using a secure protocol.
O.ADMIN	**FMT_MOF.1** satisfies the objective by ensuring that administrative functions are restricted to administrators with sufficient privileges to access the specific function. **FMT_MSA.1** meets the objective by ensuring that the management of security attributes is restricted to administrators with specific permissions to modify that data.

Objectives	SFRs
	FMT_MSA.3 meets the objective by ensuring that administrative functions are restricted to administrators with the appropriate privileges. **FMT_MTD.1** satisfies the objective by ensuring that access to TSF data is restricted to administrators that are assigned to appropriate permissions groups. **FMT_SMF.1** meets the objective by ensuring that sufficient administrative functions are provided by the TOE to manage the TSF **FMT_SMR.1** satisfies the objective by ensuring that users are associated with roles or permission groups by the TOE to provide access to specific TSF management functions, security attributes, and TSF data. **FTA_SSL.3** meets the objective by ensuring that the TOE initiates a termination of an idle interactive session. **FTA_SSL.4** meets the objective by ensuring that an administrative user can initiate the termination of an interactive session. **FTP_TRP.1** satisfies this objective by ensuring the protection of network traffic between remote administrators and the TOE via a secure protocol.
O.AUTHENTICATE	**FIA_ATD.1** meets the objective by ensuring the TOE stores administrative user security attributes that are used for identification and authentication. **FIA_UAU.2** meets the objective by ensuring that the TOE successfully authenticates users prior to permitting access to TSF functions or data. **FIA_UAU.5** meets the objective by providing a local authentication mechanism for authentication. **FIA_UID.2** meets the objective by ensuring that each user is successfully identified before access to TSF functionality is granted.
O.USER_DATA_PROTECT	**FDP_SDI.2** meets the objective by ensuring user data is monitored for integrity errors and corruption. **FPT_FLS.1** meets the objective by ensuring the TOE maintains a secure state should a drive, node, or site fail. **FRU_FLT.1** meets the objective by ensuring the continued operation of all TOE capabilities in the event of a drive, node, or site failure.

7.3 TOE Summary Specification Rationale

37 Table 18 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 18: Map of SFRs to TSS Security Functions

	Object Access Control	Data Protection	Security Management	Security Audit	Secure Communications
FAU_GEN.1				X	
FAU_GEN.2				X	
FDP_ACC.1	X				
FDP_ACF.1	X				
FDP_SDI.2		X			
FIA_ATD.1			X		
FIA_UAU.2			X		
FIA_UAU.5			X		
FIA_UID.2			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_STM.1				X	
FRU_FLT.1		X			

	Object Access Control	Data Protection	Security Management	Security Audit	Secure Communications
FTA_SSL.3			X		
FTA_SSL.4			X		
FTP_ITC.1					X
FTP_TRP.1					X